Bluetooth Low Energy in Wireless PKI deployments

mToken BLE ecosystem White Paper

Century Longmai Technology Co., Ltd.

CONTENTS

1. Introduction

The evolution of mobile applications and mobile payment industries is accompanied by two technologies i.e. Bluetooth Low Energy (BLE) and host card emulation (HCE) with Near Field Communication (NFC). With the increasing consumer demands for greater privacy of their communications, network security problems have drawn much attention, especially in government telecom, and financial industries. In this paper, we define Bluetooth from the technical and organizational context, and discuss the security and privacy designs when using this technology in Public key infrastructure. Bluetooth silently connects so many of our gadgets together, it's easy to forget it's a pretty impressive piece of technology on its own. It helps us listen to music, talk on our phones, and play video games, all without being frustrated by miles of cables strewn around the place. We present Century Longmai's newly launched wireless token series that utilize the Bluetooth communication protocol to secure a wide range of applications and realize robust identity authentication functions especially in mobile and wireless transaction markets.

As one of the leading digital Information security device manufacturers in China, Century Longmai is always excited on best informing those in IT security and related industries about technologies used in our innovative products.

Who Should Read This Document?

Because this document comprises conceptual and future mobile payment market security, its audience is broad. This document sets the stage with an overview of Bluetooth technology. Then, it describes how Century Longmai implements Bluetooth technology in its Public Key Infrastructure (PKI) tokens to meet end-users' mobility needs. If you are unfamiliar with Bluetooth technology in general, you can read this document for a high-level summary. If you are primarily interested in learning about Century Longmai mToken BLE ecosystem product series, you will find a thorough description and application scenarios in this document. Finally, if you are involved in deploying mobile payment solutions that utilize wireless Public Key Infrastructure or communicate with Bluetooth enabled devices, you should read this document to discover your options.

Get more technical information on Bluetooth technology including core specifications, FAQs and Quick Reference Guides. Links to tools and information:

- Quick Reference Guide
- Frequently Asked Questions
- Bluetooth Brand Guide

Getting Additional Information

Century Longmai provides reference documentation for the mToken BLE ecosystem wireless PKI token products series that utilizes Bluetooth low energy. If you have any questions

regarding mToken BLE ecosystem, review our frequently asked Questions at http://lm-infosec.com/about-us/faqs/ ; if you would like to request for technical assistance or would like to provide feedback about our products and solutions, visit Contact Us Page at http://lm-infosec.com/contact/

Definitions

- **Bluetooth** is a technology that makes short-range wireless connections between devices at distances up to 10 meters (33 feet).
- **Bluetooth Smart** refers to qualified products incorporating Bluetooth Core Specification Version 4.0 (or higher) with a Low Energy Core Configuration or Basic Rate and Low Energy Combined Core Configuration and using the GATT-based architecture to enable particular functionality of the product.
- ***Bluetooth Smart Ready*** refers to qualified products incorporating Bluetooth Core Specification Version 4.0 (or higher) with a Basic Rate and Low Energy Combined Core Configuration, and using the GATT-based architecture to provide a means by which the end user can choose to update the Bluetooth Smart Ready product with the functionality of a Bluetooth Smart product.
- ***Bluetooth Smart technology*** is a wireless communications system intended to replace the cables connecting many types of devices, from mobile phones and headsets to hear monitors and medical equipment. Learn more about how Bluetooth Smart increases opportunities for developers to make consumers' lives easier.

2. Bluetooth Overview

This section seeks to give you an overview of the Bluetooth technology. If you're already familiar with the Bluetooth specification and how Bluetooth devices work, you might choose to skip ahead to mToken BLE ecosystem. Bluetooth is an open specification that enables low-bandwidth, short-range wireless connections between computers and peripherals, such as keyboard, mouse, Smartphone, and personal data assistant (PDA). The appeal of the Bluetooth model lies in its convenience for wirelessly transferring information and small data files between devices. Meanwhile, the Core Bluetooth framework enables support for communication between applications and Bluetooth devices. For example, when a health monitoring app can discover, explore, and interact with peripheral devices, such as heart rate monitors, digital thermostats, and even other multi-platform based devices.

How Bluetooth Works

Bluetooth devices operate at 2.4 GHz in the license-free, globally available Industrial, Scientific, and Medical (ISM) radio band. Bluetooth chips produce wavelengths that are bound to frequencies operating within a range specifically set aside for short-range communication. The advantage of operating in this band is worldwide availability and compatibility; but the potential disadvantage is that Bluetooth devices must share this band with many other Radio Frequency (RF) Emitters. To overcome this challenge, Bluetooth employs a fast frequency-hopping scheme and uses shorter packets than other standards in the ISM band. The frequent change in wavelength means that even a consistent signal won't interrupt, and won't be interrupted, for longer than 1/1600th of a second.This scheme makes Bluetooth communication more robust and more secure.

Frequency Hopping

Frequency hopping is literally jumping from frequency to frequency within the ISM band. After a Bluetooth device sends or receives a packet, it and the Bluetooth device or devices it is communicating with "hop" to another frequency before the next packet is sent. This scheme has three advantages:

- It allows Bluetooth devices to use the entirety of the available ISM band, while never transmitting from afixed frequency for more than a very short time. This ensures that Bluetooth conforms to the ISM restrictions on transmission quantity per frequency.
- It ensures that any interference will be short-lived. Any packet that doesn't arrive safely at its destination can be re-sent at the next frequency.
- It provides a base level of security because it's very difficult for an eavesdropping device to predict whichfrequency the Bluetooth devices will use next.

Of course, the connected devices must agree upon the next frequency to use. The Bluetooth specification ensures this in two ways. First, it defines a master-slave relationship between Bluetooth devices. Second, it specifies an algorithm that uses device-specific information to calculate frequency-hop sequences.

A Bluetooth device operating in master mode can communicate with up to seven slave devices. To each of its slaves, the master Bluetooth device sends its own unique device address (similar to an Ethernet address) and the value of its internal clock. This information is used to calculate the frequency-hop sequence. Because the master device and all its slaves use the same algorithm with the same initial input, the connected devices always arrive together at the next frequency.
Click to go to section 3 to learn more about the mToken BLE Ecosystem core framework change

Power Consumption

As a cable-replacement technology, it's not surprising that Bluetooth devices are usually battery-powered devices, such as wireless mice and mobile phones. To conserve power, most Bluetooth devices operate as low-power, 1 mW radios (Class 3 radio power). This gives Bluetooth devices a range of about 5 – 10 meters. This range is far enough for comfortable wireless peripheral communication but close enough to avoid drawing too much power from the device's power source.

Security

Security is a challenge faced by every communications standard. Wireless communications present special security challenges. Bluetooth builds security into its model on several different levels, beginning with the security inherent in its frequency-hopping scheme (described in Frequency Hopping). At the lowest levels of the protocol stack, Bluetooth uses the publicly available cipher algorithm known as SAFER+ to authenticate a device's identity. The generic-access profile depends on this authentication for its device-pairing process. This process involves creating a special link to create and exchange a link key. Once verified, the link key is used to negotiate an encryption mode the devices will use for their communication.

Bluetooth Core Specification 4.2

Bluetooth 4.2 is an important update to the Bluetooth Core Specification delivering exciting new features and benefits for Bluetooth Smart technology. Release on December 2, 2014, this update has created significant advantages for Century Longmai product development by enabling us provide a hardware based wireless PKI solution for mobile users to transact from anywhere with better user experience and assured privacy. The mToken BLE ecosystem series of products from Century Longmai feature Bluetooth Low Energy communication protocol in addition to USB support; making us the first in the Industry to realize PKI powered by Bluetooth Wireless technology in a smarter, faster and more secure fashion.

Features and Benefits

Key features of Bluetooth high speed wireless technology include:

- **Power Optimization.** The new Bluetooth technology reduces power consumption. The high speed radio is used only when necessary, which means longer battery life for your devices.
- **Improved Security:** The Generic Alternate MAC/PHY in Bluetooth high speed enables the radio to discover other high speed devices only when they are needed in the transfer of music, video and other large data files. This decreases power consumption and increases radio security.
- **Enhanced Power Control:** Drop-out reduction is now a reality: enhanced Bluetooth technology makes power control faster and reduces the impact of a power or signal loss.

- **Lower Latency Rates:** Unicast Connectionless Data (UCD) improves the user's speed experience by moving small amounts of data faster, which lowers latency rates.

For complete information on Bluetooth 4.2 features and benefits, technical details, tools and more please visit: https://www.bluetooth.org/en-us/specification/adopted-specification

Bluetooth Architecture

The topic of Bluetooth Architecture (including Bluetooth Protocol stack and Bluetooth profiles) is beyond the scope of this document. For more information on Bluetooth Protocol Stack and Profiles, visit https://www.bluetooth.org/en-us/specification/adopted-specifications/

BLE Application services

Bluetooth has evolved to be a perfect mobile connectivity option, because it doesn't take much energy, and the signal isn't broadcast for miles. The data transfer speed of Bluetooth isn't particularly high, so while uses like streaming music, transferring larger amounts of data would take far too long to be practical. The low power consumption is also important when Bluetooth is used in mobile devices. Bluetooth 4.2 brought a new low power option that allows wireless objects to operate for long periods of time, even on the smallest of batteries. This enables all sorts of useful devices to be incorporated into the Internet of Things, from showerheads to ovens to countertops. These kinds of connections are part of the work being done to create greater connectivity between everyday objects, and the already heavily-used Bluetooth protocol will surely be a part of that movement.

3. New Generation (NG) Wireless Token

Background

Century Longmai developed mToken BLE ecosystem portfolio of products strongly backed by deep security and cryptography research and development, to provide reliable, versatile and standard compliant solution – the product's framework adopts an abstraction of Bluetooth wireless communication and supports a broad range of international digital security algorithms. The ecosystem consists of wireless bio-communication (supporting Bluetoothand USB) smartcard chip based tokens specifically designed to meet users' growing mobility and privacy demands.
It works with cross-platform operating systems, multi-vendor mobile terminals and custom designed client software to provide secure connection to network based resources such as during online transactions, message transmission or when accessing

any public key infrastructure (PKI) applications for example Email, VPN, E-documents, etc.

Typical usage includes:

- Network logon
- Computer access control
- Data protection
- Logical Access control (LAC)
- Trusted document exchange
- Secure Internet and remote access
- e-Commerce and online banking

Structural Design

- Features a peripheral Micro USB interface and in-built Bluetooth module and antenna for short-distance wireless communication support.
- The Secure element (SE) and Bluetooth modules are physically separated to avoid any leakage of sensitive data.
- Featuresbuilt in battery management module to control device's working time and connection overBluetooth. The device turns off automatically after 60 seconds * without user interaction.

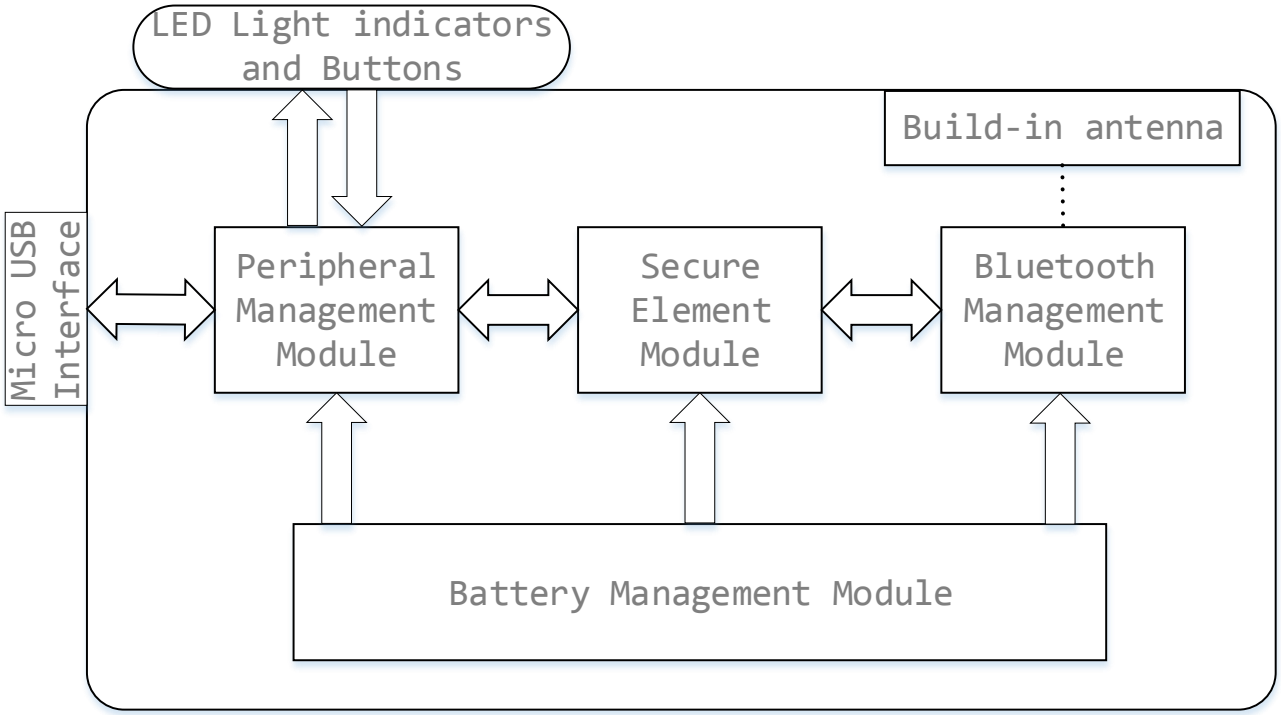


Fig 3-1: Structure design of mToken BLE-B1 device

Model Appearance

Century Longmai offers 4 standard and customizable mToken BLE ecosystem models as listed below:

mToken BLE-B1

- Single button Bluetooth Token
- Support for Bluetooth communication
- Supports for USB connection

mToken BLE-B4

- 4 buttons LCD display
- Support for Bluetooth communication
- Supports for USB connection

mToken BLE-B16

- 16 buttons
- Features LCD display
- Support for Bluetooth communication
- Supports for USB connection

mToken BLE-B56

- Full keyboard Bluetooth token Secure Payment terminal
- Support for Bluetooth communication
- Supports for USB connection
- Features standard LCD or a customized OLED display.

For customized product models, please contact us.

Strong Two factor authentication (2FA)

mToken BLE ecosystem product portfolio offers the highest level of security for two factor authentication (2FA): the token itself and a PIN, providing an extra level of security for the most sensitive applications. E-Government and E-Banking enablers or retailers can choose from a wide range of wireless form factors including mToken BLE-B1, mToken BLE-B4, and mToken BLE-B56.

Scalable portfolio of authentication devices

mToken BLE ecosystem can secure logical access control services hosted on any system through the USB connection or by Bluetooth communication. There is guaranteed and proven support for all major mobile operating systems and desktop operating systems including Windows, Mac and Linux.

New Smart card based Security

Adopting 32-bit smartcard chip technology can connect to PC terminals via High speed USB interface, ensure transmission security and fully protect application data and with onboard security algorithms.

Exchange & Storage of Sensitive Data

The mToken BLE ecosystem secures by cryptography stored and exchanged data cryptographic keys are secured through both physical and logical security measures.

Communication security

- Uses Bi-directional authentication between the host and token device
- Uses Encrypted USB and Bluetooth communication protocols.

PIN code security

- Two-level user rights (administrator and users)
- Users must logon with PIN when communicating with token wirelessly. This is an advanced security protection enabled by two factor authentication: something users have – the device, and something they know – their PIN. The PIN ensures the holder of the device is its legitimate owner.

- Password verification and editing operations can be performed through in-build keyboard

Transaction security

- Internal signature based on RSA algorithm, onboard secret keys
- Trade double check, exchange information show on LCD display, users need to type PIN code to make verification, and press button to confirm
- All exchange information is analyzed inside the key to prevent information leakage and data falsification.

Device Address

The mToken products' device address is uniquely assigned and is used when setting up pairing connections with other Bluetooth devices.

Get more technical information on Bluetooth technology including core specifications, FAQs and Quick Reference Guides. Links to tools and information:

- Quick Reference Guide
- Download the Core Specification

Portability & Usability

The mToken BLE ecosystem of products are especially convenient in situations that require secureauthentication and when smart card readers are not available.Features built in Lithium ion battery for long time usage support without need to charge by USB connection.

Mobility Convenience& Compatibility

Highly scalable

Leverages existing infrastructure and supports both mobile operating systems and major desktop operating systems including Windows, Linux, and OS X. Also devices in this series can be customized with acustomer's logo and other branding requirements.

Mobile terminals and OS supported

- iOS Terminals running iOS 6.0 and above
- Android Terminals supporting Android 4.3 and Bluetooth 4.0

- All Windows 8+ and Windows Phone devices supporting for Bluetooth communication

mToken BLE ecosystem products are fully compatible with Apple products and Android mobile terminals.

- **Desktop OS:** supports for Windows, Linux, and Mac OS X. Users could use USB interface with CSP, PKCS11 middleware and corresponding tools to operate and manage the token device.
- **Bluetooth communication:** We offer different model versions to support for latest Bluetooth Low energy and earlier Bluetooth core versions.

The Bluetooth Low energy model version are recommended since they are backward compatible and fully compatible with both Android and IOS devices.

Multiple applications Security & Flexibility

The mToken BLE ecosystem products are designed for secure storage of cryptographic keys and certificates, strong authentication, encryption, and digital signature of email and data while supporting non- repudiation, a crucial feature for proof of financial transactions. They also offer extended flexibility while securing a broad range of applications when provisioned with custom Middleware. Meanwhile, the custom Middleware integrates Century Longmai's smart card cryptography with Public Key Infrastructure (PKI) services to realize high level access control and network security.

Card Operating System Features

Century Longmai self-designed Card Operating System (COS) with proprietary IP:

- Designed according to FIPS 140-2 standards.
- Meet ISO7816-4 communication standards featuring secure messaging to ensure confidentiality between token device and application
- Supports for storage of X.509 v3 digital certificates and PKCS12 certificate importing
- Onboard RSA 2048 key pair generation, signature and encryption
- Supports DES, 3DES, AES128/192/256, SHA1/SHA256/SHA384/SHA512, RSA(1024/2048)

- Supports multi-applications, multi-containers and storage of multiple certificates on one device.
- Supports custom and standard Middleware such as MS CAPI, PKCS11.

4. mToken BLE-B1 Overview

Overview

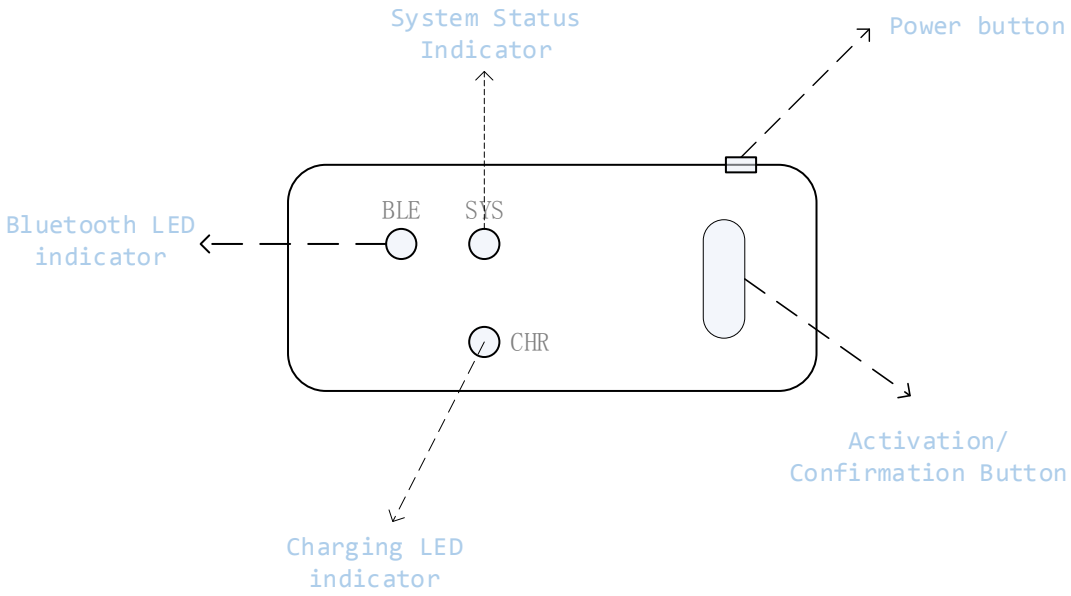
The mToken BLE-B1 offers all the power of a multi-applicationsmart card token in a USB form factor with additional capabilities of Wireless PKI, making it anideal solution for organizations that require a combination of security, portability, robustness and convenience for their end-users.
mToken BLE-B1 is single button USB and Bluetooth powered PKI solution, easy-to-carry and operate, can be applied in multiple enterprise mobile systems. It supports for USB connection and Bluetooth communication:-

- USB communication model is designed to work exclusively with desktop terminals
- Bluetooth communication model is specifically designed to securedata and data transmission on mobile terminals.

In addition to support for PKCS11, CSP, X.509 digital certificates, the mToken BLE-B1 supports international algorithms such as DES, 3DES, AES, RSA and SHA1/256/512and is able to meet multiple PKI application requirements.

Design

The mToken BLE-B1 features a dramatic innovative and seamless design. The mToken BLE-B1Panel features the following components:



- **Power Button -** Though the device features an auto power-off mode, users are highly recommended to turn off the device manually when not in use.
- **Activate/Confirm Button -** This button is multi-function button:
  - When the system or token is in inactive state, pressing this button re-activates the system or token;
  - After powering on the token, user needs to press hold this button for at least one second for token to transitinto working state.
- **LED Indicator lamps -** includes 3 LED light indicators to differentiate device and system status.

Operation

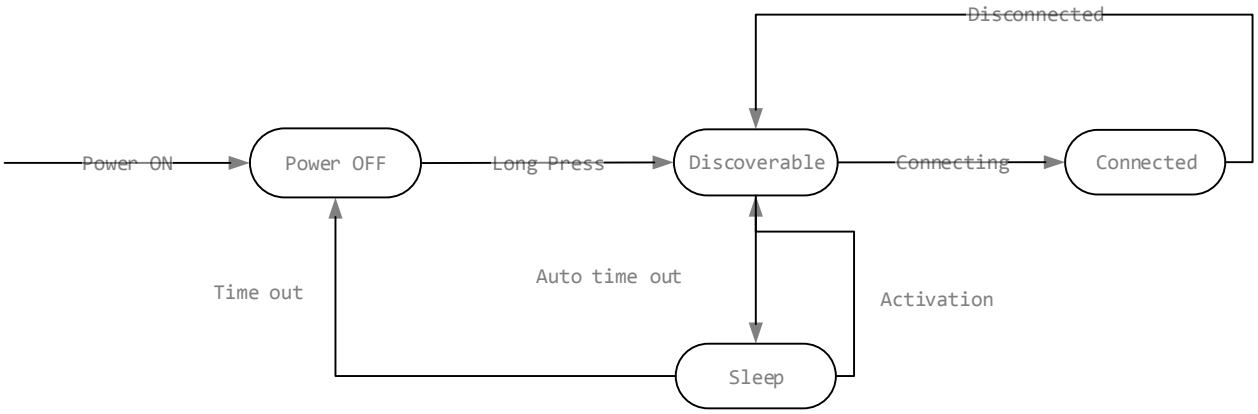


Fig 4-1 mToken BLE-B1 workflow

Power On

- Power on the device with Power button.
- Press and hold the Activation button for at least 1 second, the Green and Blue LED indicator will light at the same time. At this stage, the token is in standby mode -waiting for connections.

Initial Connection and Pairing

A flashing Blue LED light indicates standby mode, and it turn to steady Blue after connection.

System Status

If no operation with the token for 60 seconds, the token system goes in sleep mode. At this time, the BLUE LED light is turned off, and the GREEN LED light keeps flashing slowly.

Press the Activation button to re-activate the device.

Power off & Auto Power Off

The mToken BLE-B1 supports power save mode i.e. the token system will automatically turn off after 60 seconds of inactivity. User must press hold the activation button to turn on the Bluetooth token after the device is automatically or manually turned off.

User is suggested to turn off the device manually if not in usage for a long time.

Charging

Users can charge the token via USB interface connection. The Red LED indicator lights during charging, and is turned off when the device is fully charged.

The entire charging takes about 1hour, and the token can be used during its charging.

Important Notes

- All mToken BLE ecosystem products support for both USB and Bluetooth wireless communication:
- The USB interface is designed to connect with PC terminals
- Bluetooth communication is designed specifically forconnection with mobile terminals
- Using two models at the same time is NOT recommended
- The effective operation range of mToken BLE ecosystem devices is 2 meters *
- * Data based on internal testing. Actual performance may vary

5. Appendix A: Glossary

- **2FA** Two factor authentication
- **BLE** Bluetooth Low Energy
- **Chip:** An electronic component that performs logic, processing, and/or memory functions.
- **Connectable**: A Bluetooth enabled device in range that will respond to another device and set up a connection.
- **Connected**: A Bluetooth enabled device is within range and communicating over the Bluetooth wireless link. The Bluetooth preference pane shows a green dot indicating a successful connection.
- **Device discovery**: A process that allows one device to detect another device.
- **Discoverable**: When a Bluetooth enabled device is “discoverable,” other Bluetooth devices can detect, pair, or connect to it. Century Longmai wireless token will flash its indicator light when it is in discovery mode and will turn off discovery mode after approximately one minutes* to save battery life.
- **HCE** Host Card Emulation
- **IC** Integrated circuit.
- **ISM**Industrial, Scientific, and Medical
- **Issuer:** The bank that provides a credit card to a cardholder.
- **Key:** In encryption and digital signatures, a value used in combination with a cryptographic algorithm to encrypt or decrypt data.
- **Mobile contactless payments:** A payment to a physical merchant that is initiated from an NFC-enabled mobile phone held in close proximity (within a few centimeters) of the merchant's POS equipment.
- **Mobile proximity payments:** Mobile payment transaction in which a consumer uses a phone to pay for goods or services at a physical POS.

- **Name discovery**: The mechanism that requests and receives a device name.
- **NFC** Near Field Communication
- **Pairing**: The process of creating a persistent link between two Bluetooth devices, which may involve the exchange of a passkey between two devices. *This may only occur once; future connections between the devices are authenticated automatically.
- **Passkey**: The authentication key used to establish a link between devices. A passkey is similar to a password, but the passkey is only used once: you enter the passkey once and won't need to remember it.
- **POS Point-of-sale:** The merchant's physical location where the payment transaction takes place. This term is also used to describe the equipment used by the merchant to complete the payment transaction.
- **Profile**: A Bluetooth service that may be provided or used by a Bluetooth device. Such services can include file exchange, stereo audio, and tethering.
- **SE Secure element:** The component in a mobile phone that provides security and confidentiality.
- **Smart card:** A device that includes an embedded secure integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a secure memory chip alone.
- **SMS** Short Message Service
- **Tethering**: The use of an Internet enabled smart phone linked via Bluetooth to a computer to provide Internet services to the computer.

Sources: http://www.pcmag.com/encyclopedia_term/
http://lm-infosec.com/techno/glossary-terms/

6. Appendix B: Document Revision History

The table below describes the changes to the BLE in Mobile Payments White Paper.

Document Name	Revision and Date	Status	Notes	Status
	Version 1.0, 2015-02-29	Final	Release R1 Initial Release	

7. About Century Longmai

Established in 2003, Century Longmai Technology Co., Ltd is one of the most leading digital security device vendors in China with extended experience in developing latest generation of digital security solutions and products for secure information access and transmission. Our product portfolios include USB PKI token, wireless PKI tokens, OTP tokens, smartcard, JAVA cards, software license dongles, Smartcard readers, Electronic document protection (DLP) solutions and OEM services. Proved to be secure and convenient, our solutions and products are dedicated to help customers build safe, efficient and sustainable networks, financial systems and enjoy secure access to data and information everywhere whenever they want; you can work with us to benefit from deployment of standard technology solutions and our industry experience:

- We have over 12 years' experience in digital security industry
- We offer a wide range of technologies in the Information security industry
- We have Bluetooth Low energy products that realize true wireless PKI.

We guide our customers through the various stages of information privacy and security deployments and support them further with a range of customizable products and services. We really do much more than you can imagine! GET STARTED

Have a question or Need more info?

To learn more on how the unique features of mToken BLE ecosystem offers strong security, differential access to data and definitive auditing in multiple industries, please request for access for **mToken BLE ecosystem Technical Paper** or contact our sales directly.

Contact Details

Century Longmai Technology Co., Ltd
3/F, GongKong Building, No.1, WangZhuang Road, Haidian District, Beijing, P.R.China
Postcode: 100083
Tel: (86) 10-62323636 | Fax: (86) 10-62313636
Sales E-mail: info@longmai.net Support E-mail: support@longmai.net
Website: http://lm-infosec.com/