Mobile & NFC Council
WHITE PAPER
Smart Card Alliance

Bluetooth Low Energy (BLE) 101: A Technology Primer with Example Use Cases

A Smart Card Alliance Mobile and NFC Council White Paper

Publication Date: June 2014

Publication Number: MNFCC-14001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

Table of Contents

1 Introduction

The evolution of mobile applications and mobile payments industries has been accompanied by the continual introduction of new technologies. Currently, two mobile technologies are attracting attention: host card emulation (HCE) with Near Field Communication (NFC) and Bluetooth® low energy (BLE). With high expectations for mobile payments and major investments in mobile wallet platforms and NFC enablement, these two technologies have raised questions about business models, product development plans, and the pace of deployment.

This white paper defines BLE, including the key features that can benefit businesses and consumers, and the BLE ecosystem. The paper explores the origins of BLE's development, the BLE design principles, and the applications to which it can respond. BLE is discussed in the context of merchant, venue, and transportation-oriented applications. Example use cases illustrate category-specific issues and are included to stimulate thought on how to overcome constraints and explore new applications.

BLE is compared with similar technologies, such as WiFi, GPS, NFC, and QR codes; the comparison identifies BLE's advantages and disadvantages and discusses how technologies may complement each other to enrich the application experience. Lastly, the paper discusses security as it relates to BLE's use for payments, mobile marketing, and mobile commerce.

This white paper is intended to inform the reader, clarify misconceptions, and illustrate the synergies between technologies, encouraging integrated solutions that bring about the greatest possible consumer value propositions.

2 Overview of BLE

Bluetooth low energy (BLE) is a wireless computer network technology designed and marketed as Bluetooth Smart by the not-for-profit non-stock corporation Bluetooth Special Interest Group (SIG). While originally intended for use in the healthcare, fitness, security, and home entertainment industries, BLE shows promise for geolocation and other functions in stadium, retail, restaurant, transit and other applications. In comparison with "classic" Bluetooth, BLE requires considerably less power and incurs lower costs while providing a similar or larger communication range.

Key features of BLE include:

- Three power consumption modes: ultra-low peak, average, and idle
- The ability to run for long periods with standard or coin-cell batteries
- Multi-vendor interoperability
- Enhanced range (vs. classic Bluetooth)
- A frequency-hopping capability that detects other devices in the spectrum and avoids the frequencies they are using
- A hands-free customer experience

BLE is a subset of Bluetooth 4.0; support is available on most major platforms as of the versions listed below:

- iOS5+ (iOS7+ preferred)
- Android 4.3+ (numerous bug fixes in 4.4+)
- Apple OS X 10.6+
- Windows 8 (XP, Vista and 7 only support Bluetooth 2.1)
- GNU/Linux Vanilla BlueZ 4.93+

Figure 1 illustrates multiple industry uses of BLE at the sensor, host, and cloud services levels.

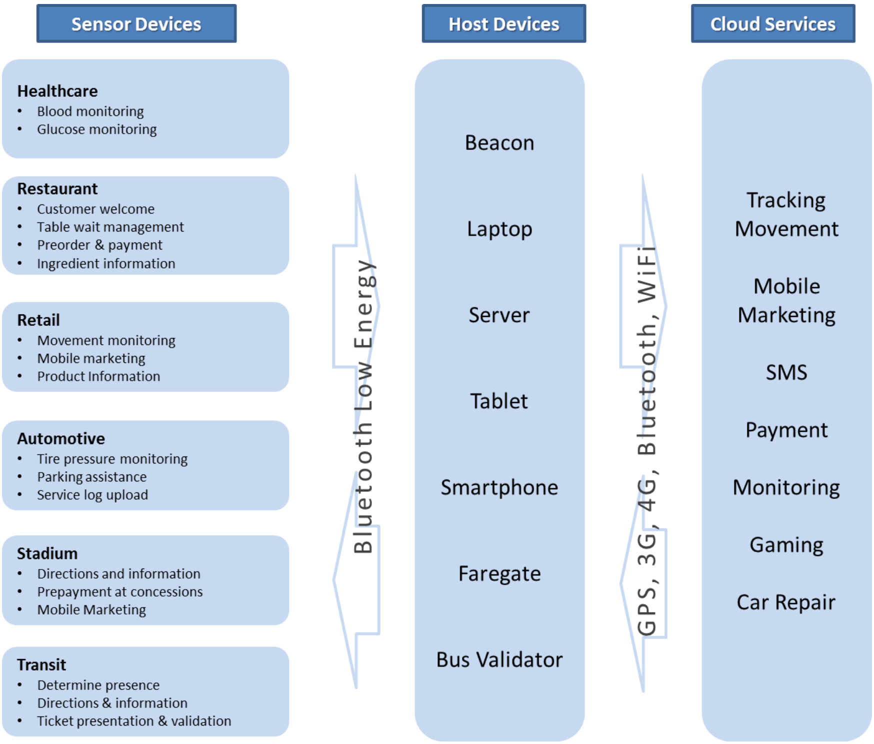


Figure 1. Use of BLE in Different Industries by Sensors, Hosts, and Cloud Services

2.1 Requirements for BLE-Enabled Applications and Solutions

It is important to understand the commercial language distinctions when looking at deployment of BLE solutions. The use of BLE requires devices that are Bluetooth 4.0 enabled. Products that use BLE technology include accessories for smartphones, health devices, watches, and proximity beacons, which can communicate with and transmit data (such as a welcome message, offers or coupons) to BLE-enabled devices such as smartphones and tablets. Most new smartphones in the last year are BLE-enabled.

In the predominant use of BLE beacons today, the primary roles are played by the merchant to consumer. A consumer entering a merchant's premises with a BLE-enabled smartphone opens a variety of new opportunities for engagement. The merchant can engage the consumer through the deployment of beacons, which are battery operated, or plug-in BLE-enabled devices that are form, fit and function designed to promote or create interactivity between the merchant or brands and the consumer. (For more information on beacons see Section 2.4.1). Additionally, the merchant could choose to upgrade their point-of-sale (POS) infrastructure to support BLE in which case the connections between the POS terminal and consumer smartphone could be used for multiple functions from coupons to loyalty to payments.

2.1.1 Provisioning BLE Applications

To provision a BLE application, a consumer's BLE-enabled smartphone or tablet requires an app that enables the mobile device to interact with a proximity beacon using BLE at a location such as a merchant, restaurant, stadium, airport, or transit station. When the beacon triggers the phone or tablet, the beacon relays a message from the server to the consumer's mobile device (see example in Figure 2). The exchange is initiated by the beacon; the mobile device collects content from the cloud that is appropriate for the beacon that initiated the exchange. Any messages that can be sent to a BLE-enabled device are stored in the cloud and can be changed in real time.

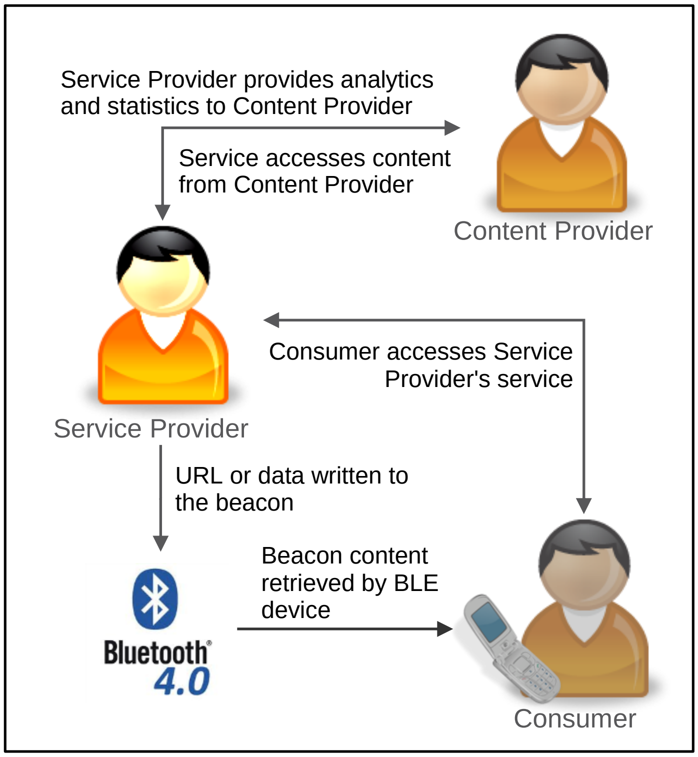

Service Provider provides analytics and statistics to Content Provider
Service accesses content from Content Provider
Content Provider
Consumer accesses Service Provider's service
Service Provider
URL or data written to the beacon
Beacon content retrieved by BLE device
Bluetooth 4.0
Consumer

Figure 2. Example BLE Deployment Delivering Content to BLE Devices

A BLE-ready smartphone or tablet can detect a BLE device (such as a proximity beacon) without the need to pair. This capability enables passive discovery, spontaneous interaction, and new methods of customer engagement for retailers and brands.[1]

2.1.2 Provisioning Processes

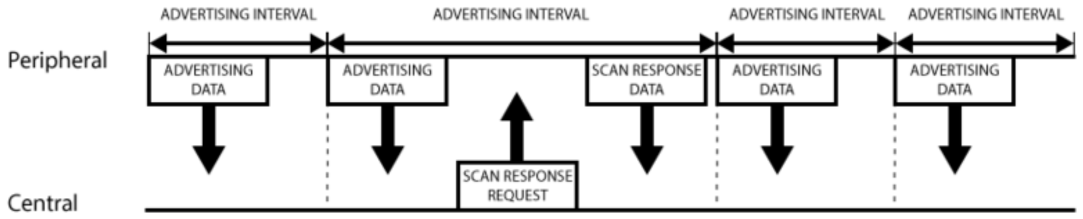
The BLE communications process relies on two profiles: the generic access profile (GAP) and the generic attribute profile (GATT). The GAP controls connections and advertising. (Advertising in this context does not refer to an offer or coupon but identifies a step in the process of establishing a dedicated connection between two BLE devices.) The GATT defines how two BLE devices exchange data.

2.1.2.1 GAP: Significance and Transactions

The GAP enables a smartphone or tablet to be visible to the outside world and defines how two devices, such as a smartphone and a beacon, can interrelate.

The GAP contains a list of central devices and definitions of those peripheral devices with which it can communicate. Central devices are typically tablets or smartphones. Peripheral devices are low-power small devices that can connect to a much more powerful central device. Peripheral devices include items such as a beacon, a heart rate monitor, a BLE-enabled proximity tag, or a watch.

Peripheral devices, such as a beacon, can broadcast a data packet at set intervals. If a listening device, such as a laptop or smartphone, is open to communicating with the beacon, it can request and receive the message. Figure 3 illustrates this process.



Source: adafruit. https://learn.adafruit.com/introduction-to-bluetooth-low-energy/gap

Figure 3. Central and Peripheral Device Communication

2.1.2.2 GATT: Significance and Transactions

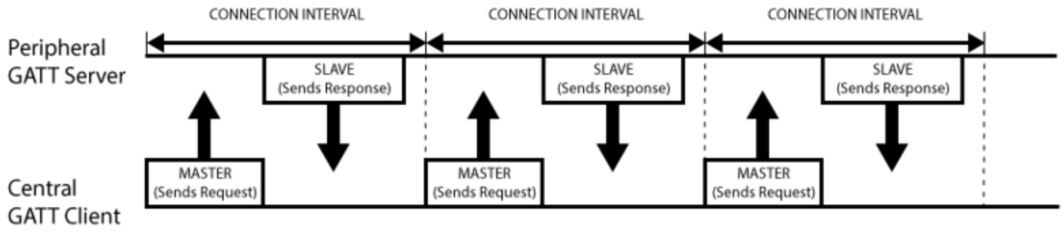
Once a dedicated connection is established between two devices, the GATT takes over. Originally, GATT connections were exclusive. A BLE peripheral could only be connected to one central device at a time. As soon as a peripheral device attached to a central device, it stopped advertising, and other devices were not able to see it or connect to it. However, some newer Bluetooth devices support multipoint connections. For example, an LG HBS-730 headphone can be connected to an iPhone and an iPad simultaneously. With multipoint connections, it will be important to understand how many devices are expected to connect in order to ensure capacity.

GATT relies on a client-server relationship. The GATT client, which is the central device, sends requests to the GATT server, a peripheral device. The GATT client initiates all transactions; the GATT server is the slave device. The GATT server contains the attribute protocol (ATT) that

[1] Merchants and businesses interested in propagating BLE should develop applications that leverage BLE and deploy them to the appropriate store, such as Google Play or the Apple Store. Developers should reference the BLE specifications at https://developer.bluetooth.org/TechnologyOverview/Pages/BLE.aspx.

contains the services offered by BLE. These services include lookup data as well as service definitions and characteristic definitions.

Figure 4 illustrates the client-server data exchange process.



Source: adafruit. https://learn.adafruit.com/assets/13827

Figure 4. Data Exchange between the GATT Server and Client

GATT transactions are based on high-level nested objects: profiles, services, and characteristics. A profile is a collection of services that has been defined by either the Bluetooth SIG or by the peripheral designers. Each service is distinguished from other services by a unique numeric ID. The services break data up into logical parts and contain specific data parts (characteristics). An individual service can have one or more characteristics. Each characteristic includes a single data point only. Characteristics are what client developers need to communicate a client request with a BLE peripheral; characteristics are also used to send data back to the BLE peripheral.

2.2 Key Technical Data

The key technical data for BLE are as follows:

- Range: ~50m but capable of ~150 m in open field.
- Output power: ~ 10mW (10dBm).
- Max current: ~ 15mA.
- Latency: 3 ms.
- Topology: Star. A star network consists of one central switch, hub, or computer that acts as a conduit to transmit messages.
- Connections: The number of connections can be very large; depending on the implementation and available memory.
- Modulation: GFSK at 2.4 GHz.
- Robustness: Adaptive frequency hopping, 24 bit CRC.
- Security: 128bit AES CCM.
- Sleep current ~ 1µA.
- Modes: broadcast, connection, event data models with reads and writes.

BLE devices consume very little power and can last at least six months on a single coin-cell battery.

2.3 Bluetooth Core Specification

Unlike other wireless standards, the *Bluetooth Core Specification*[2] provides product developers with both link-layer and application-layer definitions that support data and voice applications.

[2] Bluetooth SIG. http://www.bluetooth.com/Pages/Basics.aspx.

2.3.1 Spectrum

Bluetooth technology operates in the unlicensed industrial, scientific, and medical (ISM) band at 2.4–2.485 GHz, using a spread-spectrum frequency-hopping full-duplex signal at a nominal rate of 1600 hops per second (1Mbps). The 2.4 GHz ISM band is available and unlicensed in most countries.

2.3.2 Interference

Bluetooth technology uses adaptive frequency hopping (AFH) among available frequencies at 1 MHz intervals to reduce interference between wireless technologies sharing the 2.4 GHz spectrum. AFH works within the spectrum to take advantage of available frequencies, detecting other devices in the spectrum and avoiding the frequencies they are using. AFH provides a high degree of interference immunity and also allows for more efficient transmission within the spectrum. For users of Bluetooth technology, AFH enhances performance even when other technologies are being used at the same time.

2.3.3 Range

BLE range is application specific. Although a minimum range is mandated by the *Core Specification*, there is no limit. Manufacturers can tune an implementation to support a specific use case. With Bluetooth v4.0, manufacturers may choose to optimize range to 100 m, particularly for in-home sensor applications where longer range is a necessity.

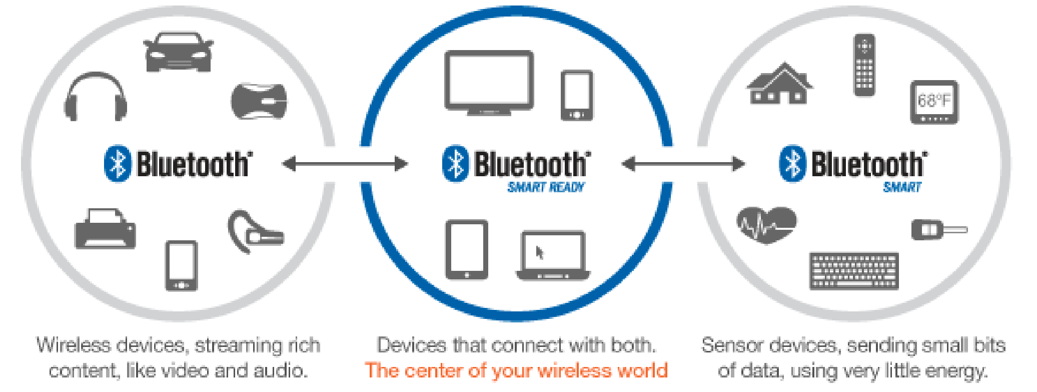
2.3.4 Device Compatibility

BLE was first introduced in June 2010 as part of the Bluetooth 4.0 specification. The specification allows Bluetooth communication protocols to be implemented in two different modes:

- Single mode implementation, which enables BLE use.
- Dual mode implementation, which supports legacy implementation (or classic Bluetooth) as well as single mode implementation. Devices that support dual mode implementation can function as a BLE device.

The guidelines provided by the Bluetooth SIG permit devices that implement the Bluetooth specifications to be differentiated with special marks. Devices that support only BLE can carry the Bluetooth Smart mark, whereas devices that support the dual mode implementation can carry the Bluetooth Smart Ready mark. Devices based on the earlier versions of the Bluetooth specification continue to carry the Bluetooth mark.

Figure 5 provides an overview of the compatibility of devices using Bluetooth technology.


Bluetooth
Bluetooth SMART READY
Bluetooth SMART
68°F
Wireless devices, streaming rich content, like video and audio.
Devices that connect with both. The center of your wireless world
Sensor devices, sending small bits of data, using very little energy.

Source: www.bluetooth.com.

Figure 5. Compatibility between Different Bluetooth Devices

Each BLE device is associated with a Bluetooth profile that is specific to that device's particular function, such as heart monitor, proximity locator, or temperature meter. The Bluetooth profile also defines the interaction between compatible Bluetooth devices.

For example, Apple's iBeacon transmitter is an implementation of BLE and advertises information defined by the profile associated with that iBeacon. The information can be received and processed by an app in a Smart Ready device, such as a smartphone running iOS 7.0. Because they implement BLE specifically, iBeacon devices are Bluetooth Smart and not Bluetooth Smart Ready, meaning that they can only communicate with Smart and Smart Ready devices, such as an iPhone running iOS 7.0, but not with older devices that implement classic Bluetooth. It is important to note that a BLE Smart Ready device is also capable of sending information similar to BLE Smart devices.

Note, too, that even though the Bluetooth 4.0 specification is backward compatible with previous versions of the technologies, the BLE single mode implementation is not.

2.4 Comparative Technologies

BLE is similar to ZigBee and Z-Wave and has been compared to NFC, although NFC has limited range. These technologies are all relatively low-data-rate technologies intended for control and telemetry applications. BLE is distinguished by throughput rate (200 Kbps), range (greater than 10 m), security and integrity features such as very low connection set-up times, and excellent power-consumption characteristics.

Table 1 compares BLE with Bluetooth Classic, geolocation, QR code, NFC, and WiFi.

Table 1. Comparison of BLE with Similar Technologies

	BLE	**BLE Beacon**	**Bluetooth Classic**	**Geolocation**	**QR Code**	**NFC**	**WiFi**
Underlying technology or standard and frequency	Bluetooth 4.0 2.4 to 2.485 GHz	Bluetooth 4.0 2.4 to 2.485 GHz	Bluetooth 4.0/4.1 2.4 to 2.485 GHz	Global Position / Geodesy via satellites	ISO/IEC 18004:2006 2D matrix code or bar code	ISO/IEC 14443 ISO/IEC 18092 13.56 MHz	Near Field 2.4 GHz/ 5GHz Microwave
Range	~50 to 150 m	~1 cm to 150 m	~10-100 m (based on radio class)	Outdoor satellite range	~10 cm	<10 cm	~650 m
Network requirement during transactions	NA	Need data channel to redeem content	NA	No	Needed for dynamic data population	No. Needed during provisioning of credentials [3]	No
Connection speed (sec)	~0.03	~0.03	~1	NA	NA	~0.1	~0.03
Use/payload/ transfer rate	Data transfer ~300 kbps	Data transfer ~300 kbps	Data transfer up to ~25 Mbps in 4.0	Location identification/ coordinates	Data transfer rate based on scanner Numeric chars 7089 in QR code version 40	Data transfer, contactless payment credentials ~424 kbps	Data transfer up to 250 Mbps

[3] If an application uses an architecture where credentials are stored in an MNO-controlled asset (e.g., the UICC or secure element).

	BLE	BLE Beacon	Bluetooth Classic	Geolocation	QR Code	NFC	WiFi
Use cases	Location ID, hands-free payment, promotions, offers	Consumer recognition and promotion, localization in store	Pairing with PDAs, printers, PC accessories, headsets, smart devices	Device ID, location monitoring and tracking	Tracking, ID, payments, marketing, Web site login	Contactless payment, access, transit, ID, coupons	Data transfer, payment, network access

2.4.1 Bluetooth Beacons and GPS

One of the uses of geolocation technology is to identify when a smartphone is in proximity to a business, so that the business can make offers for services or enable services (such as an automated fuel dispenser at a gasoline station). The smartphone identifies its location by means of an embedded GPS chip. This chip and the smartphone use satellite or mobile cell tower signals to identify the phone's location. However, geolocation was built for use outdoors. Location accuracy can suffer when geolocation is used in closed areas such as malls and subways, unless tracking devices are installed.

Both GPS and the Bluetooth beacon can determine the location of a person indoors, such as in a mall, office building, or airport, or on Main Street. However, there are some major differences between Bluetooth and GPS.[4]

GPS requires a lot of battery power and is often turned off by the smartphone owner. BLE consumes little power and can be on whenever the consumer's smartphone is on. Unlike GPS, Bluetooth also has a sleep mode to save energy.

GPS is a satellite-based localization method and is typically not accurate indoors. GPS is affected by microwave appliances, and the GPS signal can be reflected off roofs, walls, and other impediments. Moreover, when a mobile network is congested (such as in a stadium or mall during a holiday period), it may be difficult or impossible to coordinate direction.

BLE, on the other hand, can be used to track movement indoors. A Bluetooth beacon uses radio frequencies to deliver a Bluetooth data package at specific intervals to BLE-enabled smartphones that are within range of the beacon. The data from a Bluetooth beacon describing where someone with a BLE-enabled smartphone is very accurate. Beacons can be directed to a specific location or distance, up to a maximum range of about 100 m.

Combining geolocation with BLE for mobile payments can be a fraud reduction tool that both tracks the customer's location and streamlines the payment process.

2.4.2 BLE and NFC

Near field communication (NFC) is a technology used for short range data transfers over distances of less than 4 cm and is compliant with ISO/IEC 14443. NFC-enabled smartphones support three modes of data transfer: card emulation, peer-to-peer, and reader/writer. When used for proximity payments in card emulation mode, NFC transfers payment credentials to existing contactless POS terminals.

NFC card emulation supports two methods for securing payment credentials:

- Credentials are stored in the physical secure element on the device.
- Credentials are stored securely in the cloud and used with host card emulation (HCE).

BLE and NFC can both complement and compete with one another. BLE can complement NFC, providing offers and advertisements when a consumer enters a store, while NFC can be used for

[4] http://bluetoothbeacons.com/.

payment. When NFC with a secure element is used for payment, the transaction uses standard payments application security, including dynamic cryptograms and security codes that leverage the current contactless payment infrastructure.[5] EMVCo has published a tokenization standard for mobile transactions that could be used with any technology to provide security for payment account information.[6] It important to note, however, that tokenization is only one component of a security infrastructure.

BLE can supply value-added services such as offers and discounts to NFC-based phones. However, use of BLE requires a new infrastructure to target users with smartphones who subscribe with BLE.

User permission for NFC interaction is also expressly given once the user chooses to tap an NFC tag with an NFC-enabled smartphone. The NFC tag does not require any power as it is derived from the phone. As such, an NFC tag can live in an environment indefinitely while a BLE solution will either need to be plugged in (and thus proximity limited to the range of BLE), or if battery-operated (such as a BLE beacon), replaced according to the battery duration.

2.4.3 BLE and WiFi

WiFi enables electronic devices to exchange data and connect to the Internet wirelessly, using microwave technology that conforms to IEEE Standard 802.11. Consumers must accept the WiFi connection, and WiFi often requires proper authentication to prevent unwanted use. Enabling a WiFi connection requires a configuration and security pass-code matching process. Connecting two devices over BLE is relatively simple, involving a key matching process.

There are additional differences between WiFi and BLE in the following areas:[7]

- Data transfer rates
- Maximum range
- Limitation on the number of connected devices
- Security

The latest specifications for Bluetooth 4.0 discuss data transfer rates of up to 25 mbps. The latest version of WiFi direct can achieve data transfer rates of up to 250 mbps. While 25 mbps is adequate for some transactions, it limits the use of BLE for transferring larger files and data elements such as jpg files, apps, and other files a merchant would load to a store system.

The specified range for BLE is approximately 50 m (and up to150 m in an open field); WiFi extends up to 650 m. The WiFi range depends on the version of the WiFi protocol used and whether antennas have been added to the communication system to extend the range of the WiFi network.

Bluetooth security is limited to key matching, which represents a major issue with BLE that could limit its use in transferring payment credentials, specifically primary account numbers. However, BLE does support full AES-128 encryption using CCM [8] to provide strong encryption and authentication of data packets. WiFi is secured by the Wired Equivalent Privacy (WEP) algorithm (less secure) and WiFi Protected Access (WPA).

[5] *The Mobile Payments and NFC Landscape: A U.S. Perspective*, Smart Card Alliance Payments Council white paper, September 2011, http://www.smartcardalliance.org/pages/publications-the-mobile-payments-and-nfc-landscape-a-us-perspective

[6] *New EMV framework to support NFC, QR, Bluetooth LE and more*, NFC World, March 6, 2014, http://www.nfcworld.com/2014/03/06/328218/new-emv-framework-support-nfc-qr-bluetooth-le/

[7] *Difference between Bluetooth and WiFi*, EngineersGarage, http://www.engineersgarage.com/contribution/difference-between-bluetooth-and-wifi

[8] CCM mode combines the counter mode of encryption with the CBC-MAC mode of authentication.

Because WiFi can work at longer distances with larger data transfer rates and includes high quality security protocols, WiFi consumes more power than BLE.

2.4.4 BLE and 1D Bar Codes, 2D Bar Codes or QR Codes

The 1D and 2D bar codes are machine-readable matrices or bar codes that have been used in product identification and are now being used in mobile payments and mobile marketing. The technology can transfer limited amounts of data in alphanumeric, numeric, or binary format. One example of successful bar code implementation is the Starbucks mobile app.

Compared to BLE, QR code technology is simple to implement at the merchant POS and in a mobile wallet application. QR codes can be more cost effective than BLE, and QR codes can be generated even when a mobile device does not have network access. However, the technology has limitations in scope, range, security, and consistency.

While QR codes and BLE-based solutions can be standalone implementations for mobile payments, QR codes can also be used to complement BLE as an authentication mechanism for consumers at checkout. In addition, QR codes can also be used in advertising, ticketing, checking in/out, and offer redemption.

Table 2 compares bar codes and BLE.

Table 2. Comparison of 1D and 2D Bar Codes and BLE

	1D and 2D Bar Codes	BLE
Range	1 to 1.5 cm.	~50m but capable of ~150 meters (in an open field).
Implementation cost	Requires a merchant to invest in scanners at each POS station. Scanners can cost from $100 to $400 per device.	Requires investment in and setting up an infrastructure. Typical beacon costs are between $5 to $50 but a larger retail area or stadium has multiple beacons.
Mobile marketing applications	Can relay a token and other information between buyer and POS system.	Allows the merchant to send offers and coupons to a consumer with a BLE-enabled phone upon entry into a store or location within a store.
Power consumption	Very low power consumption. Phone's camera must be activated.	Very low power consumption.
Consumer usability	Consumer must become accustomed to pointing the phone to a scanner, which can cause queuing issues.	No consumer interaction necessary.

3 Example BLE Use Cases

BLE's proximity detection capability offers multiple advantages:

- Improved operational efficiency for targeted promotions and information, which reduces the cost of marketing and customer service.
- A more positive customer engagement. Customers and prospects who receive the right content in the right place at the right time are far more likely to act. Transit customers can receive correct information when and where they need it.
- The opportunity for managers to capture and analyze data on how customers behave and adjust digital content and the physical environment accordingly.
- The opportunity for creating innovative check-out and payment processes.

These advantages rely on knowing customers and customers' current locations. The use of proximity beacons is an important part of contextual awareness, especially indoors.

This section is not intended to provide an exhaustive list of use cases; instead it covers several applications that could take advantage of BLE features. Some of the use cases describe applications that have been implemented using BLE, while others are hypothetical, postulating how BLE may be used.

3.1 Parks and Stadiums Use Cases

Some professional and college sports teams are looking to technology to make the trip to the park or stadium a more enjoyable event and are turning to BLE for help. While GPS is reliable for routing a person to a destination, it is not good at navigating people indoors, especially in buildings made of concrete and steel. Instead, Major League Baseball, for one, is turning to BLE, for a variety of reasons.[9]

First, BLE enables parks and stadiums to create micro-locations throughout the facility where a consumer can enjoy different experiences. In addition, teams can automate processes to reduce confusion and streamline traffic. Approaching the stadium, consumers can use BLE to activate the appropriate app and display a ticket. The app can recognize a first-time user and provide a guide with information specific to the event, park, or stadium. After entering the gate, the app can display a map to show the ticketholder's seats, the restroom, and concession stands.

The use of BLE and mobile enables stadiums to offer their customers an individualized experience. These facilities can leverage BLE to track patron movement before, during, and after an event for traffic analysis and for the interest people have in exhibits or a particular part of the facility.

Many major league ballparks have also recognized the advantages that BLE has over WiFi. For example, Target Field's WiFi network could only accommodate about one-fourth of those in the stadium at one time. The system is being upgraded and should allow the majority of fans to log on to the ballpark's wireless network at the same time.[10] This is important because guests and fans are frequently on their smartphones or tablets to check baseball statistics, watch instant-replay videos, and share their experiences over social media.

Other services that BLE makes possible include:

[9] *iBeacons: Coming soon to a baseball stadium near you*, Jason O'Grady for The Apple Core, ZDNet, http://www.zdnet.com/ibeacons-coming-soon-to-a-baseball-stadium-near-you-7000021354/.

[10] *Target Fields iBeacon will reach out to Twins fans' iPhones*, TMCnet.com, April 5, 2014, http://technews.tmcnet.com/news/2014/04/05/7763174.htm

- Directions and parking information
- Checking for stadium or team offers and rewards
- Interactive concourse maps and directories
- Integration with social media
- Access to a team's season schedule, ticket ordering information, and promotional event listings
- Access to food and beverage ordering and payment for selected ticket holders
- A comprehensive guide to all services the facility offers
- Preordering and payment at concessions, to avoid lines
- Estimates of wait times at concessions and restrooms
- Customer relationship management
- Rich analytics based on entry time, exit time and dwell times
- Footprint heat mapping

3.2 Convention Center Use Case[11]

The San Diego Convention Center Corporation (SDCCC) has implemented BLE beacons for customer communications.

Combining in-convention center proximity content delivery with outdoor geo-specific and location-aware communications, the SDCCC application uses a context aware and proximity platform, which enables delivery of personalized, highly relevant communications to consumers on their mobile devices based on interests and context both inside and outside the conventions. The app launches when attendees arrive in San Diego, guides them to the convention, and enhances the convention experience by providing information throughout their stay.

The mobile marketing app communicates directly with the visitors, welcomes them to San Diego and provides valuable information to guide the visitors to their hotel via numerous local transportation options. Once the visitor or show attendee proceeds across the geo-fence into the area surrounding the convention space, an in-app notification is delivered and provides instant and precise information about the convention, the floor map of exhibitors, and conference schedules. Permanently placed beacons inside the convention building send in-app notifications (and can send push notifications when desired) to direct attendees in common areas to check-in and registration, conference rooms for break-out sessions and service locations.

Once in the convention, location beacons are placed in key exhibitor booths to direct attendees to important show exhibitors. Once at the micro location for a booth, the mobile app enables convention managers to verify who is in which booth and how long they are there and to deliver relevant and on-point content directly to the attendee's mobile device when they are in the booth. There is no need to manually check in or scan badges, eliminating a time-consuming procedure. Dwell time in the booth can be measured and trigger the delivery of content about the product. The augmented reality recognition system can bring to life thousands of posters within the hall and exhibit providing the right message to the right person at the right time and place. This new application provides value to the attendees and analytics and tools for the exhibitors, and empowers the show managers to enhance the overall convention experience.

Upon exiting the building, the app provides added value to the exhibitors, the show managers and the surrounding city. Conventioneers now become visitors and the app can direct the visitors to numerous local dinning and tourist attractions. Numerous San Diego restaurants, sports bars and hotels are powered by permanent beacons to attract visitors with desired information, content and value. As the visitor approaches each location, the app delivers notification of the venue and in-app coupons/offers may be delivered to assist in the selection of a specific destination. Posters, menus and artwork can come to life utilizing the augmented reality video content. The

[11] The SDCCC use case was contributed by Total Communicator Solutions, Inc., and Gimbal, Inc.

app then verifies presence and can verify the use of a coupon and the amount of time spent in the establishment. Real-time analytics provide valuable marketing content to visitors. All of the information is provided to the establishment and the show managers in real-time, delivering the right message, at the right time, to the right person, at the right place.

3.3 Retail Merchant and Restaurant Use Cases

Retail merchants and restaurants are exploring how they can best increase traffic to drive new revenue and build recurring business, asking questions such as:

- What are the demographics, interests, and habits of my customers and prospects?
- What are my customers looking at and where are they spending the most time in my facility?
- How can I tailor my offers and marketing programs to the specific interests of customers and prospects?
- How can I make sure that I engage my customers in the right place at the right time?
- How do I address consumer and industry concerns about privacy of information?

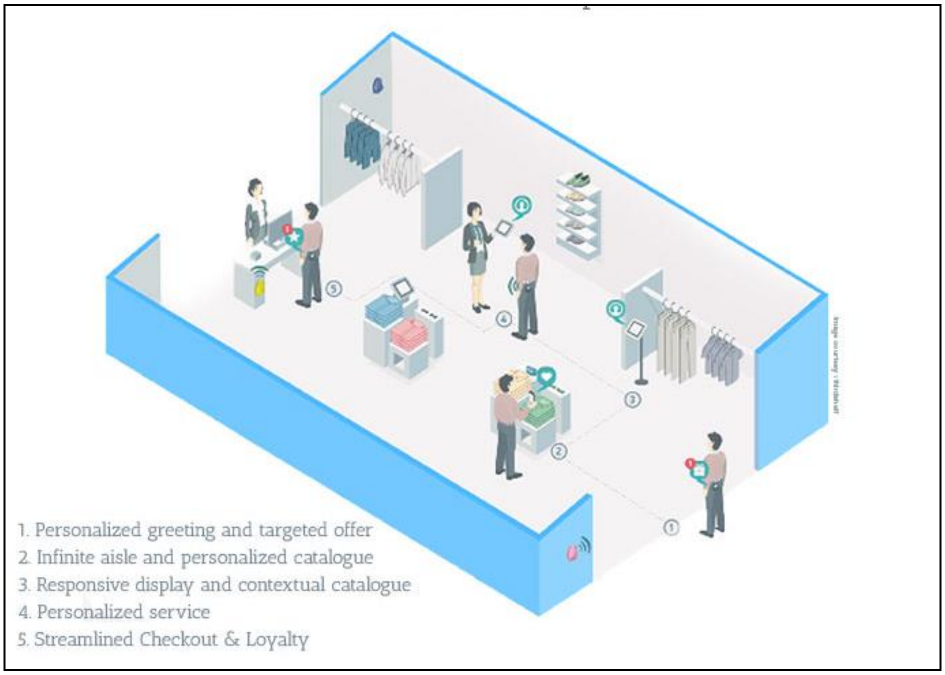
Using BLE to contact a consumer's phone when the consumer is close to a certain location can be useful for many types of businesses. BLE-enabled apps can react when a consumer approaches a business or a product or area within a business to offer a variety of business-specific opportunities.

3.3.1 Potential for BLE in Retail

BLE can be used by retailers to provide advertising, offers, coupons, product information, and other services when consumers approach a store's entrance, upon entry, or within particular areas in a store. BLE beacons can also help retailers track where consumers go (with or without consumer interaction), allowing the retailer to optimize merchandise placement.

For example, picture a consumer about to enter a department store. Before setting foot in the store, the consumer receives a coupon for items bought at that store in the past and advertisements for items the retailer believes the consumer may want to purchase, based on the consumer's purchasing history. Noting that the coupon is for something the consumer needs, the consumer heads to that department to purchase the item. On the way, the consumer passes the shoe section, at which point a coupon is sent to the consumer's phone advertising a current special; being in a hurry, however, the consumer keeps walking. On the way to checkout, the consumer sees a set of glassware that would be nice for a dinner party planned for the weekend and picks up the glassware for purchase. After checking out, the store uses BLE to thank the consumer and includes an offer to join the store's loyalty program.

Figure 6 illustrates this example.


1. Personalized greeting and targeted offer
2. Infinite aisle and personalized catalogue
3. Responsive display and contextual catalogue
4. Personalized service
5. Streamlined Checkout & Loyalty

Source: Cabot Technology Solutions. http://www.cabotsolutions.com/2014/03/ibeacon-geolocation-indoors-to-power-the-business-world/

Figure 6. A Mobile-Enabled Retail Experience

In this example, the merchant was able to use BLE to accomplish the following:

- Convert a coupon to a sale
- Expand the merchant's value in the eyes of the customer
- Offer a loyalty program that will increase customer visits and revenue from that consumer
- Evaluate where the customer went in the store and how long the consumer stayed in one place

Following are potential uses of BLE by retail:

- Offering a coupon or discount to generate traffic for a specialty retailer in a busy mall or on Main Street.
- Relaying product information to a consumer's phone to influence purchase decisions in a store, area of a mall, or public facility such as a sports stadium or museum.
- Alerting a retailer to the arrival of a VIP customer or member of the retailer's loyalty program for a personal greeting.
- Enabling remote payment away from the checkout location.
- Providing information about a customer's movement throughout a store, noting where the customer lingered and where the customer hurried. This information can help a retailer determine product placement, store layout, traffic flows, and highest performing times of day.
- Delivering demographically oriented digital signage, such as video displays focusing on products for men or women.
- Conveying real-time targeted messaging.

3.3.2 Potential for BLE in Restaurants

Like retailers, restaurants can benefit by using BLE. For example, suppose a couple with two young children decides to go out to dinner at a local restaurant. The wife notices that there is an app for the restaurant in the app store and downloads it. As the family is entering the parking lot, the app sends a welcome, asking them if they are having dinner and if so, how many are in their party. The wife responds and the family is placed on the wait list. As the family enters the restaurant, the app prompts to determine whether they would like to take part in the restaurant's "streamlined" ordering and payment service. Knowing that children have limits, they agree. In a few minutes, the app signals that their table is ready and that they are to proceed to the hostess station. As they are walking to the table, the app sends a description of that evening's specials. After placing their drink orders, the wife uses the app to request extra napkins. The waiter brings the napkins along with their drinks. While they are eating, a coupon for ice cream is sent to her phone, which she uses to order ice cream for the children. While the children are finishing their treat, the wife uses the app to request the check. When the waiter brings the check, she pays with her phone, using the app to add a generous tip, and inputs her e-mail address for the receipt.

Following are potential uses of BLE by restaurants:

- Generating traffic for a concession or restaurant located on a busy street by way of a coupon or discount offer.
- Ordering and prepaying for food at a restaurant's takeout area, an event's concession, or a quick service restaurant to speed up service, reduce queues, and reduce "walk aways."
- Sending a consumer dietary information about an entrée.
- Allowing a restaurant to provide demographically oriented digital signage, such as a video display focusing on the menu.
- Providing real-time targeted messaging.
- Alerting a restaurant to the arrival of a VIP customer or member of the restaurant's loyalty program for a personal greeting.
- Signaling that a customer's table is ready.

3.3.3 Additional Use Cases

Other event, retail, restaurant, and facility use cases include the following:

- Managing queues in a supermarket, business, or organization where a customer needs to take a ticket to get service, such as a deli, school function, local government, or hospital
- Managing tickets at events where the ticket pops up automatically when an attendee arrives at the entrance
- Asking people to switch off their phones when they enter certain areas in a hospital or arrive at the cinema
- Alerting people in a parking garage to pay before leaving
- Supporting "electronic leash" applications, where a system or high-value product sounds an alarm when it is out of beacon range

3.4 Transit Use Cases

BLE can enable a variety of new features for smartphone applications targeted at transit riders. Beacons can be placed within stations, at bus stops, or on the buses themselves. Fare terminals can support the BLE interface and expand messaging to users in areas with limited connectivity.

For subway passengers, beacons can be used to enable underground guidance capabilities to help passengers navigate between platforms and control areas. Beacons can also be used to trigger the display of a passenger's account data and prompt actions appropriate to an account or card.

Transit can also use BLE to drive promotional messaging across the array of digital screens represented by smartphones, kiosks, and fare terminals. BLE would also offer the ability to disseminate emergency information that is customized to location, maximizing impact and minimizing confusion. BLE peripherals can interact with passenger smartphones to deliver content based on time, location, and destination parameters.

Aboard buses, most operators run flat fare schemes, which capture entry data but rarely capture exit data. BLE used with a smartphone application can provide powerful origin–destination data for scheduling and service improvement programs. BLE can also enhance real-time passenger information applications, such as an app used to publish next-stop arrival times. Data can be presented without passenger intervention.

Boarding and alighting data can be used for account-based "be in-be out" processing strategies, in which valid account holders need only to board; their origin and destination data is then logged as a function of their presence on the vehicle. However, while emerging account-based fare solutions can support this approach, new enforcement strategies must be developed to ensure fare compliance. One possibility is a BLE link from the smartphone to the fare terminal that would identify a passenger to the driver, similar to the operation of a smart card tap. BLE could be used in a similar way at subway faregates to enable entry and exit processing.

The challenge for BLE fare terminal integration is the cost of the infrastructure upgrade and the time associated with transit budgeting, appropriations, and procurement processes. It is more likely that at least in the near future, BLE will simply complement NFC, which is compatible with most of the current transit fare infrastructure.

3.5 Payments Use Cases

The potential use of BLE for payment applications has generated considerable interest since a wide variety of mobile devices are expected to support BLE.

For payment at a physical merchant, the customer's payment account information must be stored securely, be easily available for use at the point-of-sale or during the payment process, and be communicated to the merchant to complete the transaction.

When using a physical payment card, the payment account information is stored on the card (in a magnetic stripe or secure chip), which is inserted, tapped or swiped at a merchant POS terminal. For mobile payments, the payment account information may be stored on the mobile device in a physical secure element or in device memory or in the cloud. Communication with the merchant POS can take place through radio frequency (e.g., a POS system that has been enabled with BLE or NFC) or via the host server for a remote mobile payment transaction.

Using BLE for payment raises questions about the security that should be implemented for storing and communicating sensitive account information. The use cases in this section illustrate potential BLE-enabled payment applications[12]; it is important to note that, with the exception of the PayPal beacon use case described in Section 3.4.3 (which has been proposed by PayPal), these are hypothetical use cases and not actual commercial implementations. It should also be noted that none of the major payment networks have standardized specifications for using BLE

[12] Use cases in Sections 3.4.2, 3.4.3, and 3.4.4 are based on use cases documented in the UL Transaction Security white paper, *Mobile Payment Transactions: BLE and/or NFC*, and are used with permission of UL. The white paper is available at: http://ul-ts.com/downloads/whitepapers/finish/6-whitepapers/282-mobile-payment-transactions-ble-andor-nfc.

as a card-present payment solution and until this occurs, the likelihood of scaled merchant adoption will remain low.

3.5.1 Tokenized Credentialing and Presentment Use Cases

The BLE specifications allow for a wide range of coverage. This has security implications when a credit card primary account number (PAN) is transmitted as part of transaction authorization. However, this risk can be mitigated (but not to a level equal to NFC or approved by any four-party payment network/scheme at this time) by using tokens that have restricted use (Figure 7). The token can be restricted to a particular merchant or hand-held device, or both. If the token is captured by a third party, it will then be of limited use.

Figure 7 illustrates an example of the use of domain restricted tokens as payment credentials, as described by the EMVCo tokenization specification[13]. The tokens could be presented at the POS using BLE and beacons. The tokens can be stored in a secure element, on a cloud-based server or within the application.

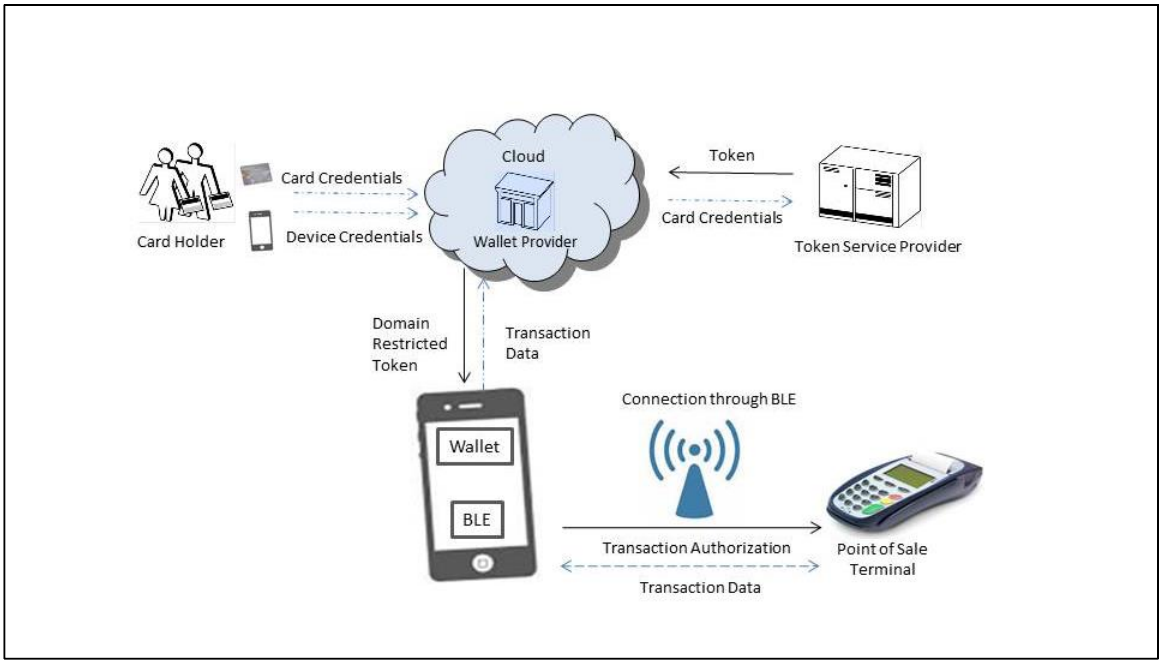


Figure 7. Use of Domain Restricted Tokens

The process could work as follows:

1. The cardholder downloads and installs a wallet application, and registers both the payment card and a mobile device with the wallet provider in the cloud.
2. The wallet provider (either a merchant or a general wallet provider) requests a token from a token service provider (TSP).
3. The TSP sends a domain-restricted token to the token requester.
4. The wallet provider sends the token to the mobile device over the air (OTA).

[13] *EMVCO Payment Tokenization Specification – Technical Framework*, Version 1.0, EMVCo, March 2014, http://www.emvco.com/specifications.aspx?id=263

5. To complete a payment transaction, the customer authorizes the payment on the mobile device, which sends the transaction authorization to the point of sale (POS) using BLE and beacons.
6. Transaction confirmation and other transaction data are sent to the mobile device using BLE from the POS.
7. The mobile device sends transaction confirmation and other data to the wallet provider's cloud OTA.
8. The payment cycle for a tokenized transaction would processed normally, as described in EMVCo's tokenization standard.

3.5.2 How BLE Might Be Used Payments

Figure 8 illustrates a potential payment process using BLE.

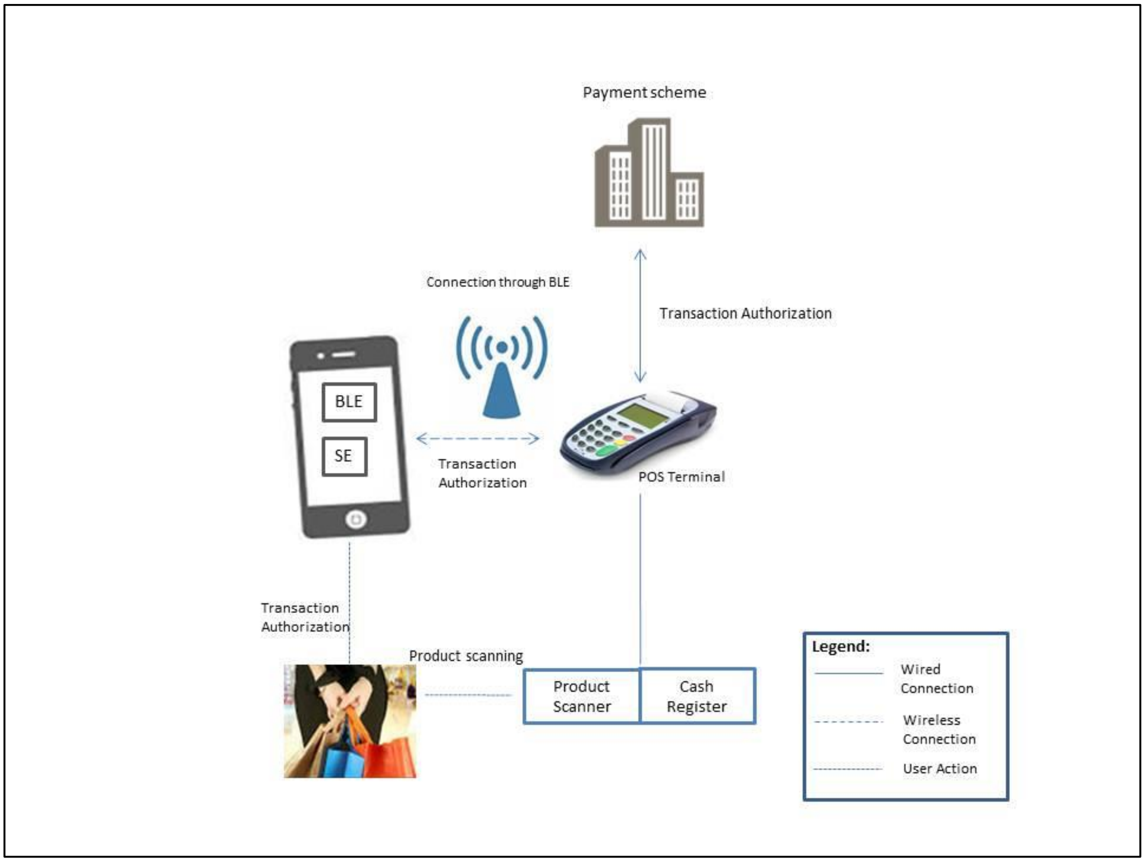


Figure 8. Using BLE for Payments

In this example, the payment account information could be stored in the physical secure element of a mobile device. The device could connect to a POS terminal using BLE. The process could include the following steps:

1. A customer is alerted using BLE that their device is checkout-enabled.
2. The merchant scans the customer's products.
3. The customer pays for the products, using payment account information stored in the secure element, by using BLE to connect to the POS terminal, and authorizes the transaction (by entering a PIN or scanning a fingerprint, for example).

4. The POS terminal transmits the transaction to the appropriate payment network for further processing.

Key questions for this use case that need to be consider for implementation:

- Is the POS terminal BLE-enabled? If so, is the POS terminal a peripheral or central BLE service?
- Does the POS have the ability to request payment credentials from a device's secure element?
- How does the payment device authenticate with the terminal? The payments industry today uses key management and payment-brand-specific contactless specifications to establish communication. How would this be done with BLE?
- Where is the consumer when BLE notifies them to checkout? How does this fit with the merchant check-out process? Is the customer in a checkout queue, in the store shopping or in a waiting area?

3.5.3 PayPal Beacons

Figure 9 illustrates the payment process using BLE with Paypal beacons. PayPal beacons work in places without mobile phone network or wireless coverage.

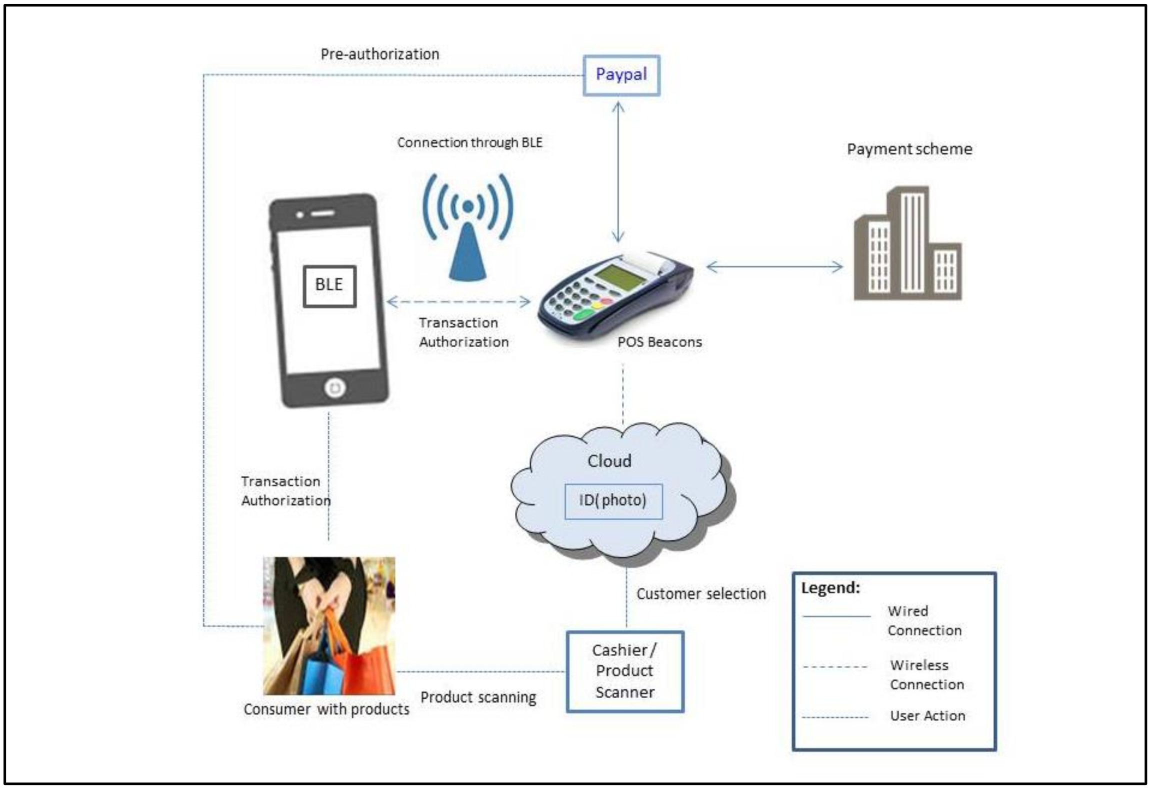


Figure 9. Payment Using Paypal on a Mobile Device

In this example, a customer makes a payment using a mobile device and Paypal. It is important to note that this process assumes that PayPal has been pre-integrated with the merchant POS to facilitate cloud requests from PayPal to the POS. The process includes the following steps:

1. When the customer enters a store in which a PayPal beacon is enabled, the Paypal app on the customer's mobile device uses BLE to announce itself to a PayPal BLE beacon.

The beacon selects a token from cache and sends across a cryptographic nonce, some metadata, and a cryptographic signature.

2. The mobile device verifies the signature with a public key embedded in the app and makes a check-in decision based on the metadata. Any data sent using BLE from the mobile app to PayPal servers are encrypted.
3. If the device has never seen this location or merchant before, the app prompts the consumer to indicate whether the consumer would like to check in now and automatically in the future.
4. At the same time as the customer registers in the PayPal system, the cashier receives a photo ID and name details for the customer.
5. When the customer is finished shopping and moves to the cash register, the customer is identified by the cashier using the name and photo received earlier.
6. The cashier scans the products received from the customer.
7. The POS contacts PayPal requesting money from the customer's account and the transaction occurs.
8. The actual transaction takes place in the cloud with a token received over a BLE connection from the mobile device. In this case, the customer does not even have to take the device out of a pocket or purse.

3.5.4 Self Scan

Figure 10 illustrates a process that allows someone with a BLE-enabled mobile device to pay at any location within a physical retail store. Payment is made without the presence of a cashier or POS terminal.

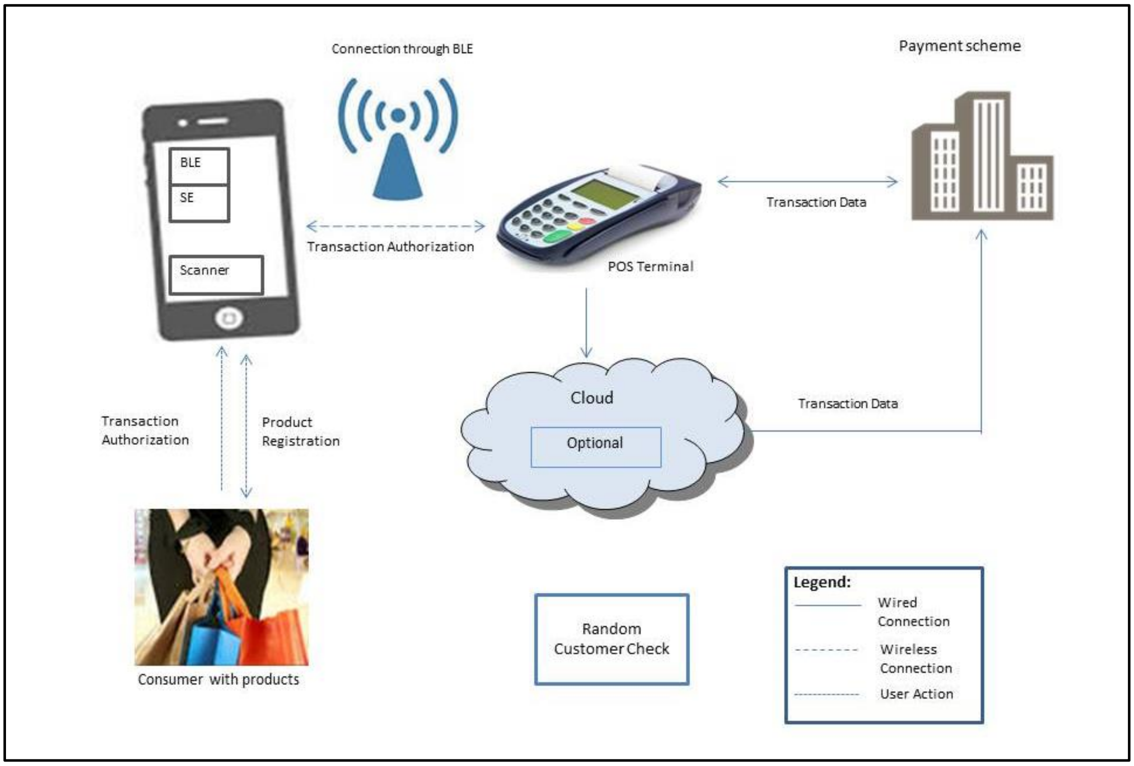


Figure 10. Payment without Involving a Cashier or POS Terminal

In this example use case, payment credentials are stored in the secure element of the mobile device. The process includes the following steps:

1. When the customer enters the store, BLE signals are exchanged between the customer's BLE-enabled mobile device and beacons spread throughout the store.
2. The customer uses the mobile device to scan products at various locations within the store using QR codes or other scanners in the device.
3. The customer uses an application on the mobile device to initiate the checkout process.
4. When prompted, the customer authorizes payment on the mobile device.
5. The mobile device uses BLE to transmit payment authorization to the nearest POS beacon.
6. The POS beacon connects to the payment network to complete the transaction.

An important consideration for this use case relates to potential theft or errors in checkout; how does the merchant know that the consumer has paid for the products when they leave the store?

4 BLE Security and Privacy Considerations

Apple and PayPal have successfully demonstrated how BLE enables a mobile phone to discover and interact with objects in its direct vicinity. When this interaction executes some form of transaction (for instance, ticketing, payment, or identification), security must be considered.

4.1 BLE Security

As proximity payment technology has developed, one consistent design principle has been interoperability. In other words, the payments technology used by the one party has to be able to communicate with the technology used by the other party in a transaction. Since in most cases the buyer and seller (or ticket holder and ticket validator) do not know each other or have never shared any secrets or credentials, the standards used for the infrastructure layer implements no authentication or encryption. Examples include the ISO/IEC 7816 protocol which is used for EMV cards and the ISO/IEC14443 protocol which is used for contactless payments In both cases, the standard does not specify how security should be implemented; the application must be designed to protect sensitive information and authenticate the payment device and user. For example, the EMV application used with payment cards and POS terminals implements security methods for both authenticating the card and verifying the cardholder.

4.1.1 Native Security

Unlike the ISO/IEC 7816 and ISO/IEC 14443 specifications, the BLE specification includes several native security features:

- Frequency hopping
- Mode control
- Privacy protection

BLE implements a scheme by which the carrier frequency in the 2.4GHz band is dynamically shifted (hopped) over available frequency bands (the three other bands are used for pairing). Such a scheme makes it difficult, although not impossible, for an eavesdropper to interpret the link. Frequency hopping is part of the classic Bluetooth protocol; however, BLE has refined the scheme.

Like classic Bluetooth, a BLE device can be in discoverable mode, limited discoverable mode, or non-discoverable mode. From limited discoverable mode, the device automatically switches to non-discoverable mode once pairing is completed.

BLE contains a privacy feature that prevents a discoverable BLE device from being tracked for location. Changing the device's private address enables a discoverable BLE device to be detected (which is the purpose of discovery) but not recognized or identified by any device other than a device with which it has previously been paired.

4.1.2 Protocol Security

The protocol itself implements several different modes and levels of security. Table 3 summarizes these modes and levels.

Table 3. Protocol Security

	Security Mode 1			Security Mode 2	
Level	**1**	**2**	**3**	**1**	**2**
Pairing	No	Unauthenticated	Authenticated	Unauthenticated	Authenticated
Encryption	No	Yes	Yes	No	No
Data Integrity	No	Yes (implicit through encryption)	Yes (implicit through encryption)	Yes	Yes

As Table 3 shows, authenticated pairing, with AES encryption using cipher block chaining of the actual data transmission, is the highest form of security offered. Depending on the BLE use case, different authentication and encryption functions can be selected.

4.2 Security Considerations for Payment Use Cases

Until BLE becomes available as a mainstream technology for payments, it is unclear how a BLE-enabled payment scheme will operate. Payment may rely on the same PAN-based payment credentials used on embossed, magnetic stripe, EMV chip, dual-interface chip, and contactless chip cards, as well as on NFC handsets. Or future BLE-based payment schemes may rely on a completely different approach, such as tokenized credentials, PKI-centric authentication, or native support for peer-to-peer transfers. Payment credentials may be stored in a physical secure element on the phone, or the implementation may resemble HCE implementations, in which a physical secure element is absent and credentials are stored in the cloud.

4.2.1 Assumptions

Regardless of how BLE-based payment systems develop, there will be a paradigm shift. In today's card payment technology, the buyer's device (card or mobile phone) makes itself known to the seller's device (POS device or acceptance infrastructure) to initiate a transaction. This is done by swiping, inserting, or tapping the card or phone on the POS device. The flow using BLE is the opposite: the seller's device (a BLE beacon) makes itself known to the buyer's mobile app. The acceptance infrastructure is owned by the consumer, not the merchant.

In addition, the payments use case relies on the fact that the payments technology connects buyers and sellers reliably and allows interoperation. Many of today's payment systems have therefore been designed with authentication and integrity controls at the application level, as opposed to the infrastructure level (for example, the authorization request cryptogram, or ARQC in an EMV scheme, or the dynamic CVV in a contactless scheme).[14] A BLE scheme could use the same application-level controls, so that any of BLE's native security features would only be needed if a successful eavesdrop attack could obtain payment credentials or privacy information.

The level of security that a BLE link should provide for payments therefore depends on the security and fraud detection measures implemented by the payments layer itself. If the payments application exhibits properties similar to those found in a (contactless) EMV application, the BLE link might not need to provide additional security mechanisms. These properties could include:

- Issuer authentication of the mobile device/transaction (e.g., using the equivalent of the ARQC), which could protect mobile payment instruments from counterfeiting and cloning

[14] Additional information on EMV can be found in the Smart Card Alliance white paper, *Card Payments Roadmap in the U.S.: How Will EMV Impact the Future Payments Infrastructure?*, available at http://www.smartcardalliance.org/pages/publications-card-payments-roadmap-in-the-us

- Application transaction counter (ATC) checking, which prevents replay attacks
- Offline data authentication (e.g., combined data authentication), which could limit the consequences of a man-in-the-middle attack (MITM) on the BLE link

In addition, if PAN use is limited to the BLE link only, the measures described above should provide a sufficient level of security for BLE payment instruments, obviating the need to rely on BLE's native security features.

4.2.2 NIST Guidelines for BLE Security

The National Institute of Standards and Technology (NIST) has published a guide to Bluetooth security[15] that covers the different versions of Bluetooth, including version 4.0 (BLE). The guide specifically targets two vulnerabilities (Table 4):

Table 4. BLE Vulnerabilities according to NIST

	Security Issue or Vulnerability	Remark
16	LE pairing provides no eavesdropping protection. Further, the Just Works pairing method provides no MITM protection.	If successful, eavesdroppers can capture secret keys (i.e., LTK, CSRK, IRK) distributed during LE pairing. Further, MITM attackers can capture and manipulate data transmitted between trusted devices. LE devices should be paired in a secure environment to minimize the risk of eavesdropping and MITM attacks. Just Works pairing should not be used.
17	LE Security Mode 1 Level 1 does not require any security mechanisms (i.e., no authentication or encryption).	Similar to BR/EDR Security Mode 1, this is inherently insecure. LE Security Mode 1 Level 3 (authenticated pairing and encryption) is highly recommended instead.

NIST is particularly concerned by the absence of security in the BLE pairing process and the potential for a successful man-in-the-middle (MITM) attack. However, if fraud prevention mechanisms similar to those found in contactless EMV are deployed, the use of BLE technology for payments instruments poses no more security risks then other chip-based payment instruments. Because BLE uses radio signals that can in theory cover distances of up to 150 meters, issuers and consumers should be made aware of the potential that an individual consumer could be recognized and tracked and that payment activity could be discovered.

4.3 Privacy Considerations

BLE allows stores to broadcast marketing information to mobile devices. While beacons are a convenient way for consumers to receive promotional information, beacons also allow companies to collect consumer location information. For example, a BLE beacon-enabled shopping mall app can know which stores a shopper visited and how long the shopper stayed in each store. If a shopper's companion also has installed the same app, the mall can find out who the companion is. This can be useful information for the mall but raises privacy concerns.

Organizations implementing BLE applications and services should consider how consumer choice is provided for opting in/out of services; how to notify consumers of terms, and what entity in the value chain is responsible for honoring both.

[15] John Padgette, Karen Scarfone, and Lily Chen, *Guide to Bluetooth Security: Recommendations of the National Institute of Standards and Technology*, U.S. Department of Commerce, National Institute of Standards and Technology, Special Publication 800-121, Revision 1.

A smartphone app can send data to a store locally through BLE. Typically all sensitive data in the message will be encrypted, but the message will contain an unencrypted advertising package. Since the BLE connection is not paired, data can be sniffed. The data itself is not sufficient to identify a person, but it can be used to locate the person and track that person's movement.

Another consideration is how the user manages their interaction with BLE-enabled applications. For example, consumers may be within range of multiple BLE beacons or have multiple applications on their phone using BLE. Mobile devices will need to be able to provide a user interface to use BLE-enabled applications and potentially to opt-in to receiving communications.

Beacons also have the risk to be spoofed. For this reason, solutions are coming which could mitigate these risks such as giving beacons trust, and then only after trust if verified, the content exposed to the consumer. Entities which look to deploy BLE should factor in the risk they expose to their customers and take the appropriate precautions or deploy the optimum solutions to ensure they both maintain customer privacy, but also not expose them to malicious attacks.

Companies that use a smartphone app to collect users' location data should disclose that information in their app. The disclosure should include why they are collecting the data, and how they will keep the data secure.

5 Conclusions

The inclusion of BLE in smartphones held by consumers is expanding rapidly. As enabled devices become more common, a range of user benefits become available across a number of market verticals. These can include, but are not limited to, venue management, event management, retail customer relationship management, food services, transportation, payment, access control, and facilities management.

BLE can serve both as a complement to and a replacement for a variety of wireless connectivity options, including NFC, WiFi, and bar code technologies. By combining cost-effective deployment of location-aware peripherals with a power-efficient, secure, and responsive communications protocol, the technology can facilitate the rapid exchange of information, including location and promotion data.

Operationally, environments such as event management facilities, retail, restaurants, and public transit can benefit from BLE's ability to facilitate frictionless engagement between the consumer's smartphone, the local terminal infrastructure, and cloud-based applications. Consumers and business operators can share valuable location data that can drive rewards, tailor offerings to be more customer centric, and enable more efficient operations and better customer service.

While there are a variety of security methodologies available to tailor security levels to the needs of the application, the nature of BLE with its long distance pairing creates opportunities for tracking of individuals, eavesdropping on transactions, spoofing of beacons, and monitoring of behavior. Consumers will need to be educated about the characteristics of these technologies and the implications of their opt-in choices. App developers will have to be vigilant in applying security strategies and technologies appropriate to their applications.

As security concerns are addressed, BLE may become a common and trusted transport layer for mobile marketing, mobile services, and, potentially, mobile payment. It is likely to grow initially as a complement to current technologies, as business concerns and related applications deal with evolving security practices and current merchant infrastructure and systems. Similarly, as the trust in BLE grows, the market will likely witness further expansion in access control and other applications.

6 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Mobile and NFC Council to provide an educational resource on Bluetooth low energy, describing what it is, how it's used, how it fits with other mobile technologies, and what security aspects should be considered for BLE-enabled applications.

Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Mobile & NFC Council members for their contributions. Participants involved in the development of this white paper included: Advanced Card Systems Ltd.; Booz Allen Hamilton; Capgemini USA Inc.; CH2M Hill; Cubic Transportation Systems, Inc.; Discover Financial Services; First Data Corporation; Fiserv Inc.; Giesecke & Devrient; Heartland Payment Systems; Identification Technology Partners; Ingenico; Intercede; IQ Devices; MasterCard; Morpho; NXP Semiconductors; Oberthur Technologies; Underwriters Laboratories (UL); Visa, Inc.

The Smart Card Alliance thanks **Michael English**, Heartland Payment Systems, who led the project and the Council members who participated in the project team to write the document, including:

- **Maarten Bron**, UL
- **Tatiana Castro**, Oberthur Technologies
- **Greg Coogan**, Morpho
- **Stu Cox**, Giesecke & Devrient
- **David deKozan**, Cubic Transportation Systems
- **Michael English**, Heartland Payment Systems
- **Patrick Ho**, Cubic Transportation Systems
- **Gonda Lamberink**, UL
- **Cathy Medich**, Smart Card Alliance
- **Robert Merkert**, Advanced Card Systems
- **Akif Qazi**, Discover
- **Lakshmi Ramanathan**, Discover
- **Steve Rogers**, IQ Devices
- **Brian Stein**, CH2M Hill
- **Sree Swaminathan**, First Data
- **Sastry Yeleswarapu**, Capgemini

The Smart Card Alliance thanks the Council members who contributed to the review of the document, including:

- **Deborah Baxley**, Capgemini
- **Peter Cattaneo**, Intercede
- **Michael Esser**, Fiserv Inc.
- **Frazier Evans**, Booz Allen Hamilton
- **Jeff Fonseca**, NXP Semiconductors
- **Simon Hurry**, Visa Inc.
- **Jeffrey Langus**, MasterCard
- **Sadiq Mohammed**, MasterCard
- **Gerry Schoenecker**, Ingenico
- **Chandra Srivastava**, Visa Inc.
- **Rob Zivney**, Identification Technology Partners

The Smart Card Alliance also thanks: **UL Transaction Security** for permission to use case studies from their white paper; **Rob Canterbury** from Gimbal, Inc., for his comments on the white paper; and **Erik Bjontegard** and **Bryan Gannon** from Total Communicator Solutions, Inc., for the San Diego Convention Center use case.

About the Smart Card Alliance Mobile and NFC Council

The Smart Card Alliance Mobile and NFC Council was formed to raise awareness and accelerate the adoption of payments, loyalty, marketing, promotion/coupons/offers, peer-to-peer, identity, and access control applications using NFC. The Council focuses on activities that will help to accelerate the practical application of the technology, providing a bridge between technology development/specification and the applications that can deliver business benefits to industry stakeholders.

The Council takes a broad industry view and brings together industry stakeholders in the different vertical markets that can benefit from mobile and NFC applications. The Council collaborates on: educating the market on the technology and the value of mobile and NFC applications; developing best practices for implementation; and working on identifying and overcoming issues inhibiting the industry.

Trademark Notice

All registered trademarks, trademarks, or service marks are the property of their respective owners.

7 References

Bluetooth Beacons, http://bluetoothbeacons.com/

Bluetooth low energy specifications, https://developer.bluetooth.org/TechnologyOverview/Pages/BLE.aspx

Bluetooth SIG, http://www.bluetooth.com/Pages/Basics.aspx

Card Payments Roadmap in the U.S.: How Will EMV Impact the Future Payments Infrastructure?, Smart Card Alliance Payments Council white paper, January 2013, http://www.smartcardalliance.org/pages/publications-card-payments-roadmap-in-the-us

Difference between Bluetooth and WiFi, EngineersGarage, http://www.engineersgarage.com/contribution/difference-between-bluetooth-and-wifi

EMVCO Payment Tokenization Specification – Technical Framework, Version 1.0, EMVCo, March 2014, http://www.emvco.com/specifications.aspx?id=263

Guide to Bluetooth Security: Recommendations of the National Institute of Standards and Technology, John Padgette, Karen Scarfone, and Lily Chen, U.S. Department of Commerce, National Institute of Standards and Technology, Special Publication 800-121, Revision 1.

iBeacons: Coming soon to a baseball stadium near you, ZDNet, October 1, 2013, http://www.zdnet.com/ibeacons-coming-soon-to-a-baseball-stadium-near-you-7000021354/

The Mobile Payments and NFC Landscape: A U.S. Perspective, Smart Card Alliance Payments Council white paper, September 2011, http://www.smartcardalliance.org/pages/publications-the-mobile-payments-and-nfc-landscape-a-us-perspective

Mobile Payment Transactions: BLE and/or NFC, UL white paper, http://ul-ts.com/downloads/whitepapers/finish/6-whitepapers/282-mobile-payment-transactions-ble-andor-nfc

Target Fields iBeacon will reach out to Twins fans' iPhones, TMCnet.com, April 5, 2014, http://technews.tmcnet.com/news/2014/04/05/7763174.htm