Airport Terminal Beacons Recommended Practice

1.0 Table of Contents

2.0 Introduction

This Recommended Practice (RP) provides guidance on the deployment and usage of airport terminal beacons. This recommended practice guide provides essential information needed to configure, implement and manage airport Beacons throughout the airport terminal, as well as the technical and managerial information needed to deliver a Beacon service.

The recommended practice was developed by an expert group established by ACI and IATA, with assistance from airports, airline and technology industry experts. As such, it is a living document that evolves to reflect industry best practice. It is not a mandated approach to Beacons at airports, and there is no obligation upon airlines or airports to implement Beacons as described in this recommended practice. International and local laws take precedence over any recommendations made within this document, and there are no regulations or requirements placed upon airports and airlines through this recommended practice.

The recommendations contained within this document have been used to successfully implement beacon infrastructure and deliver Beacon services at several airports. We hope that this Recommended Practice will be useful to Air Transport Industry. To comment on this RP, please contact:

Serge Yonke Nguewo

syonkenguewo@aci.aero

or

Andrew Price

pricea@iata.org

ACI and IATA

This recommended practice guide is a combination of industry best practices from the airlines, airports, and technology industry. The recommended practice guide has been reviewed by experts in those respective industries to assure conformance to best deployment practices. The body of the recommended practice guide will be updated on an as needed basis. This practice guide covers the broadest most general guidelines for airport adoption of beacon technology. As the technology industry changes and builds new beacon technologies changes will be detailed and published through Annexes. .

3.0 Background of Airport Terminal Beacons

A Beacon is a small device that broadcasts a short-range Bluetooth signal that can be detected by apps on mobile devices in close proximity to the beacon. Beacons themselves don't collect data.

A Beacon's core technology uses a protocol developed in 1994 by Ericsson. In 1998 a number of companies (Intel, IBM, Nokia and Toshiba) joined Ericsson and formed the Bluetooth Special Interest Group (SIG) to promote Bluetooth. The not-for-profit Bluetooth SIG has more than 24,000 member companies today. Beacons use a simple version of the standard called Bluetooth Low Energy (BLE) device. A Bluetooth LE beacon device emits a payload (known as an advertising packet). The maximum data size of this payload is limited to 31 bytes.

Bluetooth Low Energy (also known as Bluetooth Smart) became part of Bluetooth 4.0 in 2010 – so the technology has been available for several years. The primary purpose of the standard was to develop a data protocol which would create a low duty-cycle transmission which would allow very short burst transmissions over a long period. BLE devices have the following properties:

- low power requirements, operating for "months or years" on a button cell
- small size and low cost
- compatibility with a large installed base of mobile phones, tablets and computers

While Beacons have existed for several years, what triggered the interest in Beacons within the Air Transport Industry was the introduction of the iBeacon profile by Apple. This was introduced with iOS 7 in 2013. The iBeacon profile is an Apple specific format for the beacon advertising payload. With the iBeacon profile, beacons can notify iOS devices of their presence and trigger actions in apps on the device. The iBeacon payload contains (amongst other things) a UUID, majorId and minorId to identify the device.

Subsequent to the release of the iBeacon profile by Apple, Radius Networks and Google introduced their own BLE Beacon profiles. Radius Networks was the first beacon manufacturer in July 2014 to create a cross-platform beacon that supports both iOS and Google Android devices. Google responding to Apple's proprietary iBeacon standard issued the Eddystone protocol in July 2015. The newer protocols give some valuable information to an airport or a stakeholder building applications, such as beacon temperature, battery level, the ability to broadcast and trigger operations on the device. The important aspect to this is that airports need to build an infrastructure that is secure and compatible with the multiple protocols yet build a flexible solution for all stakeholders.

Common Bluetooth BLE Standards

	Eddystone (Google-Android)	**AltBeacon (Radius Networks)**	**iBeacon (Apple – iOS)**	**Proprietary (Custom– Various Vendors)**
Range	~50 meters	~50 meters	~50 meters	~50 meters
Official Android Support	YES	YES	Unofficial	YES
Official iOS Support	YES	YES	YES	YES
Open standard?	YES	YES	NO	NO
Multiple Vendors	YES	YES	YES	NO
Identifiers	10 byte namespace 6 byte instance	16 byte id1 2 byte id2 2 byte id3	16 byte UUID 2 byte major 2 byte minor	single
Interoperable with iBeacon?	NO	YES	YES	NO
Introduced	July 2015	July 2014	June 2013	Various

4.0 Technology Discussion

4.1. What is an Airport Terminal Beacon?

For the purposes of this document an Airport Terminal Beacon is defined as a device that broadcasts a restricted payload of information that can be used by apps developed for passengers and staff. Beacons can also trigger operations, notifications, open web pages, or push advertisements to devices. These features provide either an enhanced Day of Travel experience for the passenger or operational efficiencies leading to improved customer services.

Airport Terminal Beacons provide a "one-way" interaction; they transmit information for use by the app but do not receive any information back from the app. The beacon payload is essentially static and is used as a pointer into a database or other system and it is the information stored there that is used by the app to trigger some contextually relevant behaviour.

Airport Terminal Beacons are available in a wide range of formats from many different manufacturers. Beacons are generally battery powered with small form factors making them simple to deploy although "maintenance" of such devices can be a challenge. An increasingly wide range of devices are now available including USB powered devices and support for beacon and related protocols is now being incorporated into Wi-Fi access points, light fittings and even power sockets. Airports need to consider the ease of deployment, maintenance, and operational considerations beacons will demand. In addition to the beacons themselves monitoring and management is needed, which can be accommodated via management dashboards and having the beacons relay status information over a wireless network (for instance WiFi, LoRaWAN or Sigfox).

There are two general categories airport terminal beacons:

1. Beacons that communicate with applications.
2. Beacons that communicate with browsers.

The Apple standard, iBeacons are used with an application. The beacons interact with a beacon registry that is published and made available to the application via the Internet. The Google, Eddystone standard makes use of beacon registries and can communicate with physical web browsers. A physical web browser enables direct interaction with an airport beacon without opening an application. All physical web browsers can detect all physical web beacons, whereas app content is available only to users of that app.

Application Beacons

Associated with specific applications and does not work with other applications, unless a common use publically published beacon registry service is established for a major facility, such as an airport.

- Sometimes known as iBeacon™ or Eddystone-UID.
- Requires the development of a specific application, or integration with an existing application.
- Associated applications can be triggered even if they are closed and the phone is in a user's pocket.
- Because applications are continuously scanning for beacons, they can automatically record every time a customer is in the presence of compatible beacons, and even how

long a customer remains near that beacon. (In order to track in this manner, the application must receive explicit permission from the application user.)

- These applications can interpret the data and use it for location context, and then perform tasks specified by the application such as, sending a notification message.
- Bluetooth® must be turned on.
- The app needs a user's permission to "listen" for that signal.
- Notifications can be pushed to a user's phone. The user MUST have Bluetooth on, and the app set to receive these pop-up notifications.

Browser Beacons

Requires a 'beacon browser' (i.e. Physical Web browser) that can 'hear' any browser-centric beacon.

- Sometimes known as Eddystone-URL or a Physical Web beacon, they broadcast the URL of a website.
- Requires no new development as long as there is an existing mobile-friendly website to link to.
- Beacon browsers require the user have the browser open on their screen, to discover new nearby Physical Web content. Commonly relying on visual cues and a pull approach, where consumers choose what information they want to see.
- They are driven by a user's interest in the information, and present information only when requested, rather than pushing information.
- Because Physical Web pages are accessed by user choice, compatible browsers do not track ongoing interactions with beacons.
- Bluetooth must be turned on.
- Tends to have more battery life compared to iBeacon in the same hardware configuration, because most use-cases require fewer broadcasts per second.
- Notification URL links can appear on a user's lock screen, but it does not push notifications to users.

4.2. Building Beacon Business Models

4.2.1. Introduction

This section details the business models that can be used to deploy an airport beacon and related infrastructure. The infrastructure model needs to be understood for each airport based upon existing infrastructure, pending infrastructure or terminal changes, and airport business model.

4.2.2. Overview

Airports operate in a variety of different organizational structures. The most common structures are airports are either owned by local or state governments or airport authorities. The airports are operated as a public trust to make air transportation available to the communities they serve. As a part of that endeavour they work together with airlines and concessionaires to provide services for travellers.

Airports which control their own rate structures use compensatory fee structures, where the airlines pay for aviation related costs. The airports control the concessions and collect revenues and may use the revenue to improve public services and amenities. In this situation

the airport authority assumes the financial risks. The other method of airport operation is where the airlines control all rate structures and operate in what is called a residual rate structure. The airlines may use revenues from concessions to offset the aviation related costs. The airlines essentially control the level of public services and amenities that are offered. Some airports operate in what is called a hybrid method which is essential a joint sharing of responsibilities between the airlines and local authorities.

4.2.3. Impact on Technology Deployment

Technology decisions at airports can be complex depending on how they are structured as a business entity. Airline hub airports tend to have a centralized management structure based upon the dominate carriers financial position. Government or airport authority based airports tend to operate airports where dominate airlines are not present. Airline hub airports can adopt a new technology rapidly if dominant, making a business case to the dominate airline. Airlines can also make a simple business case to the airport authority and request them to implement the technology and charge the airline. Government operated airports tend to adopt technologies through consensus and establishment of business cases.

In both cases business cases must be made for adoption of a new technology. The subsequent sections describe an approach to making that business case. Stating the problem, opportunity, or service is the most important part of framing potential options for building the business cases.

4.2.4. Building the Business Case

The business case must provide a succinct problem statement, solution alternatives, recommended solution, and an implementation approach. The executive overview must give a business vision, strategy, or objectives. The overview must state what processes or technologies are not operating efficiently. In the case of new technologies (such as beacons) it is important to describe trends and commercial or operational needs that can be answered by using new technologies. How the technology could be used to meet statutory, legislative, or environmental requirements are important. It is important to discuss the pros and cons of centrally or a federated management of beacons might offer the airport for implementation options. Facts regarding these trends should be kept in a separate appendix for reference.

4.2.5. Options for Implementation

It is important that airport management be presented with at least three options for beacon deployment. This is to make certain that there is a discussion that leads to the best option to be selected for each particular airport since no one model will fit all airports. Included in these models there should one that discusses what happens if the airport decides to take no action. Each option should be described briefly and then benefits, goals, and measurement criteria should be discussed for that option. Following that should be a discussion of the costs and funding plan for that option separating capital expenditures from operating expenditures. Feasibility for each component of the project should be described for each major component. Risks also need to be identified, their likelihood of occurring, impact to the option, and mitigation measures if they occurred. Any other issues not already identified need to be discussed. The major assumptions impacting delivery of that option should be identified.

4.2.6. Recommendation

Each option should be identified and placed into a decision table for evaluation and rating. The criteria for a successful outcome should be listed against each option being considered. Weighting can be established if there are adequate reasons from a technical or business

perspective. Following the table there should be a section which describes recommended option in more detail.

4.2.7. Implementation Approach

Once the choice has been made by the project team, a discussion of how to acquire the solution must be developed. Alternatives for deployment should be discussed. These may include installation by initial stakeholders on their projects, with beacon ownership transferring to another for long term care. Another alternative may be that the airport takes the responsibility to deploy beacons as a core offering to the airport. Interaction between other initiatives also must be taken into consideration. As an example beacon deployment may be added to other airport initiatives, such as a WiFi concession contract or a distributed antenna project. It is important to describe the family of related initiatives on the application side of a beacon deployment. There will be airline, airport, and concessions programs that will all have use cases for beacons at an airport. In the implementation plan it is important to include a communication plan back to management that covers: project accountability for tasks, mitigates risk, and conveys project deliverables status. The implementation plan should have acceptance test criteria, and planned tests prior to acceptance and project close out.

An Airport Business Technology Business Case Template is included for reference into the Annexes.

4.3. Common Use Beacon Infrastructure

4.3.1. Common Use Beacon Infrastructure

Beacons provide a convenient way to address passengers needs to offer help, services, and goods based on their current location. Instead of isolated beacon use for single airlines, airports or service providers, a commonly used beacon infrastructure opens the opportunity to share the access to passengers among all involved.

Airlines and airports have proven the efficiency and feasibility of sharing equipment, e.g. kiosks, Wi-Fi access points, check-in desks, and boarding gates. Extending this philosophy to beacons across airports that all airlines and shops can utilize is the driver of the common use Beacon technology.

The main drivers of the application of Beacon technology to passenger services are:

- The increased need for a temporal, context and location driven communications to passengers.
- Technology readiness of transmitting devices, e.g. Beacons.
- Introduction of iBeacon standard by Apple in June 2013 to standardize on usage of Bluetooth beacons with iOS smart phone devices
- Introduction of BLE capabilities on the Android in December 2013
- Growth of feature rich mobile devices amongst passengers.
- Common capabilities of mobile devices, e.g. Bluetooth LE.
- Growth of passenger services through mobile applications, e.g. check-in, notifications.

4.3.2. Philosophy

We recognize that the industry around Beacons is developing fast and there are many manifestations of beacon management and applications appearing in the industry (and outside). The aviation industry approach puts accessibility, simplicity, and common use at its heart.

A beacon registry is required to provide mobile apps with information on beacons deployed throughout the airport. Each airport has a unique identifier, and each beacon has a unique set of identifiers within the airport to define its location. See Appendix 1 for the list of beacon

location identifiers. Section 3.7 and Appendix 3 go into more detail on the beacon registry services available for the beacons, like getting a list of relevant beacons for an airport and telling the registry when a beacon has been spotted.

4.3.3. Beacon Applications

Because the beacon registry is intended to be common-use, it is purposefully left general. Specific use cases, like alerting passengers, or collecting data for business intelligence, would require a separate application. The beacon ranging functionality could be included in an airport's or airline's app easily. The application just needs the user's permission for location, which the app probably already asks for.

With the registry and beacons in place, both partners will benefit from sharing a common infrastructure. The airline and airport can both provide specialized local services, as well as be able to enrich the data available from their applications. More specifically, apps can have additional location context given the addition of the beacon data, which can enrich proprietary data already available to those individual applications.

Application Examples

Using the Beacon technology mobile applications can provide a wide range of location and context driven services to the passengers. Some examples of application ideas include:

4.3.3.1. Welcome to airport

One of the simplest use cases is to provide a welcome message to the passenger on arrival to the airport, along with some instructions – go to security if already checked in, or go to check in / bag drop.

4.3.3.2. Enhanced way finding and indicating position on map

Applications pre-loaded with the airport map would be able to pinpoint the location of the device holder on the map and provide way finding instructions. The Beacons transmit their identity to the listening devices. The identity is then used to query the Beacon repository for rich metadata about the Beacon.

4.3.3.3. Walk time to gate

The beacon can provide location information to the application. If the app has the passenger itinerary, this can be combined with FIDS data to determine departure gate. From this, the walk time from current location to the departure gate can be determined (along with time to boarding).

4.3.3.4. Flight check-in notifications

Passengers in range of the check-in points can be reminded of the check-in close time through applications. The criteria to trigger notifications could be time and location.

4.3.3.5. Flight boarding notifications

The Beacon technology can be used to provide passengers with boarding notification, e.g. closing of gate, change of gate, delays, and cancellations.

4.3.3.6. Baggage arrival information

The passengers only need to know about the Baggage arrival information at a certain time and location. Beacons can be used to trigger the ideal time to communicate to the passenger about the baggage. An example usage is when passengers enter the baggage hall, the phone can display which carousel their bags will arrive on, and how long before the bags arrive.

4.3.3.7. Security queue information

Beacon technology can trigger notifications to passengers that are close to a security checkpoint with for example estimated queuing time or recommend alternative security checkpoints.

4.3.3.8. Restaurant / retail promotional notifications

Applications would be able to provide users that are within range of a shop, special offers and discounts. The promotions can be targeted to a more relevant audience by only targeting devices that are within a pre-set range of a Beacon.

4.3.3.9. Lounge access information

Beacon technology can trigger notifications to provide users information about lounge access when in proximity of a lounge, or inside a lounge.

4.3.3.10. Locate staff/passengers

The beacons are associated with a specific location within the airport (e.g. Gate A22). It is possible to locate a passenger or member of staff by associating the passenger / staff with the last known beacon proximity detection. This can be used by airports to determine which staff member to allocate a job/task to, and it can be used by airlines to determine if passengers are airside/landside or near a gate when boarding starts.

All of these applications can also feed the new beacon location data into a backend system that can provide rich business intelligence, which can help better serve customers and improve processes and practices. Some examples include:

- An airline could see a flight manifest with last known passenger locations
- a gate agent could know that a VIP passenger is in the area
- an airport could evaluate passenger flow patterns
- a shop could know that customers are in the area and provide personalized service or coupons

4.3.4. Maintenance and Monitoring of Beacons

Beacons may require routine maintenance such as changing batteries and resetting radio power. It is possible that some of the maintenance can be accomplished via a beacon application dashboard or via connection to a wireless network. It is important that once a commitment has been made to install the infrastructure it must be maintained and a clear maintenance program must be established. To reduce maintenance efforts, an airport may choose to install beacons that are integrated into the building power system.

4.3.4.1. Crowd Sourced Beacon Monitoring

Most airports have thousands of passengers walking around their venue on a daily basis. Even with a 0.1% app adoption, there are still many app users walking around the airport, and this presents one approach that can be harnessed to monitor beacons. To be more specific, the apps running on all users' devices can be used to report beacon status back to a central server in the background. Users, without any change in their app experience, can perform the monitoring of the system. This method has no additional costs and is scalable by design.

4.3.4.2. Special maintenance app

An alternative approach is to use a maintenance app that can be provided to airport staff. The app would perform bulk checking of beacons as staff walk around the airport. A dedicated staff member/team can simply walk around the airport every 1-2 weeks to measure and report

beacon status. Alternatively there will probably be various staff members who already walk through the airport as part of their role and monitoring can take place in the background.

4.3.4.3. Reporting through Wi-Fi___33

Wi-Fi___33-capable beacons (more details below) have started to emerge over the last year, which allow monitoring, reporting and even configuring of beacons in its range. This is certainly an interesting option; however, they require a degree of effort to install (due to power and Wi-Fi___33 requirements) and beacons at some locations in the airport may be difficult to cover due to lack of Wi-Fi cover or suitable power sockets.

4.3.5. Wi-Fi___33-capable beacons vs standard BLE beacons

In the industry, beacons typically imply passive BLE radio transmitters which cannot provide any interaction on its own. In typical setups (as advised by Apple and others), beacon is just a signal source and all the logic is carried out by a processing device, such as on smartphones. More advanced beacons with Wi-Fi___33 capability have started appearing in the market. In fact, some are already being used in airports. Wi-Fi___33-capable beacons, as we call them, provide regular BLE beacon advertisement but also have capability to connect to Wi-Fi___33 and transmit data. Hence, from a mobile application perspective, they are still passive beacons. However, from a back-office perspective, they enable some interesting use cases such as monitoring battery levels of all beacons in their range, monitoring if a non-provisioned/rogue beacon enters the area, or even detecting if an escalator stops working (with help of additional sensors, such as accelerometer, in the beacon). This beacon type would be an airport specific modification to the broader specification as a part of this document. The implementation would follow the same guidelines and policies for deployment.

4.3.6. Testing of Beacons

Most airports have thousands of passengers walking around their venue on a daily basis. Even with a 0.1% app adoption, there are still many app users walking around the airport, and we believe this can be harnessed to maintain beacons. To be more specific, all user apps, as they pass through the airport, can report beacon status information to a central server in the background. Users, without any change in their app experience, can effectively be the testers of the system. This method has no cost and is scalable by design.

If an app is not available on the market, or if the apps don't have a significant number of users, a maintenance app, that allows bulk checking of beacons, can be provided to airport staff. A dedicated staff member/team can simply walk around the airport every 1-2 weeks to measure and report beacon status. In fact, there will probably be various staff members who already walk through the venue for their daytime job.

4.3.7. Beacon Security Issues

This is not an exhaustive discussion of Beacon security issues, but discusses the essential concerns for building reliable and secure applications for airports and stakeholders. Airports adding Beacon technologies to their existing airport IT infrastructure need to consider security as a part of the implementation.

4.3.7.1. Physical Security

Beacons should be placed in physically secured environments to prevent theft, tampering, and placing in administrative mode. Beacons can be placed with other infrastructure equipment that is secured in cabinets, behind counters, or physically attached and secured. While attaching to display walls may ease initial deployment, it is an easy target for theft and vandalism in many environments.

4.3.7.2. Privacy

Use of beacons can potentially allow for passive surveillance of individual phones. While a beacon broadcasts identifiers publicly, an iPhone does not need to connect to an iBeacon-enabled beacon to get this information. To understand the importance of this, consider an example of how Bluetooth services traditionally work. For a temperature sensor, Bluetooth will advertise that a temperature service is available. An iPhone can listen passively for a service advertisement or can send out a request for this service. Either way, when the service is discovered, the iPhone then connects to the sensor and requests the temperature information. If a third party nearby is scanning for Bluetooth traffic, they will see the traffic and can uniquely identify the iPhone based on a built-in Bluetooth value, known as a MAC address. This is not related to the identifier used for iBeacons, but as part of standard Bluetooth. The iPhone Bluetooth MAC address can be discovered whenever the iPhone is transmitting over Bluetooth. In the example interchange above, the iPhone Bluetooth MAC address would be exposed when requesting a scan or connecting to the temperature sensor. The mobile device could potentially be tracked using the Bluetooth MAC address.

4.3.7.3. Beacon Security Practices

4.3.7.3.1. Authorized Access Prevention

The use of credentials to change settings is critical. Simply making it difficult to discover how to connect the beacon to change settings is not sufficient. Setting a complex password with sufficient length can prevent people from trying to guess the password. Having a mechanism to detect unauthorized authentication attempts and initiate progressively longer timeout periods between authentication attempts helps prevent brute force password attacks.

4.3.7.3.2. Unique Passwords

Beacons should not all have the same or similar passwords. Organizations should have the ability to set unique passwords for each beacon and should not deploy using the default vendor password.

4.3.7.3.3. Encrypted Channel

All authentications should be done over an encrypted channel and passwords should not have the ability to be extracted from the physical beacon. Since Bluetooth pairing to a beacon is usually done using Secure Simple Pairing that does not require an out-of-band password, initial pairing should be done in an area that is free from unauthorized scanning of the Bluetooth network.

4.3.7.3.4. Provide a mechanism for updates

Since security vulnerabilities can be discovered at any given time, it is important to get timely security notifications and firmware updates to keep the beacons secure. Beacons must support the ability to update the software on the beacons themselves.

4.3.7.3.5. Reduce Attack Surface Area

Since iBeacon is a broadcast only protocol, administration must be done while the iBeacon is not acting as a beacon or over a different communications channel, for instance another Bluetooth radio. Beacons must not allow service connections when deployed and broadcasting as an iBeacon. This reduces the attack surface area since an attacker could not connect to the beacon, making it difficult for automated attacks.

4.3.7.3.6. Prevent Beacon Spoofing

To mitigate risk from spoofed beacons consider adding within the applications a validation provision that could include beacon + geolocation, beacon + a software seed number, a cloud based validation step, or a hardware validation methodology. These will prevent spoofed beacons from interfering with airport or airline applications.

4.3.8. SDK and Web Services

Airports may consider the use of a SDK that hides beacon and registry complexities from mobile apps and provides generic location-based services to applications. It is important that this SDK is supplier independent and uses open standards and protocols where available. This will ensure that beacon applications are portable between airports.

4.3.9. Offline capabilities

Beacons advertise data and with the current beacon registry approach, we expect users to connect online to fetch additional information on beacons based on the reference number advertised by beacon. However, beacons are physically capable of advertising more information than just a reference number for lookup in the registry. An SDK can tap this potential to provide offline capabilities and given the significant proportion of foreign passengers at most airports, a solution that works without relying on internet would be preferable. Some SDK's provide positioning and navigation offline whilst still allowing for dynamic changes in the layout, showing this is possible.

4.3.10. Vendor dependency

Implementation should take place to assure it does not create dependencies to any one protocol. SDK's can hide complexity for beacon identification. This assures the same set of data will be consistently presented, regardless of hardware or protocol used.

4.4. Cost Recovery

4.4.1. Motivation and background

The airport/terminal operator or other common use provider should install and maintain of the beacon infrastructure.

The provider of the beacon infrastructure shall have the opportunity to the share the costs for the managed infrastructure among all using partners (airlines, retailers, handling agents, etc.) in order to guarantee a high quality of service over the whole life cycle of the beacon infrastructure.

4.4.1.1. Shall requirements

A charging methodology shall be applied for all users (retailers, airlines, handlings agents, etc.) of the airport beacon infrastructure in a non-discriminating way. This methodology shall cover the initial costs (investment - CAPEX) and the operational costs (OPEX) of the shared part of the beacon infrastructure.

4.4.1.2. Should requirements

The charging methodology for the beacon infrastructure should be described as a part of the business model for the beacon system, prior to airport-wide installation. The charging methodology may consider one or several of the following approaches.

Capital Expenditure

- Total installation cost shared by proportional percentages of airline, concession, and public space.
- Total installation cost borne by airport, airline, or common use provider with cost paid for in base rates.
- Total installation cost added to Wi-Fi concession provider and deducted from minimum annual guarantee costs over contract term.
- Total installation costs Concession provider with minimum annual guarantee costs reduced over contract term.

- Total installation costs provided by terminal advertising provider with minimal annual guarantee costs reduced over the contract term.
- Total installation cost added to Airport IT cost center and added to base rates.

Operating Expenditure

- Operating expenditure is added into leasing rates for terminal spaces
- Operating expenditure is captured via incremental increases in revenue through value added services in concessions directly through beacon based sales
- Operating expenditure is added to Wi-Fi concession provider and deducted from minimal annual guarantee costs over the contract term
- Operating expenditure is added to advertising concession provider and deducted from minimal annual guarantee.
- Operating expenditure is added to Airport IT cost center and added to base rates.

4.4.2. Alternative measures to recover costs

Where additional projects are included in the initial planned Beacon infrastructure, then these projects should be part of the initial business case. It is anticipated that future projects will be developed that make use of the Beacon infrastructure. When this occurs the business case for the project should reflect the deployment model and charging models that are appropriate based on the business model(s) that have been previously selected.

4.5. Security

A common concern among beacon owners is the mere possibility that beacons can be spoofed, replicated or even hijacked. Furthermore, it is possible to introduce rogue beacons to a venue (without venue's permission) for other uses or to even break another application's use of beacons.

4.5.1. Motivation and background

An airport/terminal operator shall provide the beacon infrastructure with a high quality of service (QoS). QoS requires not only a good maintenance of the infrastructure but also the protection of this infrastructure against fraud and unauthorized uses. This covers not only the pure infrastructure but also the business models of the authorized users. Therefore the usage of beacons should be controlled to avoid actions that compromise these business models.

Why avoid hijacking: the unauthorized party might use an airport beacon in a way that competes with airport business interests or that produces inconsistent information for passengers. Moreover, the unauthorized party might use a beacon without paying for the use.

Why avoid spoofing: spoofing will reduce the quality of the beacon infrastructure and will confuse passengers.

Why avoid unauthorized beacons: the unauthorized party might use their beacons in a way that competes to airport business interests or that produces inconsistent information for passengers. Moreover unauthorized beacons will lead to additional and unnecessary requests at a beacon registry. This will influence the service in a negative way.

4.5.2. Definitions

Hijacking: the unauthorized use of airport beacons by third parties, for example in their mobile app.

Example: A third party sniffers for beacons and uses these beacons to push location based services in its mobile app without authorization by the airport or terminal operator.

Spoofing: the simulation of existing airport beacons by an unauthorized third party at a different location.

Example: someone takes the content (UID, Major ID, Minor ID, or MAC-Address) of an existing airport beacon from a gate room and simulates a beacon with similar content at a different location, e.g. at Check-In desk

Unauthorized beacons: beacons in the airport environment that are not owned and maintained by the airport/terminal manager.

Example: third parties apply their own beacons in the airport/terminal environment to support their own business model.

4.5.3. Should requirements

The beacon infrastructure provider should implement features to prevent or at least to beacon hijacking as difficult as possible, such as:

Change to some extend some parts of the beacon content (Major ID, Minor ID, or MAC-Address – not the UID) on a regular basis (every week or month) for at least 25-50% of the beacons and usage of a synchronously adapted registry to get beacon location and required metadata information.

Thereby it is important, that the UID stays unchanged or at least in a range of predefined values, since the UID is used in Apple devices to register a smartphone app in the operating system iOS. This is for example important to start a registered smartphone app whenever an iBeacon with the relevant UID (or a UID from predefined set) has been identified by the device. Thus, changing the UID to a value out of this range will cause a lack of an important functionality.

The airport should make use of a standardized location web service that is being managed by ACI and SITA. This web service will deliver a location to a smart phone app based on available information from various infrastructures, such as:

- Beacons
- Wi-Fi networks
- 3G/4G networks
- and other information sources where available

Implementation of security should not hinder the application development or value to the airports, airlines, or stakeholders since beacons can support new customer service functions and business models. It is not recommended is the usage of a beacon hashing algorithms in combination with a dedicated and supplier specific SDK for the smart phone. These kinds of solutions will avoid interoperability, especially for airline apps covering several airports.

The beacon infrastructure provider should establish technical or organizational measures to identify beacon spoofing. Examples might be:

- An area scan for unknown beacons should be performed on a regular basis (every month to every quarter).
- Feedback functions for passenger smart phone apps in order to get feedback from passengers on inconsistencies in the location based services or localization functions.
- In case of the usage of a registry: identify requests for unexpected beacons and try to locate those using analytic functions.
- In case of the usage of a registry: identify requests on unknown beacons and try to locate those using analytic functions.

- Unauthorized beacons should be removed whenever identified

4.6. Web Services

4.6.1. Introduction

This section details the APIs available for using the common-use registry of beacons, including detailing the endpoints, input parameters and output data structures.

4.6.2. Beacon Registry API

The common-use beacon registry was initially developed by SITA and is currently operational. As such, the current services are documented on https://www.developer.aero/Beacon-Registry-API/API-Overview with the APIs featured available at https://www.developer.aero/Beacon-Registry-API/Registry-APIs/Typical-usage-description. This section details the intended use of the API, with links to the individual APIs to

Notes

The goal of the common-use registry is to provide a central repository of and API's for lookup of all the beacons in all the airports in the world. It is not the intention of the registry to provide data elements, services or infrastructure for the many use cases that can be built around beacons. All such application specific requirements must be provided by the organizations implementing the app, and stands alone from the registry.

4.7. Beacon Registry Standards

4.7.1. Introduction

This section contains details about the standards for how iBeacons should be configured and deployed in airports to ensure interoperability. Within the three classes of beacons, iBeacon, AltBeacon, and Eddystone, the ACI has elected to remain compatible with iBeacon since it contains features that are common among all beacon types. AltBeacon is an open standard which requires use of a database beacon registry very much the same way as iBeacon. Eddystone adds the ability to directly trigger events on smartphones and tablets without using a beacon registry. Airports and airlines at this point want to limit that feature within our business environments. Those features if approved at local airports may be enabled, but as an international standard would not be advisable since the triggering cannot be central secured and managed. This kind of interaction has a high risk to have security or privacy concerns and is not yet a recommended practice until the beacon industry matures.

4.7.2. Common-use Specification

The purpose of the common-use iBeacon specification is to encourage consistent beacon deployments across airports, and lower the barrier to entry for airlines & airports using beacons in applications. A successful measure of the specification will be if airline applications do not need to have any airport specific code in iBeacon related use cases.

The specification comprises several distinct parts beacon configuration, metadata, and alternative beacon type configurations.

4.7.2.1. Configuration of iBeacons

An iBeacon broadcasts a payload of 32 bytes, containing what are known as the UUID / majorId / minorId to identify the beacon. An application running on a phone can then correlate this identification data with information in a common registry to identifying the physical location of the beacon within the airport.

The beacon identification schema determines how the three identification parameters (the UUID/majorId/minorId) should be specified. In order to support application developers, and to handle iOS system implementations (specifically iBeacon Region Monitoring) there are some considerations to take into account when coming up with a beacon identification schema.

There is a hierarchical relationship between UUID, majorId, minorId. It is recommended that the following standards are adopted.

- Each airport has its own UUID value.
- Each zone (e.g. gate, lounge, security, baggage hall) within the airport shares the same majorId value
- The minor Id can be any arbitrary value (within the permitted range defined by iBeacon profile)
- The combination of UUID/majorId/minorId should be unique per airport.

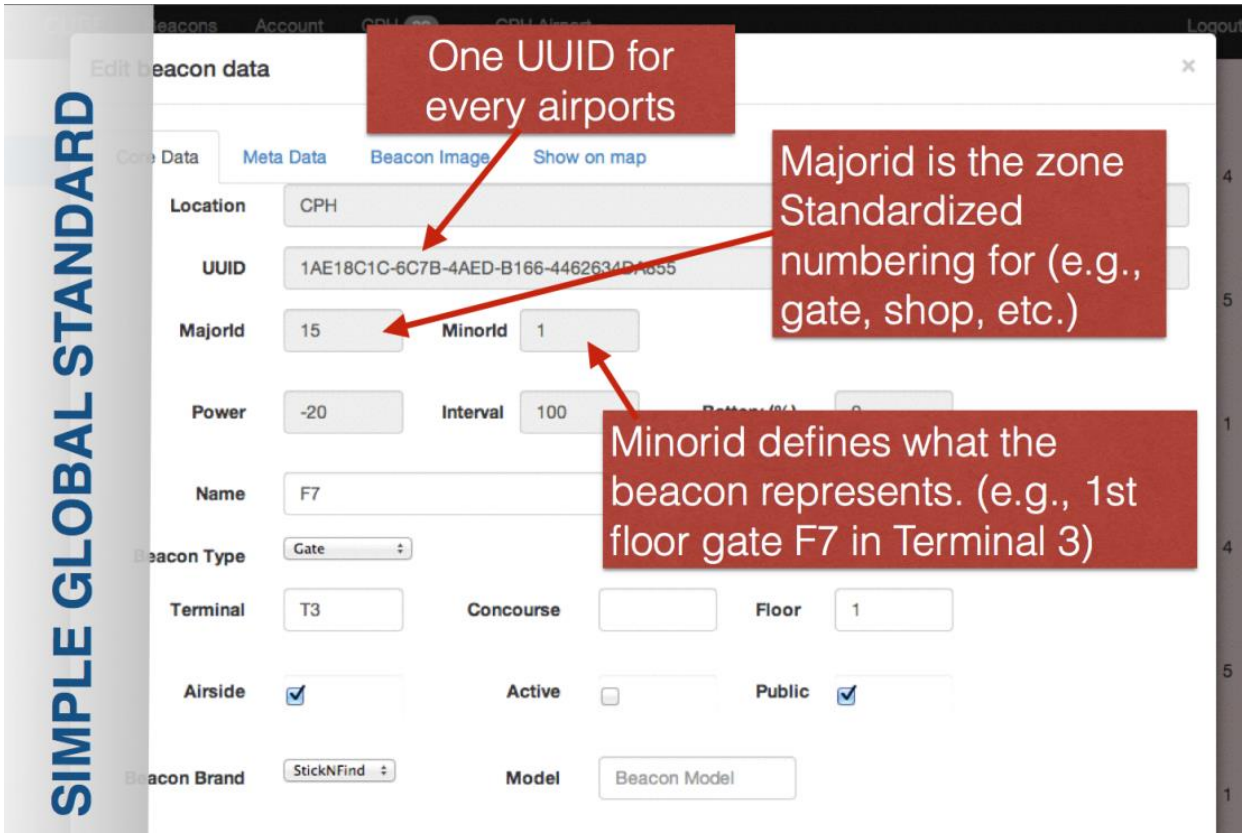

Figure 1 - Beacon Configuration and Metadata Screen

The reasons for recommending this approach are related to the limitations that iOS places on application developers for what is known as iBeacon Region Monitoring. There are some limitations which mean that apps cannot simply monitor all beacons in all airports – instead the app must take an approach of monitoring for high level granularity (UUID + majorId) and then if required change to a more granular monitoring (UUID + [majorId + multiple minorId]).

Note - the UUID values are already pre-assigned to airports, and there already exists a set of Zones defined. These can be viewed on https://cube.api.aero/. A list of defined beacon Ids is in the Technical Annex.

4.7.2.2. Meta-data for iBeacons

The iBeacon characteristics can identify what airport a beacon is in (from the UUID) and it can also identify what zone of the airport it is in (from the majorId). However it cannot provide further details such as what airport terminal it is in, or if it is airside or landside, or for Gate beacons what specific gate it refers to.

The Meta-Data part of the specification exists to provide this information.

- Beacon Type (zone)
- Airport Code
- Airport Terminal
- Concourse / pier within the airport
- Floor of airport the beacon is on
- If the beacon is airside/landside
- Beacon Transmission Power

4.7.3. Configuration of AltBeacon ID's

AltBeacon ID's should be configured to be compatible with the iBeacon format.

4.7.4. Configuration of Eddystone Beacon ID's

Eddystone ID's should be configured to be compatible with the iBeacon format. Eddystone beacons can also be configured to directly trigger interactions with the smartphones or tablets as approved by the airport authority, airline, or stakeholder at the airport where the beacons are deployed. Advertising and gaming beacons should not be used without airport authority authorization.

ANNEXES

Annex 1 - Abbreviations and Terms

Abbreviation / Term	Description
AltBeacon	AltBeacons is an open-spec, free beacon design provided by Radius Networks. It looks to be gaining some momentum. The AltBeacon spec seems to be a direct response to the closed source iBeacon spec that Apple is using; it covers the same functionality that an iBeacon has but is not company-specific.
beacon	Bluetooth beacons are a device that broadcast signals that can be heard by smart devices nearby. Paired with a smartphone application or web browsers, businesses are able to deliver contextually relevant content and information to users at very specific locations. Beacons transmit a unique identifier called a UUID that helps a device "understand where it is" and display contextually relevant content for that location, as defined by the individual or company that placed the beacon. In addition to transmitting messages to phones, beacons can also be used to understand traffic patterns and other behaviours by detecting the location and path of individual mobile devices.
Bluetooth	Bluetooth is a telecommunications industry specification that describes how mobile phones, computers, and personal digital assistants (PDAs) can be easily interconnected using a short-range wireless connection. Using this technology, users of cellular phones, pagers, and personal digital assistants can buy a three-in-one phone that can double as a portable phone at home or in the office, get quickly synchronized with information in a desktop or notebook computer, initiate the sending or receiving of a fax, initiate a print-out, and, in general, have all mobile and fixed computer devices be totally coordinated. Bluetooth requires that a low-cost transceiver chip be included in each device. The transceiver transmits and receives in a previously unused frequency band of 2.45 GHz that is available globally (with some variation of bandwidth in different countries). In addition to data, up to three voice channels are available. Each device has a unique 48-bit address from the IEEE 802 standard. Connections can be point-to-point or multipoint. The maximum range is 10 meters. Data can be exchanged at a rate of 1 megabit per second (up to 2 Mbps in the second generation of the technology). A frequency hop methodology allows devices to communicate even in areas with a great deal of electromagnetic interference. Built-in encryption and verification is provided. The technology got its unusual name in honour of Harald Bluetooth, king of Denmark in the mid-tenth century.
Bluetooth LE, BLE, also marketed as Bluetooth Smart	Bluetooth low energy (Bluetooth LE, BLE, marketed as Bluetooth Smart) is a wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group aimed at novel applications in the healthcare, fitness, beacons, security, and home entertainment industries. Compared to Classic Bluetooth, Bluetooth Smart is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range. It was merged into the main Bluetooth standard in 2010 with the adoption of the Bluetooth Core Specification Version 4.0. Mobile operating systems including iOS, Android, Windows Phone and BlackBerry, as well as OS X, Linux, and Windows 8, natively support Bluetooth Smart. The Bluetooth SIG predicts that by 2018 more than 90 percent of Bluetooth-enabled smartphones will support Bluetooth Smart.

Eddystone	Eddystone is Google's competing protocol. Apple licenses the iBeacon protocol, whereas Eddystone is open source. Eddystone works on both Android and iOS. Eddystone transmits three frame types as opposed to iBeacon's one. One is a URL frame that can activate a mobile device to directly open a web page when the passenger are in close proximity to the beacon. One is a UID frame type which is very similar to the iBeacon frame allowing interoperability. One is a TLM frame type that enables telemetry status from attached sensors, battery levels, or administrative data.
iBeacon	iBeacon is the name for Apple's technology standard, which allows Mobile Apps (running on both iOS and Android devices) to listen for signals from beacons in the physical world and react accordingly. In essence, iBeacon technology allows Mobile Apps to understand their position on a micro-local scale, and deliver hyper-contextual content to users based on location. The underlying communication technology is Bluetooth Low Energy. Apple's implementation requires the use of web based registration of the beacons and there locations to enable the application functionality. Additional information (metadata) can be added to the registry. iBeacon differs from some other location-based technologies as the broadcasting device (beacon) is only a 1-way transmitter to the receiving smartphone or receiving device, and necessitates a specific app installed on the device to interact with the beacons. This ensures that only the installed app (not the iBeacon transmitter) can track users, potentially against their will, as they passively walk around the transmitters.
LoRaWAN	Also known as Low-Power Wide-Area Network (LPWAN) or Low-Power Network (LPN) is a type of telecommunication network designed to allow long range communications at a low bit rate among things (connected objects), such as sensors operated on a battery.
QoS	Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies.
Sigfox	Sigfox's goal is to develop a system to connect intelligent devices. Its network costs are reduced and it requires little energy, being termed "Low-power Wide-area (LPWA) networking". It utilizes a wide-reaching signal that passes freely through solid objects, what it terms "ultra-narrowband", which consists of free sections of the radio spectrum, particularly the ISM band. Telecommunications companies usually intend on developing shortwaves capable of carrying the largest amount of data possible (such as 5G), whereas Sigfox intends on doing the opposite, that is using the longest waves. Sigfox posits that their messages can travel up to 1,000 kilometres (620 mi) and each base station can handle up to a million objects, consuming 1/1000th the energy as a standard cellular system.
UUID	A universally unique identifier (UUID) is an identifier standard used in software construction.
WiFi	Wi-Fi (or WiFi) is a local area wireless computer networking technology that allows electronic devices to connect to the network, mainly using the 2.4 gigahertz (12 cm) UHF and 5 gigahertz (6 cm) SHF ISM radio bands.

Annex 2 – Major ID Codes

SITA Original MajorId	Additional Metadata Use Code	Zone Name	Description
	1000-2000	Landside Zones	Beacons that are located from the first facilities used by passengers or stakeholders to the Security Screening Check Point
	1000	Rental Car Check-in	
	1100	Public Transit Stop	
	1200	Ground Transportation Center	
	1300	Commercial Vehicle Staging Areas	
2600	1400	CarHire	This beacon identifies the car hire area
1700	1500	CarPark	These beacons are the airport carpark.
1000	2000	Ticket/Check-in	These beacons are to identify a check in desk, or a check in hall
	2100	Staffed Check-in Counter	
2400	2200	Self-Service Kiosk	This beacon identifies a kiosk at the airport, such as a self-service check in kiosk
	2300	Bag Drop Counter	
	2400	Self-Tagging Stations	
	2500	Curbside Check-in	
1600	3000	Security Screening Check Point (formerly Security Zone)	These beacons are placed in the security check point between landside and airside.
	4000	Terminal Zones	Beacons that are generally located within the secure areas of Terminals
	4000	Public Spaces	
	4100	Restrooms	
	4200	Public Seating Areas	

	4300	Domestic Meeter/Greeter Area	
	4400	International Meeter/Greeter Areas	
1100	4500	Secure Circulation (formerly Walkway)	This is a general purpose waypoint beacon. It can be used to indicate which terminal, concourse, floor of the airport a passenger is in. These are typically placed in the long walkway areas in airports.
	4600	FIS Sterile Circulation	
2200	4700	Connector Corridors	This beacon identifies the airport transport areas, such as transit trains from one terminal to another.
2200	4800	APM Stations	This beacon identifies the airport transport areas, such as transit trains from one terminal to another.
2200	4900	Conveyances	
	5000	Non-Public Circulation	
	5100	First Aid	
	5200	Visitors Aid	
1300	5300	Retail	Retail beacons are used to identify a single shop, or if a passenger is in the general retail area of the airport.
2000	5400	Restaurant	Retail beacons are used to identify a single restaurant/cafe, or if a passenger is in the general food hall area of the airport.
	5500	News / Gift	
	5600	Specialty Retail	
	5700	Duty-free shop	
	5800	Business Center	
	5900	ATM Machine	
	6000	Currency Exchange	
	6100	Miscellaneous Retail	
	6200	Advertising	
1200	6300	Gate	Gate beacons identify a boarding gate at the airport.
1500	6400	Lounge	The lounge beacons are used to identify an airline or airport lounge.

1400	6500	BaggageHall	These beacons are used to identify that a passenger is in the baggage hall, or at a specific baggage carousel.
1800	6600	Not used	Not used
2100		Other	A general purpose beacon.
2300	6700	ArrivalsHall	This beacon identifies the arrivals hall in the airport.
2500	6800	Plane	This beacon identifies the entry/ exit point of an aircraft
	7000	Non-Public Terminal & Airside	Beacons that are located in non-public areas of terminals or airfield
1900	7100	Airline Administration Office (formerly SalesOffice)	This beacon is for an airline sales office.
	7200	Baggage Service Office	
	7300	Airline Operations Office	
	7400	Ramp Tower	
	7500	Baggage Make-up Area	
	7600	Baggage Off-Load Area	
	7700	Baggage Train Circulation Area	
	7800	Baggage Handling System	
	7900	Mechanical, Electrical, and Plumbing	
	8000	Information Technology Rooms	
	8100	Maintenance, Janitorial, and Storage Areas	
	8200	Receiving Areas and Loading Docks	
	8300	Airport Operations Office	

	8400	Public Safety Offices	
	8500	Isolation Areas	
	8600	Tornado Shelters	
	8700	Mobile Assets	
	8800	Baggage Carts	
	8900	Wheelchairs	

Annex 3 Identification of locations

Ranging vs. Monitoring

Ranging usually takes place in the foreground of an application and allows to actively scan for beacons. Monitoring allows to get notified when the device app is running on enters or exits a specified beacon region. Monitoring can take place in the background. Depending on the use cases one may want to implement based on beacons, it is important to select the correct mode.

At least in the iOS concept of handling iBeacons two different modes of interaction are defined:

Ranging

This is when a user opens an application (in the foreground) that will actively scan for beacon IDs to react on those of interest. This mode consumes substantially more battery power; the ranging mode is the most reliable way to detect any beacon and is closer to a "real-time" identification.

Monitoring

This is when a user places the application in background mode and will allow for notification to a user when they enter or exit pre-defined regions. The application for a given list of "region" definitions for each app, iOS will detect and report "region enter" and "region exit" events to the respective app. The app may be started in background by iOS to handle the event. Different beacons with overlapping ranges and the same region definitions will NOT trigger new events when passing between them. This is a power-effective way to configure beacons, although triggering is not reported to be not reliable in all cases. This is because the polling frequency is much longer in monitoring mode as opposed to ranging mode. This is not considered a "real-time" identification mode.

Note: ranging mode is currently the only mode Android is supporting.

Zones vs. Regions

Under iOS Apple defines regions as one contiguous area for the purpose of a given application; generally this refers to the entrance or exit of a major venue, such as an airport. Each region has one and only one UUID.

The SITA beacon repository has two mandatory rules to be applied to beacon identification:

Rule 1 - One airport has exactly ONE UUID - Any "zone" on that airport has ONE major ID

With the iOS region concept as described above, a SITA zone will mostly be one region, defined by UUID plus major ID. Larger zones, like "GATE" thus may have only one enter event being triggered when first entering the zone. This will require the app to enter ranging mode as soon as the zone has been entered to find a dedicated gate within the GATE zone – that is, the app has to remain active in the foreground and actively do scanning for beacons.

Rule 2 – Each airport has a maximum of 20 MajorID's – This is an iOS limitation.

Regions are defined through the majorID numbers. Additional granularity on location can be provided through the minor Id numbering system. Further definitions can be supported by adding the Additional Metadata Use Code.

Basic mandatory beacon data

As a basic requirement, a beacon's location must be known geographical and level-wise. Advisable data is:

- **Mandatory**: geolocation (latitude/longitude, fractional numbers)
- **Mandatory**: absolute level (physical level relative to ground floor=level 0, positive/negative integer number)
- Optional: position in regards of the security control (airside/landside/other)
- Optional: position in regards of the immigration (local/transfer/other)
- Optional: local level (level designator as used locally on the airport)
- Optional: terminal/concourse names
- Optional: URL to retrieve additional data that may be provided by the beacon owner.

Zone identifications

The following bases on the SITA zone definitions (https://www.developer.aero/Beacon-Registry-API/Beacon-Registry-APIs/What-are-Beacon-Types*3F*) and extends these.

A beacon must belong to one of the zones to be recognized. For a finer localization, some zone definitions will require additional data for the beacons. In the zones table below, these data fields are given, if applicable. (M): mandatory, (C): conditional, (O): optional data.

Formal definition of the additional data field formats and enumeration sets yet to be defined!

Zone	Description	Additional Data	Remarks
GATE	beacons identifying a specific gate, or region of gates	(C) gate ID	Def. by SITA
CHECKINDESK	beacons at a check in desk, or in check in hall	(C) counter ID	Def. by SITA
SECURITYZONE	beacons inside the security check area		Def. by SITA
BAGGAGEHALL	beacons at a baggage carousel or in the baggage hall	(C) carousel ID	Def. by SITA
RETAIL	beacons in the retail area or at a specific store in the airport	(C) shop type (C) shop name	Def. by SITA, extended to retail area
RESTAURANT	beacons at a specific restaurant/cafe/food outlet	(C) food type (C) restaurant name	Def. by SITA
CARPARK	beacons in the airport parking area	(C) parking area name	Def. by SITA
LOUNGE	beacons in an airport lounge	(C) lounge operator (C) lounge name	Def. by SITA
TRANSITZONE	beacons in an airport terminal transfer area (e.g. bus, monorail)		Def. by SITA
SALESOFFICE	beacons at an airline sales office	(C) airline	Def. by SITA
WAYPOINT	beacons for wayfinding in the airport		Def. by SITA

Zone	Description	Additional Data	Remarks
JETBRIDGE	beacons on a Passenger Loading Bridge (aka Jet Bridge)	(C) position ID	Def. by SITA, was "RAMP"
OTHER	Any other general purpose beacon	(C) description of location	Def. by SITA
TERMINAL	beacons at an entry of a terminal	(C) terminal name	
BAGDROP	beacons at bag drop area or counter	(C) counter ID (C) baggage type	
CURBSIDE	beacons at curbside facility	(C) curbside service type	
LOUNGEENTRY	beacons at the entry of a lounge	(C) lounge operator (C) lounge name	
LFSERVICE	beacons in baggage service facilities (lost & found office)	(C) operator	
SANITARY	beacons at sanitary areas	(C) F/M/PRM/BABY	
PRAYER	beacons at a prayer room/church etc.	(C) confession	
PUBLICTRANS	beacons at public transportation terminals (bus, rail, taxi etc.)	(C) transport type (C) local name	
INFO	beacons indicating general information points		

Notes

Zones can be overlapping with more than one beacon present giving different zone types (like beacon 1: LFSERVICE and beacon 2: BAGGAGEHALL in the surroundings of a lost & found office in the claims area).

- There is no obligation to cover all areas of an airport
- There is no obligation as well to have all zone types being used at an airport
- Conditional data should be provided as is available and will help white-label service apps, but are not guaranteed

Annex 4. Navigation

Great strides have been made towards indoor navigation during the past ten years. Indoor navigation is accomplished by many different methods with varying degrees of success. Initial use of WiFi signals was quite poor and many smartphone manufacturers sought methods to enhance this technique. They added sensors to the phones to augment the data being received from the triangulation of signal strength. This method was also not very successful but did enhance the indoor location mapping considerably.

Recently both Apple and Google have announced changes to their location services offerings using known mapped signal strength for large venues. Both companies are commencing the scanning of the largest urban facilities for WiFi signal strength in addition to indoor photography of the venue. This is what both Apple and Google are recommending to major application developers to make use of for mapping and way finding. Where applied that locational accuracy is quite good generally within 5-10 feet. Airports need to work with both vendors to complete the WiFi signal strength mapping of their venues. Apple and Google will then bundle this as web service for location to their development community. Neither Apple nor Google intend to directly make money from the mapping of the signal strength – it is from the applications and their related sales that they will be able to make additional revenue. Airports need not seek financial remuneration for the companies to map the signal strength of the facility. It should also be noted that if significant reconfigurations of the space occur the mapping would have to be redone to improve the accuracy of the location services.

Beacons can be used to augment the core location services provided by WiFi and works together with the signal strength mapping to give micro-location level accuracy. Beacons were developed by Apple and Google to enhance the user experience by triggering applications when in proximity of a beacon. They were not intended to be the primary navigation system for indoor facilities; however applications can be built using them as a network of sensors to perform that function.

Beacons provide a very attractive platform for precise indoor positioning and navigation, including the various features that are associated with this, such as tracking, heat maps and point of location (POL) search. Providing a navigation service through beacons requires a good level of accuracy to be useful, since poor accuracy could result in incorrect travel times (for example from the other side of a security wall). In addition to this, poor accuracy can result in losing operational benefits, such as calculating queue lengths from visitor activity and understanding how customers are interacting with the shops which can lead to additional revenue streams. The downside of using beacons as a primary navigation solution is that since this makes use of the ranging mode a devices battery life will be severely reduced.

A position can either be based on proximity to other things (such as by check-in gate 36) or as a grid reference across the airport – enabling many more features as a result. Proximity struggles with the accuracy problems mentioned above and can result in a less efficient beacon distribution since if a shop is next to a gate then two beacons may be needed, despite the locations being close to each other.

Providing navigation to customers can achieve several benefits, from assisting visually impaired users to navigate the airport, to helping customers relax with the knowledge they know where they are going. Further benefits can include the precise location of important customer services assets such as wheelchair locations, customer service agent locations, or finding specific points of service for passengers.

Annex 5. Installation and Maintenance

During the installation, beacon orientation should be noted and standardised where possible, since some beacons have different signal strengths in different directions, particularly when mounted on a wall vs. on a ceiling. This variation can have a big impact on beacon performance.

Beacon maintenance can significantly affect an installation since small changes in performance or configuration can have big impacts on the cost and effort to maintain. Each airport will have a different approach to this situation and hence the idea of this section is to give a list of discussion topics which can be used to help confirm the most effective setup for each airport.

Beacon batteries last between 18months and 48months, depending on the performance they are configured for. Alternatively beacons can be powered by solar panel, light fitting, USB or mains power, hence integrated into other devices to reduce maintenance. The top effects come from:

1) Advertising power – beacons send their signal at a chosen power level and the higher this is the shorter the battery life is, though the signal is heard from further away. Beacon power levels should be set based on the beacon surroundings, but should normally be the same across the airport to help standardise the installation and use of the beacon network.
2) Advertising interval – beacons send out their signal every X milliseconds, this should be set depending on the responsiveness required. When higher, the beacon will consume more battery.

Beacons rarely require replacement at the same time due to variances in performance and it is suggested that processes are designed to understand beacon performance across the airport with minimal labour requirement. Replacement may be required due to damage, theft, battery depletion or general upgrade processes and will be mixed between emergent work and planned work.

Annex 6. Beacon Use Cases

Title	Problem Statement	Value Propositions	Location	Category
Airport Train Way Finding	Many leisure travellers are unfamiliar with the airport train system, which can lead to a stressful experience. While there are only a few stops, many passengers do not know when to get on or off the train at their destination.	Smartphone applications can detect platform mounted iBeacons in time to enable passengers to make informed decisions, i.e., stay on train or get off at the appropriate platform.	Train or Shuttle Platform	Time Crumbs
Checkpoint Wait Time	Almost every passenger is concerned about the time required to pass through the security checkpoints. This uncertainty can lead to a stressful, unpleasant travel experience.	Beacons installed at entrance lanes and retesting positions at security checkpoints can be used to compute average wait time for Pre-Check and other lanes.	Checkpoints	Location Analytics
Satellite Way Finding	A common way finding problem has been the number of international travellers who fail to find the escalator down to the airport train systems. A variety of signage efforts have helped but iBeacons may prove to be a superior solution.	Mobile app provides personalized, way finding assistance and immediate notification when a passenger walks past escalator to Satellite.	Way point navigation	Redirect Notifications
Ground Transportation Way Finding	Passengers seeking ground transportation are often confused by the need to cross to the parking garage, walk to the metro bus stop, travel to the light rail station in the garage or find the nearest rental car bus stop.	Arriving passengers are given personalized way finding directions from terminal exits to third floor ground transportation objectives: taxi, limo, metro bus, rental car bus, light rail station.	Ground Transportation	Way Finding

Airport Lounge Advertising	The airport lounge product offering includes single day, walk up opportunities for passengers. The hours of operation are not visible to many travellers and the locations of the lounges are often difficult to find in the airport.	A prototype loyalty smartphone app provides way finding and notification when in close proximity to walk up lounge opportunity. Beacons serve as way points for self-guided travel to each lounge.	Airport Lounge	Way Finding
Common Use Way Finding	Increasing the use of the Port's investment in common use technology is aligned with several airport strategies. Our international carriers use kiosks extensively to assist improving their passenger experiences.	Passengers are given way finding assistance to common use kiosks when arriving at south end of the parking garage.	Check-in and Bag Drop	Location Analytics
Taxi/Limo Vehicle Tracking	Accurately and cost effectively tracking the activity of taxi and limo vehicles is important to the collection of non-Aero revenue. The current system requires costly automated vehicle identification (AVI) technology and an audit capability is desired.	Tests demonstrate the accuracy and precision of vehicle tracking using iBeacons mounted on a taxi or limo. A smartphone will capture and log test vehicle movements and compare the results with the AVI system.	Ground Transportation	Asset Tracking
Green Initiative Messaging	Surveys indicate that 1/3 of passengers knew little or nothing about our initiatives. The average dwell time by passengers presents an opportunity to communicate our messages.	The Port's environmental messages can be presented to passengers via Beacon-popup notifications with relevant web pages on laptops, tablets and smartphones.	Environment Program	Info & Entertainment

Port Vehicle Tracking	Situation awareness is critical to our safe and secure management of the airport. Several technologies can be used to track vehicles with varying degrees of accuracy and investment cost.	Beacons mounted on Port vehicles are identified by time and location with a high degree of accuracy with Beacon detectors on mobile and stationary devices.	Vehicle Tracking	Asset Tracking
Art and Music Initiative Messaging	The airport's support of the arts has gained visibility in recent months. Unfortunately the location of our art exhibits and music venues is not widely known by our passengers.	Beacons are used to both identify and promote the airport's art and music programs. This technology is superior QR code campaigns.	Art Program	Info & Entertainment
Concessions Advertising	Static signage and stylized airport maps available from the Port web site do not meet the needs of mobile passengers. Opt-in advertising with a location aware smartphone is the recognized future of retail advertising.	Beacons are used to both identify and promote the airport's concession opportunities. Pop up notifications will drive revenue growth while meeting passenger privacy concerns.	Dining and Retail	Marketing
Automated Passport Control Way Finding	Way finding for our international travellers will present new challenges as CBP introduces new processes and the construction of the IAF adds to complexity to signage strategies.	Beacons present personalized way finding directions to international travellers and leverage mobile technology in smartphones, e.g., mobile passport control apps.	International Arrivals	Way Finding
Connecting Passenger Way Finding	Way finding for connecting passengers is often difficult for the leisure or the infrequent business traveller, when arrival and departure gates are on different concourses or satellites.	Beacons present personalized way finding directions to connecting travellers and leverage mobile technology in smartphones, e.g., airline apps, Tripit, etc.	Connecting Passenger Way Finding	Way Finding

Disabled Person Way Finding	Way finding for connecting passengers is difficult without personal assistance from airline or airport staff to make it from the entrance to the terminal, to ticketing, screening, concessions, and to the aircraft	Beacons present a personalized way finding directions for disabled passengers through the use of technology in smartphones.	Terminal Way Finding	Disabled Services / Way Finding
Wheelchair Tracking and Dispatch	It is difficult to know when and where a wheelchair and attendant may be to meet a passenger.	Beacons present personalized way assist disabled populations to make use of the airport.	Connecting Passenger Way Finding	Disabled Services / Way Finding
Concessions Advertising	Airport loyalty applications could target specific passenger services for up sales, or concierge services.	Beacons present personalized way for passengers to locate desired items for purchase, also the applications could suggest up sale items. Beacons could also provide a method to provide advanced personalized concierge services to deliver goods, services, or food directly to know passengers by locating them via Beacons.	Dining and Retail	Marketing
Terminal Construction	Construction many times has a large amount of documentation for specific areas that must be referenced during construction, inspection, and commissioning.	Beacons a method where a construction management company could install beacons at specific locations where a web service could automatically reference and pull up lists of construction, inspection or commissioning documents.	Terminal Construction	Airport Development

Annex 7. CYBER SECURITY RISK MITIGATION TECHNIQUES

Bluetooth, WIFI and Hybrid Beacons leverage commonly used wireless communications standards that can be easily detected by nearly every modern smartphone from a distance of nearly 100 meters. This raises concerns regarding the security of the identity of the beacon and the data received and transmitted by these beacons located in public places. By default, beacons constantly broadcast static UUID, Major and Minor IDs that can be detected easily exposing the beacons to the risks of Spoofing and Hijacking (or Piggybacking) for potential unauthorized deployment or use.

Potential Cyber Security Risks:

The following examples indicate potential risks involved in any implementation of the current beacon technology:

- An unauthorized third party application could use these beacons (Hijacking or Piggybacking) to push location based services without authorization by the airport.
- The identity (UID, Major ID, Minor ID, or MAC-Address) of an existing airport beacon located at a gate could be cloned (Spoofing) to simulate a beacon with similar content at a different location, e.g. at Check-In desk.
- Unauthorized third parties could easily install their own beacons (Unauthorized Beacons) in the airport/terminal environment to support their own business.

Cyber Security Risk Mitigation Techniques:

Geolocation Validation:

The mobile device detecting the registered beacon validates (for each session) the geolocation of the beacon to ensure it is near the intended physical space. This type of control prevents spoofing.

Changing (or Rotating) Beacon IDs and Cloud Validation:

Beacons are programmed to changing IDs at regular intervals. This feature prevents spoofing and piggybacking. The ID sequence and change interval are registered in the Beacon Registry database located in the cloud.

Remote management through hardware controllers:

WIFI or Bluetooth connected Hardware controllers could be provisioned to remotely manage and update beacons. This feature will allow for automated software program managed changes to beacon IDs.

Secure mode firmware:

Beacon are automatically registered in the cloud and associated with its owner, based on the email and personal details provided during the purchase process. The secure firmware version will only allow the owner to connect to and update the beacons they own. This feature is being implemented in the Google beacons made by Estimote.

Annex 8. Acknowledgements

The following have actively contributed to the Beacons Recommended Practice document and its supporting documents (in first name alphabetical order):

	Name	Organization
1	Alan Glasby	SITA
2	Andrew Price	IATA
3	Aneil Patel	ACI-NA
4	Antoine Rostworowski	ACI World
5	Arie Van Der Veek	Schiphol Group
6	Arturo Garcia-Alonso	ACI World
7	Axel Katalan	Pointrlabs
8	Barrett Clark	Sabre
9	Catherine Mayer	SITA
10	Daniel Young	Easy Jet
11	Dave Wilson	Port of Seattle
12	Derek Harn	Alaska Airlines
13	Ege Akpinar	Pointrlabs
14	Gilles Brentini	Geneva Airport
15	Helena Marruecos	IATA
16	Juan Francisco Garcia Lopez	Indra Airports
17	Jurjen Braakhekke	Schiphol Group
18	Kevin O'Sullivan	SITA
19	Mark Call	Pointrlabs
20	Mark O'Connor	Los Angeles World Airport
21	Maurice Jenkins	Miami Airport
22	Micha Harwerth	Deutsche Lufthansa AG
23	Nora Duus	Fraport
24	Philip Stranger	Apple
25	Raoul Cooper	British Airways
26	Rolf Felkel	Fraport
27	Samuel Ingalls	McCarran Las Vegas Airport
28	Serge Yonke Nguewo	ACI World
29	Sri Sagaram	Arora Engineers, Inc
30	Yuval Kossovsky	Apple

ACI and IATA would like to thank them for their contribution, effort and continuous support.