

SYSTEM, DEVICE AND METHOD FOR ACCESSING SHARED INFRASTRUCTURE

5 FIELD OF THE INVENTION

This invention relates in general to a system, method and a device for providing access to shared infrastructure, such as a computer-implemented device. The shared infrastructure may be may be a device such as a printer for printing a boarding pass or bag tag, a
10 scanner for reading documents, or a kiosk for printing a boarding pass or a bag tag. The system may for example be for use by customers, passengers, and agents providing services to the customers or passengers.

BACKGROUND OF THE INVENTION

15

Usually, airlines share a common infrastructure, such as computing devices which are generally provided by an airport, to process their passengers. Known shared common infrastructure solutions are inflexible, costly, difficult to deploy and operate, and do not easily accommodate the latest technology such as the use of mobile devices. This is
20 because known solutions force airlines to work with the lowest common denominator environment. For example, a specific version of Microsoft WindowsTM, a specific version of AdobeTM FlashTM, or a specific version of JAVATM which are commonly used by shared devices in the airport environment may determine how know solutions interact with, or access specific services. This may lead to technical difficulties in providing access to the
25 shared devices.

It will also be appreciated that known platforms, such as the MicrosoftTM WindowsTM platform which may operate on shared devices, are closed platforms. This forces users to access devices in the local airport environment by way of a local interface to communicate
30 with the platform. Thus, there is no provision to be able to commute remotely with one or more devices in the local airport environment.

Accordingly, it will be appreciated that known solutions link the features of end peripherals (such as a printers, scanners, and so on) through the application interface thus preventing
35 peripherals to evolve and add passenger usability features without impacting the application.

Further, Virtual Private Network, VPN, systems have the problem that they require users to input additional data such as further log-on credentials after accessing remote systems via the VPN, which can simply be thought of a tunnel through which communications are sent.

5 SUMMARY OF THE INVENTION

The invention aims to address these problems by providing a computer processing device for providing access to one or more electronic devices. The device comprises processing means configured to: determine a location identifier associated with a user login event;
10 associate the location identifier with a user session identifier; and communicate the location identifier and associated user session identifier to an application.

Further, embodiments of the invention provide a mechanism which provides one or more tokens to one or more devices. Use of particular tokens by devices facilitate communication
15 without intervention.

This is in contrast to VPN systems which do not have a number of different functional components which transform the data content as the data is passed between the functional components.
20

Thus, the system allows airlines to operate in their own environment without any restriction imposed by another airline sharing the common infrastructure. The invention provides cloud based services that lowers cost and provides efficient deployment and operational model. The invention allows segregation of an airport environment from the airline
25 environment, thus allowing all entities to evolve based on their business needs. The invention provide a timeless interface for airlines applications based on essential data exchange using latest web technology. The interface removes the influence of client devices. The invention may comprise an easy-to-use portal that allows device providers at an airport to setup an environment which is independent of an airline's users. The portal
30 allows airlines to activate their application instantly at available airports and locations with no dependency on a third party.

The core functionality of the solution provides common API's that allows an airline's applications to dynamically subscribe to shared or dedicated infrastructure at any location
35 in any available airport at global scale. The shared or dedicated infrastructure is not limited to airports, and it may include parking lots, hotels, railway stations, convention centres, city

centres, cruise ships etc. The API's may use location identification to associate airline user sessions to shared infrastructure. Location Identification is based on an easy-to-build naming convention that uniquely identifies any infrastructure at airports and non-airport locations. Client applications may obtain the location identification in a number of different
5 ways, such as QR labels, Beacons, NFC and so on.

The architecture of the solution relies on separating the user interface from the physical devices that requires user interaction, for example the obtaining of boarding passes, dropping bags, scanning documents, payment and boarding gates etc. This may be
10 achieved by way of 2 communication channels and this may provide the flexibility for user interface devices such as workstations, tablets, smart phones to evolve independent of devices such as a passport scanner, chip and pin for payment, self-bag drop and so on.

Embodiments of the invention also provide a solution to the need for backward
15 compatibility. The platform provides a means for airlines to continue using their existing software with little or no modification, while taking advantage of the flexibility the new platform offers them. This may be achieved by way of a field gateway functionality.

Embodiments of the invention may employ an architecture which is able to provide access
20 to shared infrastructure in a distributed framework. This implementation is not limited to a specific version of MicrosoftTMS WindowsTM, or LinuxTM or CiscoTM IOxTM, or AndrodTM applications.

Embodiments of the invention employ an architecture which is able to run on any of these
25 systems. This may be achieved with the use of an internet browser. Usually, the browser is provided with html 5 standard. This may allow access to a Next Generation Portal, NGP distributed network or frame work of devices according to the html 5 standard. This has the advantage that the only local resources are those needed to run the browser. Accordingly, many of the processes requiring considerable processing power may be pushed into or
30 performed in a host environment such as an airline back-end system, open server system, departure control system, in a data centre or in the cloud. This means that the only local resources which need to be used are those used by the browser. This allows certain applications to run faster than known solutions because for example a database does not need to be locally downloaded.

35

According to a first aspect of the present invention a data processing system for providing user access to one or more devices (108) is provided. The system comprises processing means (103) configured to: determine a location identifier for a user; associate the location identifier with a user identifier for the user; and communicate (3013) the location identifier and associated user identifier to an application (301).

According to a further aspect of the present invention a computer processing device for providing access to one or more electronic devices is provided. The device comprises processing means (103) configured to: i. determine a location identifier associated with a user login event; ii. associate the location identifier with a user session identifier; and iii. communicate (3013) the location identifier and associated user session identifier to an application (109).

According to a further aspect of the present invention an electronic device comprising a field gateway component for facilitating authentication with a remote environment is provided.

According to a further aspect of the present invention a method for providing access to one or more electronic devices is provided. The method comprises the steps of: a. determining a location identifier associated with a user login event; b. associating the location identifier with a user session identifier; and c. communicating (3013) the location identifier and associated user session identifier to an application (109).

According to a further aspect of the present invention a computer program product is provided for providing access to one or more electronic devices. The product, when executed performs the steps of determining a location identifier associated with a user login event; associating the location identifier with a user session identifier; and communicating (3013) the location identifier and associated user session identifier to an application (109).

An application may be provided in a remote data centre, and this allows for additional resources to be provided in the data centre. This allows performance to be increased as desired. In other words, embodiments of the invention allow for easy vertical scaling capability for example by adding additional memory or servers to the remote data centre as necessary.

A further benefit of using an html 5 enabled browser is that additional certification of any application is not needed. This provides a huge benefit to airlines since new functionality does not need to be certified as it is not deployed using a new application in the airport environment, but is rather provided via the html 5 enabled browser. Further, because there
5 is no need for an application to share an environment with other vendor applications, liability for other vendor applications is avoided.

Further, it is easier for systems running embodiments of the invention to achieve PCI compliance since the environment is not shared between a number of different
10 applications.

Embodiments of the invention may separate the data required to print or read a document from the features related to usability of the peripheral. The data exchange is part of the application interface where the usability part of the peripheral is controlled through
15 configuration this allowing the peripherals to add usability features without impacting the applications and this preserves the longevity of the interface.

Embodiments of the invention employ a solution, referred to as a Next Generation Portal, NGP, solution. The solution may be implemented by providing 2 distinct channels. These
20 channels may be referred to as a device channel, and a graphical user interface, GUI channel. This, coupled with an internet browser enabled with html 5, may provide many of the benefits outlined above.

Thus, the solution is based on a pure data exchange between different functional
25 components. Other capability may be governed by configuration settings. Thus, if changes need to be made, then these changes may be performed by way of configuration capability settings. Accordingly, in some embodiments, an application interface is driven by pure data alone. Usability of the application is configured through configuration settings.

30 On the device side, a similar architecture may be employed. For example, this focuses on the logical separation of data exchange services and configuration services, which may relate to the look and feel of the device interface.

For example, the airport environment may make services available or in other words
35 publish services to the API environment used by users. Subscribers to the application environment, such as an airline, may view the published services. This allows users to

subscribe to any one or more of a number published services. The publication and subscription services may be provided independently.

5 In contrast to known VPN systems, in the present invention, data content is transformed by a number of functional components, also using bi-directional communication and end-to-end authentication. The data may be transformed based on a rules engine. Of course, the nature of the data transformation may be different for each user of the system, based on their needs.

10 Thus, embodiments of the invention may be based on a cloud platform such as Microsoft™ AZURE™ technology, specifically the use of IoT Hub, Service Fabric, API gateway, Stream Analytics and Machine learning. The solution is built using multifaceted security, specifically the use of stream analytics, machine learning and deep learning to profile the user and system behaviour to identify and adapt to anomalies.

15 According to an aspect of the present invention a data processing system or device for providing user access to one or more further devices (108) is provided. The device comprises processing means (103) configured to: determine a location identifier associated with a user login event; associate the location identifier with a user session identifier
20 wherein the user session identifier is preferably associated with the user login event; and communicate (3013) the location identifier and associated user session identifier to an application (301).

25 According to a further aspect of the present invention a method for providing access to one or more electronic devices is provided. The method comprises the steps of a. determining a location identifier associated with a user login event; b. associating the location identifier with a user session identifier; and c. communicating (3013) the location identifier and associated user session identifier to an application (109).

30 BRIEF DESCRIPTION OF THE DRAWINGS

An embodiment of the invention will now be described, by way of example only, and with reference to the accompanying drawings, in which:

35 Figure 1 is a schematic diagram of the main functional components embodying the invention;

Figure 2 is a schematic diagram showing the system architecture of an embodiment of the invention; and

Figure 3 is a flow diagram showing the sequence flow of various different functional components according to an embodiment of the invention.

5

The following description is of a system for use in the aviation industry, but this is exemplary and other applications of the invention will also be discussed. For example, the system may be used in any environment where infrastructure is shared. The system may be embodied in a hosted system which may use API communications protocols to communicate with external systems such as reservation systems or departure control systems.

In this particular embodiment, Application Programming Interface, API, services or modules are built on a Microsoft AZURE platform. However, other platforms known to the skilled person may be used, such as an Amazon Web Services, AWS, cloud platform, an IBM cloud platform, or a Google cloud platform.

Further, it will be appreciated that the functionality may be implemented in any programming language, for example, html 5, C++TM, JAVATM, and .xml may be used as well as other programming languages which will be known to the skilled person. For example, embodiments of the invention may use one of these programming languages to provide a web-based service.

Referring now to figure 1, this may be thought of as a schematic diagram showing the architecture of a system embodying the invention. This system may be provided as a part of a Next Generation Protocol, NGP, system.

In this specific embodiment, the system comprises three distinct zones: an API environment 103, an application environment 109, and an airport environment 105.

30

Usually, one or more of these zones are in different physical locations. For example, the API environment 103 may be physically located in a particular state, such as California in the United States, while the local airport environment 105 may be located for example in Bohemia in the United States. The specific airline application environment 109, hosting the one more applications 141, 143, 145 may also be in the United States. The application

environment may be communicatively coupled to a departure control system, which may be hosted, for example, in a different region, location or country such as Germany.

In another specific example, the API environment 103 maybe physically located in the Netherlands, while the one or more user devices 107 and associated GUI's running on the devices may be located in Frankfurt, Germany, while the one or more shared devices 108 may be located in Bohemia, United States. The application environment and associated applications 141, 143, 145 may also be located in the United States, while the departure control system or other back end system 102 is located in Germany.

Description of user devices 107, shared devices 108, and local and remote environments

Usually, the airport environment comprises one or more computing devices, 107, 108. These computing devices may be divided in to 2 groups. The first group of computing devices 107, may comprise any one or more of shared workstation or tablet which an airline agent may bring to the airport to perform one or more functions such as check-in or boarding functions. The first group of computing devices may also include smart telephones or tablets or any other portable computing devices which passengers may bring to the airport environment in order to perform the function of printing boarding passes or bag tags or making payments such as payments for overweight baggage and so on. These computing devices will be referred to as user devices 107. In essence, these computing devices 107 provide a way to access shared infrastructure such as a second group of computing devices 108.

The second group of computing devices 108, may comprise any one or more of a printer or scanner or reader, check-in counter device, boarding counter device, kiosk (such as a kiosk for printing a boarding pass or bag tag), bag-drop counter device, security screening device or self-boarding gate device. In other words, the second group of computing devices 108 relate to shared infrastructure computing devices. The scanner or reader is usually configured to read a boarding pass or a bag tag, passport or identity card or other machine readable document. This is usually performed using an optical scan of the boarding pass or bag tag using Optical Character Recognition, OCR algorithms which will be known to the skilled person.

Figure 1 shows an airport environment as an example but of course, it will be appreciated that this zone 105 may be any environment where shared infrastructure may be provided

such as a railway station, a hotel, a convention centre, a cruise ship and so on. This zone 105 will be referred to as a local environment 105.

5 The application environment 109 is usually referred to as a remote zone 109. The application environment may comprise a data center or one or more computer servers used by, for example an airline. Further, the application environment functionality may be provided in a hosted environment.

Description of main functional components

10

The system 100 may comprise any one or more of the following functional components: one or more modules or interfaces 111 for providing one or more services. The modules are usually respectively communicatively coupled to one or more applications 141, 143, 145. Further, each of the modules or interfaces may be communicatively coupled to one or
15 more devices 108. Any of the functional components within the API environment 103 may be referred to as a module for performing one or more different functional operations.

For example, a server or computer 101 may be configured to run an Application Programming Interface, API, in an API environment 103. The computer server is usually
20 communicatively coupled, via wired or wireless transmission means which will be known to the skilled person, to any one or more different functional components, shown in figures 1, 2 and 3 of the drawings.

The application environment 109 and airport environment 105 may be provided by third
25 parties and each of these environments 105 and 109 is usually communicatively coupled to one or more API services through a published interface. As previously mentioned, the application environment 109 usually resides on one or more computers or computer servers.

30 Usually, the local environment 105 is communicatively coupled to the API environment 103 via a wired or wireless communications protocols which will be known to the skilled person. Similarly, the remote environment 109 is usually communicatively coupled to the API environment 103 via a wired or wireless communications protocols which will be known to the skilled person.

35

Description of database 104 and beacon 110

As shown in figure 1 of the drawings, a database 104 may be provided as part of the system. Usually the data associated with the database is stored in a storage means or memory such as read only memory or random access memory. However, it is not essential
5 that the database is located within the API environment. For example, the database may be provided at any location provided it is communicatively coupled to the API Azure environment. The database is usually searched by means of an API 106. The database usually comprises one or more different beacon identifiers such as a UUID and one or more different location identifiers, IDs. An association between each beacon identifier and
10 each location identifier is provided, and the database, its structure and interaction with the other functional components shown in figure 1 will be described in further detail below.

The system usually further comprises one or more beacons 110. Each beacon is usually placed in close proximity to any one or more of the user devices 107 which may be used in
15 the airport environment. For clarity, in figure 1, a single beacon 110 is shown. However, usually a plurality of beacons are provided at different locations. Each beacon is usually associated with a single piece of shared infrastructure 108.

Multiple shared devices 108 may be provided at a specific location. Each shared device
20 usually has a unique identifier, for example a device identifier. The device identifier is usually in the form of an alphanumeric string. One specific example of a device identifier is deviceId: '413dc6c0a03d4d6a9cd2c1=='.
25

Further, in order to distinguish between the different functionality of multiple shared devices
25 108 at a particular location, each shared device 108 may have an associated device type or generic device label definition.

For example, a device type of LSR may indicate a barcode scanner used to scan a boarding pass or bag tag. A device type or label of MSR may indicate that the device is a
30 Magnetic Swipe Reader used to read a credit card, or loyalty card. Other device types or labels may be BTP indicating that the device is a Bag Tag Printer or Boarding Pass Printer, referred to as ATP (Automated Ticketing and Boarding Printer) which indicating that the device is a Boarding Pass Printer. The combination of device type and location identifier
allows a particular device to be uniquely identified in a particular region of the airport.

35

Description of User Session Identification Data and Authentication Services 114

An authentication services module 114 may be provided in the API environment 103. This allows users to subscribe to the system, and also provides subsequent access to the system with a user login and password.

5

Once a user has logged in, a login event is created. This generates a Location Identifier, ID, and user session identifier, ID. The location identifier may be determined by search a database (112) of previously stored location identifiers associated with different users. The location identifier may be selected based on a match between the user login and a matching user login and associated location identifier stored in the database (112). Additional information such as the location (e.g. longitude or latitude coordinates, country, state, or region) from which the user is logging on may also be used to uniquely determine from the database (112) a location identifier for the user.

10

15 Description of published interfaces

One or more of the interfaces or functional components shown in figure 1 of the drawings may be interfaces which are published or made available to 3rd parties outside the API environment 103. For example, the configuration portal 115, Web Proxy service 113, and API services 111 and specific device service interfaces 117 may be thought of as published interfaces. The published interfaces have 2 distinct responsibilities.

20

Firstly, the API's or services 111 provide data exchange between the one or more applications 141, 143, 145 running in the remote environment 109 and one or more devices 107, 108 running at the local airport environment.

25

Secondly, the details related to specific device capabilities and end-user experience is provided via the configuration portal 115 shown in figure 1. The configuration portal 115 may seamlessly integrate API data with the device interface which couples the device services interface 117 to the one or more shared devices 108 in the airport environment. This allows the system to make use of the full capabilities of the devices 108. The configuration portal 115 and associated configuration settings associated with each shared device 108 are described in further detail below.

30

35 Functional description of API's 111: acknowledgement and routing function

The one or more API's 111 provided in the API environment may have two main functions. Firstly, they transmit acknowledgement messages in response to receiving message(s) 121, 122 from the one or more applications 141, 143, 145 in the remote application environment 109. Secondly, they have the function of routing messages to the correct device service within the device services API interface 117. Usually, this is needed because a number of different device services are provided within the device services interface, 117. For example, the services within the device services interface 117 may relate to printing a boarding pass or printing a bag tag or scanning a boarding pass or bag tag or to reading a credit card or loyalty card using a magnetic swipe reader and the like.

Thus, the API service(s) 111 may perform the function of both routing messages to the correct service within the device services interface 117, and also sending an acknowledgement message to acknowledge that a request from one of the applications 141, 143, 145 in the remote application environment has been correctly received by the API service 111.

CUTE Wrapper API 301

An API 301, shown in figure 3 of the drawings, may also be provided and located in the API environment 103. This is referred to as a CUTE Wrapper API. One of the functions of the application 301 is to translate between the different protocols used. Further, the application 301 may also translate commands between the API environment 103 and the remote application environment 109. In addition, the API performs an authentication function to check that messages 122 received from the remote application environment are associated with a genuine user. The CUTE Wrapper API is particularly useful when integrating legacy airline applications for use into the NGP system. However, it is of course optional, and the airline applications may be configured to directly receive messages from the NGP system, within the need from the CUTE Wrapper API 301.

Description of data exchange between functional components

In figure 1, data exchange between different functional components is represented by the arrows labelled 121, 122, 123, 124, 125, 126, 127, 128, and 129. Of course, for clarity purposes, not all of the communications between the different functional components are shown. However, these further details are described in detail below.

In one specific example, the messaging 121,122 between the API services 111 and the respective, and usually associated, applications 141, 143 in the remote application environment shown in figure 1 may be implemented using Java Script Object Notation, JSON™ xml messages. This is a data-interchange format based on Java™ Script programming language. These are described in further detail with reference to figure 3 of the accompanying drawings below. Of course, other messaging protocols known to the skilled person may be used.

Detailed description of beacon placement and functionality

As previously described, the beacon 110 is usually placed in close proximity to the location where one of the user devices 107 may be used. Alternatively, a matrix barcode, such as a one dimensional bar code, a Quick Response, QR, code or 2-D bar code may be used. In this case, a location identifier is encoded within the QR code or within the 2-D bar code. These codes allow information to be encoded within them. This is described in further detail below.

A beacon identifier value may be associated with each beacon. This may be set up with a companion application such as a beacon management tool. The user device 107 may use wireless signals such as Bluetooth to communicate with the beacon 110.

Usually, each of the user devices 107 comprises an application for allowing access to the shared infrastructure. This application, which may be in the form of an API may be executed by the user, airline agent or passenger when they approach the shared infrastructure 108.

The application is usually configured to detect one or more of the beacons 110 by way of wireless communications protocols such as Bluetooth. Once the application has detected a beacon's UUID, this is sent to the API environment 103.

The beacon identifier or UUID data, may, for example, be a 32 digit alpha numeric code. The code may for example be in the format 1 AE18C1 C-6C7B-4AED- B166-4462634DA855 which is associated with a beacon. The API may also return one or more of majorId=14, minorId=2. In another specific example, the API 106 may return one or more of UUID=1 14A4DD8-5B2F-4800-A079-BDCB21392BE9, majorId=1 100, minorId=1292. majorId and minorId may be used to distinguish between beacons in a particular area

having a common UUID. The API 106 may return data associated with one or more beacons.

Description of UUID's stored in database 104 are mapped to location identifiers

5

Within the API environment 103, a Beacon 110 identifier-to-location identifier ID mapping may be performed as a service. Thus, as part of the initial configuration process, a beacon identifier and a location identifier are passed to the API environment. The location identifier may be in the form of an alphanumeric string such as "JFKT5CK01" which indicates that
10 the beacon, and therefore the user device 108 is located at John F Kennedy Airport, Terminal 5, Check-in Desk 01.

A mapping between each beacon identifier and a location identifier is performed, and the association or mapping is stored in the database.

15

Thus, the database comprises at least one beacon identifier associated with a location identifier. This allows a link to be made between the beacon identifier and a user device
107.

20 The database may also include local airport environment map. This allows for a visual representation of the physical location of the beacon(s) 110, as well as the associated user devices 107 which are near each beacon 110.

In one specific embodiment, the database 104 may include data defining an airport map
25 and locations of beacons and associated shared devices 108 within the map.

Further description of Location Identifier

As previously described, the Location Identifier, ID, may be thought of as an association or
30 link between the device communication channel 124 and the GUI communication channel 125 shown in figure 1.

Further, a number of different associations between the communication channel 124 and communication channel 125 and one of the applications 141, 143, 145 running in the
35 remote application environment 109 may be provided. This allows a user to use multiple locations.

As outlined above, the location may be determined with use of a beacon, NFC, or a label. The Location Identifier, ID, may be parsed by a back-end service.

- 5 The description below focusses on further details of the Location Identifier, ID, concept. The location identifier may follow the format of any one of the following examples:

1. BOH-PREPROD-T01-GATE01-WKS-001
2. JFK-T01-GATE03-WKS-002
- 10 3. MIA-ADM-FLR1-CONF1-WKS-001

Example 1

- 15 In this example, the Airport =BOH, Area = preproduction, Terminal = 1, gate = 1, and Work Station = 1.

Example 2

- 20 In this example, the Airport = JFK, Terminal = 1, Gate = 03 and Work Station =2.

Example 3

- 25 In this example, the Airport = MIA, Area = administration, Floor = 1, Conference room = 1 and work station = 001.

- 30 These examples define a relative location or a location which may be at any location within one or more predetermined areas. The location identifiers may define areas, regions or volumes within two dimensional or three dimensional space. The two or three dimensional space may be defined by one or more x, y or z coordinates which are associated with each area or space. The coordinates defining each area or space may be stored in a data base, such as database 112, along with the associated location identifier defining each area or space.

- 35 In the above examples, the location identifier may define different regions. Usually, at least some of the different regions overlap with one or another or are may be contained wholly within another region. Thus, and airport may be thought of as a region 1, an administration

area may be thought of as a sub region 2, and a conference room may be thought of as a sub-region 3 of sub region 2. Sub region 3 may be wholly contained within sub region 2. Similarly, sub region 2 may be wholly contained within sub region 1.

- 5 The location identifier may define the location of a particular device 107 such as a work station as part of a hierarchy. In a specific example, the actual work station may be a kiosk or a bag drop work station of one or more of these.

This hierarchical structure is extremely flexible and provide human readable text format.

- 10 Further, a database of area acronyms and associated explanations of those acronyms may be provided.

- It will be appreciated that the location identifier does not define locations relative to a single point of origin. This is in contrast a coordinate system such as a longitude and latitude coordinate system in which all locations are defined relative to a single point of origin.
- 15 Rather, each location identifier is associated with a predetermined location. A hierarchical tree defining the location relative to each predetermined location is provided. This has the benefit that the location identifier may be interpreted by the skilled person and the hierarchical structure understood without the need to refer to a database of acronyms. This
- 20 allows for the hierarchical structure to be easily expanded as necessary.

For example, suppose a check in kiosk is deployed in Times Square, New York.

- The location identifier may be defined by NYC-TSQ-
- 25

The location identifier may be communicated between different functional components as a text string.

- The string may be searched. The logical structure of the location identifier is usually only traversed when the tree is created. The tree may be viewed by way of a GUI on a workstation. The GUI shows how the location identifier defines a nested structure.
- 30

- Thus, the location identifier usually start with an IATA defined code specifying location such as JFK, LGA, LAX or a well-known abbreviation of a location such as NYC.
- 35

As the hierarchy is built, each step is added to the Location Identifier, ID, which renders it human readable and understandable. This provides a very accurate view of the physical location of the workstation. When the location identifier is defined with sufficient precision such that the workstation is actually located, a marker may be added. The marker may be referred to as a WKS marker and then an identifier may be added which defines the workstation number. This scheme can be used to depict virtually any location in the world.

Description of device type or generic device label to distinguish between different types of shared devices 108

10

If a location ID is associated with multiple shared devices 108, then the device types previously described may be used to distinguish between different devices at a particular location. Alternatively, a unique device identifier may be used to distinguish between different shared devices 108.

15

This may be done by associating one of the shared devices 108 with a particular location identifier and the device type label. Example of device type labels are ATP, BTP, LSR, MSR as previously described.

Thus, each device 108, such as a bag tag printer or a bag tag scanner for example may be identified by its location identifier and device type label. As previously noted, the labels are usually generic, but the combination of location identifier and label provides a way to identify one device from a number of different shared devices 108 which may be at a particular location.

25

The specific way of uniquely determining which shared device 108 a particular a message is sent to may be performed in 2 different ways.

As a first option, the shared device 108 may be uniquely determined based on the location identifier and the device type label, such as ATP, BTP LSR.

As a second option, the shared device 108 is uniquely identified using the beacon UUID which is mapped to the location identifier JFKT5CK01 and label ATP. This means that the location of the shared devices 108 is the same or similar to the location of the user devices 107. The beacon identifier, such as beacon UUID may provide a link or association between the shared device identifier or label and location identifier.

Figure 2 of the drawings shows a schematic diagram of a specific embodiment in which an adapter 201 is provided. This adapter is provided for current devices at the airport 107 which are not capable of connecting to the cloud 203 IoT-Hub directly. Thus, an adapter service is used to allow a legacy device to function as an IoT device. This adapter together with device interface is published to allow device vendors to develop devices that have native IoT support. The adapter 201 shown in figure 2 may also be referred to as a field gateway, FG shown in figure 1 of the drawings.

10 The location ID abstracts the position of a device to a logical placement, e.g. check-in desk, hotel lobby, without knowing knowledge of connected workstations or IT layout. The Location Identifier is described in further detail below.

The message routing from devices to the airline/airport applications and from airline/airport applications to the devices is handled by the unique internal routing mechanisms and Azure routing mechanisms. The routing mechanisms are described in further detail below with reference to figure 3 of the drawings which shows a sequence flow diagram of an embodiment of the invention.

20 The IoT Adapters, Location Abstraction and Capabilities Services deliver a distinctive solution for managing and operating devices on a global scale while bounding the complexity of device hardware, capabilities and message routing within the cloud application.

25 Detailed description of device services interface API 117

A device services interface API, 117 may be provided within the API environment

30 The device services interface API 127 provides an interface with any one or more of the shared devices 108. This allows the services which any one or more of the shared local devices may perform to be listed, and made available for use by any one of the user devices 107.

For example, supposing the shared device 108 is simply a printer coupled to a networked work station. The device services API 117 indicates that the device can perform printing.

Further detail regarding the nature of the printing may be provided by the device services API. For example, it may indicate that the printer is capable of printing a bag tag which can be attached to a passenger's luggage. Similarly, the device services API may indicate that the printer is able to print a boarding pass in a particular format or size or following a particular style sheet or table. For example, a boarding pass printer may print a boarding pass using a PECTAB print language. In this, data to be printed on the boarding pass is formatted according to one or more tables.

In any event, the configuration portal 115 is communicatively coupled to the device services interface 117. This is schematically illustrated with the arrow labelled 128 in figure 1. Thus, the configuration portal 115 is also communicatively coupled to the capability services interface.

Configuration of workstations and associated peripherals

Before describing the sequence flow diagram of figure 3 in detail, the optional configuration of workstations and associated peripheral devices such as bag tag printers or boarding pass printers will be described.

Workstations with peripherals connected to the workstation may be deployed using the following steps. This assumes that the workstation is running for example Windows 10 and has the required device drivers pre-loaded on the image.

After a work station or portable device has started at step 3010, an installation engineer starts a browser and enters an NGP URL to connect to NGP portal. The installer is usually required to enter security credential to start the installation process. The NGP portal provides intuitive GUI to guide the installer to connect and configure peripherals. This process automatically installs and configure all necessary software on the workstation based on a location ID provided by the installer at step 3011. Usually, the NGP Installation Portal GUI requires the Installer to test all peripherals for validation of successful installation. The peripherals may in principle be any shared device 108 such as a boarding pass printer or bag tag printer.

A user then enters a specific URL in the browser running on user device 107 to access the NGP system. Usually, each airline has a different URL to access the system.

Referring now to Figures 1 and 3 of the drawings, the messaging sequence flow will now be described. It will be appreciated that the specific order of the steps is exemplary and that the steps may be performed in a different sequence to that shown in figure 3.

- 5 The following description assumes that the user has previously created an account with the NGP system so that the user has a user name and password stored in the system which allows access to the system. Further, it also assumes that the device 107 is enabled with a browser to connect to the NGP portal, which provides access to the API environment. Usually, the term API environment 103 is used interchangeably with the term NGP portal or
- 10 system. It also assumes that one or more peripheral devices such as a bag tag printer or boarding pass printer have been configured as previously described.

Portable device solution

- 15 In some examples, an airline agent may bring a portable computing device such as a tablet to an airport counter, kiosk, or Bag Drop location to perform for example a check-in or boarding pass issuing functionality. Similarly passengers using smart phones/tablets can approach kiosks or other locations to print boarding pass, bag tags and make payments directly from their own devices. Passenger will usually run a particular airline application to
- 20 perform these functions. This allows a passenger to have seamless experience at the airport.

As outlined above, the beacons, using for example NFC technology, allow a device 107 to associate with shared devices 108 at the counters and inside the kiosks and the bag drops.

- 25 The association of particular beacons with shared computing devices, or in other words, location identifiers, ID's associated with shared computing devices 108 has been previously described above.

- 30 The Location Identifier, ID links, or associates the 2 channels 124, 125. This informs the platform about which printer in the local airport environment 107 the application 141, 143, 145 in the remote environment needs to communicate with.

- When a user logs-in from tablet or other device 107 a predetermined Location Identifier is
- 35 sent to the API environment 103. Alternatively, when the user logs-in, they may manually select their location. The location may be determined using a beacon or using Near Field

Communication, NFC, or a QR label, as outlined above. In this way, airline agents may bring their own tablets and simply approach airport counters, kiosks, Bag Drops and other locations to perform check-in and boarding functions.

5 The tablet may be associated with one of the devices at the counters (at for example a kiosk or bag drop) using for example a beacon or NFC. This allows the device to receive a Location Identifier, ID, and for the portable device to pass the Location Identifier on to the API environment 103.

10 Thus, a user may bring a portable computing device 107 to the local airport environment 105 to access the API environment 103.

The user launches an application on the device 107 which detects the beacon 110 which is nearby the user using wireless communications protocols, such as NFC to detect a beacon
15 identifier, such as UUID.

The application running on user device 107 may wirelessly send a request to the search API 106 located in the API environment. The request includes the UUID, and the request includes a command which instructs the API 106 to search the database 104 for beacon
20 identifiers stored in the database which match the beacon identifier detected by the API running on the user device 107.

Once the API 107 has determined a match between the UUID identifier associated with the detected beacon and a beacon identifier stored in the database, then the API 106 searches
25 the database for location data or in other words a location identifier, ID associated with the matching beacon identifier stored in the database. The particular format of the location identifier, ID, is described in further detail below.

Fixed counter solution

30

As an alternative to the portable device solution, the user may use a work station, also labelled as 107 in figure 1, to access the API environment. This is referred to as a fixed counter solution. In this example, the location ID is passed to the airline's back end service transparently. The user does not have to take any action to obtain the location ID.

35

Thus the fixed counter solution may perform the following steps:

1. When the fixed location workstation is installed and the Field Gateway is deployed the workstation is given an identity. Usually, this identity is the location ID.
 2. When user logs in to the NGP system to access his/her applications, the location ID is
5 passed as part of the login credentials.
 3. The NGP system may then dynamically build a menu with application icons that is displayed to the user where each icon is a URL associated to the backend airlines application services 141, 143, 145. The URL has three associated parameters; LocationID, UserSessionID and NGP URL.
10
- These parameters provide all the information needed by the airline's backend application services 141, 143, 145 to subscribe to the location needed by the user logging in.

Detailed sequence flow steps and messages

- 15 Unless indicated otherwise, the different functional components shown in figures 1 and 3 may be implemented using an API call, such as a Representational State Transfer, REST, API call using an http protocol.
- 20 Thus, data within the messages shown in figure 3 is usually in the format of an alpha-numeric string and an associated field defining the type of data, which may also be in an alpha-numeric string format. Further, the different functional components shown within the API environment 103 and application environment 109 may be implemented as different modules which are coupled to one another to exchange data as necessary between the
25 different modules.
- Referring now once again to the sequence flow diagram of figure 3, the user is prompted to enter a user name or user ID and password (UserLogin) to login to the NGP system. A user login message 3012 is therefore sent from the user device 107 to the API environment 103.
- 30 The user login prompt is usually in response to the user entering a specific URL in the browser, as previously described.
- If the NGP API environment is provided as part of a cloud service, then any authentication steps required by the cloud service provider may be used. Usually, a number of users are
35 provided with access to the system and groups of users may be defined as belonging to particular associations or companies, such as a particular airline.

In order to access the particular URL the user device may be provided with a security certificate. The security certificate may be provided over a separate channel, and the certificate may be revoked at any point. Access to the NGP system is usually not allowed
5 unless the appropriate security certificate has been provided.

The Authentication services 114 then authenticates the user based on the credentials entered by the user.

10 After user login, the configuration portal 115 or authentication services application 114 determines whether the user is associated with a particular group of users, such as those belonging to a particular airline. This may be performed by searching a database 112 of logon credentials which may a particular company or group identifier associated with them, such as an airline identifier.

15 If the user is using a portable device, the location of the portable device may be determined at this stage. This may be performed by the application running on the client tablet or device 107 instructing a scanner or reader associated with the device to scan for or read a beacon identifier, as previously described, for example using wireless Near Field
20 Communication protocols. Alternatively, the application installed on the mobile device may be used in conjunction with reading means such as a camera to read or scan a QR bar code. The beacon or QR bar code is usually placed in predetermined positions within the airport where a user may wish to user shared infrastructure. In the case of the QR bar code, the bar code comprises data defining the location ID encoded within it. Alternatively,
25 the user may simply enter the location identifier manually once he is prompted to do so.

If the mobile device reads a beacon identifier, the beacon identifier is sent to the API environment from the user device 107 via wired or wireless connection. Then, the application 106 searches the database 104 to locate a beacon identifier corresponding to
30 or matching the beacon identifier read from the beacon 110. The API 106 then determines a location identifier stored in the database 104 which is associated with the location identifier matching the beacon. Thus, the API 106 is able to determine a location identifier associated with the beacon. Usually, all of the functional components shown in figure 1 of the drawings are able to access a location identifier, ID associated with a particular beacon
35 identifier when needed. The determined location ID may then be transmitted back to the user device 107.

Thus, the NGP system and usually, the API 106 running the application environment receives the location ID from the fixed work station, or the API 106 running within the API environment 103 determines the location ID by searching the database 104 for a location
5 identifier which matches a particular beacon identifier. This is usually in response to the API 106 receiving the beacon identifier from the user device 107.

In either case, an association between the location ID and the particular user device 107 accessing the shared infrastructure 108 is made. The user device 107 may have an
10 associated identifier.

After the user has successfully logged in to the API environment 103, at step 3012, a login event message **3013** is sent from the Authentication services interface 114 within the NGP portal to the CUTE_Wrapper API 301. Usually, the login event message 3013 comprises
15 data identifying a user location in the form of the location ID and a user session identifier, referred to as a user_session_ID. The user session ID may be generated by the authentication services API, 114. As will be known to the skilled person, the user session ID identifies a user session and may be an alphanumeric string.

20 The login event message may comprise an optional airline ID or user group identifier, ID. A region identifier, such as "US", "East-US", "West-US", "Netherlands", "Ireland", and "Asia" may also be used. This is useful if for example multiple different instances of the API environment need to be provided in different locations, and thus allows a global solution to be provided. The data within the event message may be in an alphanumeric string format.

25 In one specific example, the user_session_ID incorporates data defining a user and data defining association or group with which the user is associated. For example, the data defining the association may be a string such as "BA" or "AA" which may define an airline as "British AirwaysTM" or "American AirlinesTM" respectively. Other associations, for
30 example such as ground handler associations may be linked to the user. Usually, the URL used to access the NGP system is used to map, associate or provide a connection between the location ID, user session ID and the airline ID.

At step **3014**, the user is provided with a menu, referred to as an Application Menu, based
35 on the logon credentials and the determined location ID. This may be done by one of the API's within the API environment 103 (such as the authentication services API 114)

5 sending a call to the user device 107. Usually, the application menu is provided as a URL (which may be an alpha-numeric string) which points to the corresponding URL of the application 141, 143, 145 in the remote airline application environment 109. Thus, the menu may provide functionality which allows the user to perform one or more different functions, using the user device, at the particular local airport environment. Two specific examples of functions which may be performed by the user using the user devices at the local airport environment 105 may be the printing of a bag tag or a boarding pass using one or more shared devices 108.

10 Thus, using one of the user devices 107, a user is able to click on one of the menu items, and this allows connectivity to the application in the remote airline environment. A CITRIX™ application may be used to perform this step, although other applications may be used to remotely launch one of the applications 141, 143, 145 from one of the devices 107 in the local airport environment 105.

15 The step of displaying a menu of items and functionality to allow the remote launch of one of the applications 141, 143, 145 may be performed using an application in the API environment 103 (for example using one of the API's 111), which may be referred to as an NGP portal application to search a database 112 of stored preconfigured settings defining the types of applications available to the user at the particular location. This application may first authenticate a user and then determine what applications should be available to the user when logging on using the client device 107 at a particular local environment 105.

25 Thus, the NGP portal application 103 is able to determine what applications have been previously configured for this user, based on the location. In a similar manner, an airline may remove applications for user based on the user id and location.

30 This is analogous to the way in which specific devices, such as a bag tag printer or boarding pass printer may initially be configured, at step 3011 for user at a specific location, for example using the configuration portal 115. This allows specific devices 108 in the local airport environment to be configured for specific users and for those devices and services to be published.

35 An airline may configure the desired applications 141, 143, 145 which are available to a specific user at a specific location by logging on to the configuration portal 115. The database 112 associated with the configuration portal API 115 may store settings which

define the type of application a particular user, identified by their user id has available when logging on at that specific location. For example, a user may have applications for printing a boarding pass or printing a bag tag configured to be available when they log on. This may be performed based on a user ID and location.

5

Thus, exemplary applications may be a boarding pass application or bag tag application which allows an agent or passenger to print or process a boarding pass or bag tag.

The application menu allows the user to select one of the available applications 141, 143, 145 in the remote application environment 109 (LH_Application). This may be performed by way of a published and subscribed communication between the NGP API system 103 and a CUTE Wrapper application 301, shown in figure 3 of the drawings.

Usually, the CUTE_Wrapper application is located in the remote application environment 109. The CUTE Wrapper Client application 301 may act as an intermediary between an airline's legacy applications 131, 134, 145 and the applications 111 in the API environment.

One of the functions of the application 301 is to translate between the different protocols used. Further the application 301 may also translate commands between the API environment 103 and the remote application environment 109. Thus, the CUTE wrapper application 301 may be optional depending upon the application type being used in the remote airline environment. Nevertheless, the core data exchanged between the NGP API environment 103 and the application in the remote airline environment 109 is usually the same irrespective of whether a CUTE wrapper application is used.

25

In response to the user selecting one of the applications 141, 143, 145 indicated in the menu, the user device 107 then communicates with one of the applications 141, 143, 145 in the remote application environment 109 to start one of the applications 141, 143, 145 using message 3015. As outlined above, the step **3015** is performed using a link to the application in the remote airline environment 109. Thus, one of the applications 141,143,145 in the remote airport environment is launched based on the information received in the message 3015, such as the client or user identifier.

It should be noted that usually, the link or message 3015 does not allow for any associated parameters to be sent, other than a URL. Thus, at step 3020, when the specific application 141, 143, 145 in the remote airline environment 109 is started using the URL, one of the

remote airline applications also usually makes a local call to the local CITRIX environment to determine a client identifier which may identify the device 107 which started a particular user session.

- 5 Thus, when the CUTE wrapper functionality is used, usually, the previously determined location ID is not sent to the application 141 in the remote application environment.

Rather, when one of the applications 141, 143, 145 in the remote environment 109 is launched, the application instance starts a port forward. This allows one of the applications
10 141 to receive a client ID because the local CITRIX environment passes the client identifier to the application 141 running in the remote application environment. This is usually sent from the user device 107 to the application 141 via the CITRIX interface in response to the user device 107 receiving such a request from the application or CITRIX interface in the remote application environment 109.

15 For example, a client ID may identify a particular user by name, and identify the type of device being used to launch the remote application 141, 143, 145. Thus, the client ID may be in the form of "NAME_TABLET_1". The client or user device 107 communicates the client ID to the CITRIX environment (which is usually within the remote application
20 environment), for example by communication means 129. The previously described user login is usually associated with a particular client identifier, IDs.

At step 3030, the application 141 sends a Get Device List message 3030 to the CUTE wrapper API 301. The device list message includes the determined client ID, usually as an
25 alphanumeric string.

The CUTE Wrapper API 301 then performs a mapping of the received client ID to the previously determined location ID. Usually, the received client ID is uniquely associated with a particular user and hence with a device used by that user.
30 The Get Device List message 3030 sent by one of the applications 141, 143, 145 in the remote application environment to the cute wrapper API 301 instructs the cute wrapper API to provide a device list associated with the particular application 141 which has been launched.

35 Usually, the message 3030 includes the determined client ID and data defining the type of document to be processed, such as a boarding pass or bag tag. Thus, the message 3030

may comprise text such as alpha-numeric text in the form of "BP" or "BT" which indicates that a boarding pass or bag tag respectively are to be processed.

5 Once the CUTE wrapper API 301 receives the message 3030, it examines the message contents to determine the client ID and the type of document required. Further, the CUTE wrapper API 301 also has knowledge of the user session ID which is associated with that particular location ID, because the user session ID may be stored in a storage means within the API environment for use by the cute wrapper API 301 .

10 CUTE Function of mapping of client ID to location ID.

The CUTE Wrapper API may perform a client ID to location ID mapping.

15 To perform the mapping, the CUTE Wrapper API 301 uses the information received in the login event message 3013. Thus, the Cute Wrapper may use the location ID and session identifier received in message 3013 to map the received client ID to an associated location ID.

20 This may be done by searching a database (such as database 112 associated with the configuration portal) for a client ID which matches the client ID received in message 3030. The matching client ID stored in the database is associated with a location ID or/and user session ID for a particular user. Similarly, a mapping of client ID to location ID may be performed for fixed the work station solution.

25 Thus, the CUTE Wrapper API 301 translates the client ID (which may be associated with a particular user or device) received in message 3030 into a location ID (which may be associated with the particular user or device).

30 At step 3040 the CUTE wrapper API 301 sends a location subscribe message 3040 to the configuration portal 115 in the API environment 103 to subscribe to a particular location via one of the API services 111, using the location ID determined by the CUTE Wrapper API 301. Usually the location subscribe message comprises parameters defining the location ID and User Session ID.

The API configuration portal service 115 may transmit an acknowledgement in response to receiving the location subscribe message 3040, although this message is not shown in figure 3 because of its optional nature.

- 5 Step 3040 is performed because usually an airline, and hence users registered to use the system, need to subscribe to a location before device operation can be requested. The following should be noted:
- Subscription is implicitly linked to a user session. In other words, during the configuration process, when an airline application is subscribed to or associated with, a location, it is assumed that an airline agent is using the application 141 in question. Hence Subscription requests are usually mandated to have a corresponding user session ID.
 - One user can usually ONLY have one active subscription per location; however, the user can initiate multiple subscriptions across locations through the airline application
 - 15 • One airline can have multiple users or agents subscribe to a location through the airline application(s) 141, 143, 145.
 - Subscription is controlled by airline having access to the location. A scheduler may be used to enforce this based on one or more rules.
- 20 The location subscribe message 3040 usually comprises the location ID and User session ID information and optionally an Airline ID parameter. As previously described, the Location ID parameter defines the location identifier of the workstation or portable device 107 being used, the user session ID defines the logged in user session ID, the Airline ID may define an airline codes, such as an IATA airline code and there are usually defined by alpha-
- 25 numeric strings. Optionally, a time stamp may also be included in the sample JSON location subscribe request message 3040 shown below:

Parameter	Type	Optional / Mandatory	Description
AirlineId	string	Mandatory	IATA Airline code
LocationId	String	Mandatory	Location Id of the workstation
ConnectionId	String	Mandatory	GUID for Subscribe calls to NGP
UserSessionId	string	Mandatory	Logged in User session id
Timestamp	DateTime	Mandatory	Airline service Timestamp in UTC

Sample JSON Request Format

```
{
  "AirlineId" : "LH",
  "LocationId" : "LAX-T1-GateB21-WK5-001",
  "UserSessionId" : "372d4802-8ede-47a6-aa73-5cb2850a3d2c",
  "Timestamp" : "2016-08-10T08:43:01.511Z",
```

```
"ConnectionId" : "8B5FFA7E-9045-414B-B44B-426FE21C5F51"
```

Table 1: Exemplary structure of the location subscribe message 3040.

The API service 111 in the NGP API environment 103 receives the message 3040 and communicates with the device services interface 117 via messages 131 and 132 to determine the particular devices associated with a particular location as well as the associated capabilities of each device. Information may be included in the message which allows it to be routed to one of the API's 111 shown in figure 1, if more than 1 API service 111 is provided.

Thus, the device services interface API 117 and configuration portal 115 communicate with one of the API services 111 in the API 103 environment to determine a list of devices associated with a particular location ID, and their associated capabilities.

This may be done by searching the database 112 using a particular application. The database 112 includes details of the devices 108 which are associated with the particular user location or more precisely, the location identifier.

The device capabilities are returned to the CUTE wrapper API 301, which is usually part of the API environment 103.

The CUTE wrapper API 301 translates the received device capabilities in to a JSON message type, shown as 121, and 122 in figure 1 and message 305 in figure 3.

An exemplary JSON location subscribed response message 3050 is shown below:

Parameter	Type	Optional / Mandatory	Description
AirlineId	string	Mandatory	IATA Airline code
LocationId	string	Mandatory	Location Id of the workstation
Timestamp	DateTime	Mandatory	
SubscriptionId	string	Mandatory	Unique identifier for each subscriber
MessageId	String	Mandatory	MessageId from the Request (CorrelationId)
SubscriptionChannel	string	Mandatory	Service Bus URI
AuthenticationToken	string	Mandatory	Token for accessing Service Bus.
LocationCapabilities	object	Conditional	This element represents the currently configured capabilities of the device. Only currently configured capabilities will be returned as part of the response
ConnectionId	GUID	Mandatory	ConnectionId for the subscribe call
Error	Object	Conditional	Contains error details if interface call

			status is 'Error'
Code	String	Mandatory	Error Code
Status	string	Mandatory	If success it will give Success else Error
Description	String	Mandatory	Error description detail

Sample JSON Response Format – On Success

```
{
  "AirlineId" : "LH",
  "LocationId" : "JFK-T1-Gate1-WKS-001",
  "Timestamp" : "2016-08-10T08:45:01.511Z",
  "Status" : "Success",
  "SubscriptionId" : "53DE9585-2148-4E66-B5DE-03686F140363",
  "MessageId" : "F95DC8D9-FF11-4983-A833-4DC6F64512F7",
  "SubscriptionChannel" : "<Service bus connection string>",
  "AuthenticationToken" : "3A70ACCD-1181-4DA6-9DD0-3FED1BC408F6",
  "ConnectionId" : "8B5FFA7E-9045-414B-B44B-426FE21C5F51",
  "LocationCapabilities" : {
    "ReadBoardingPass" : {
      "LSR1" : {
        "Status" : "Online",
        "Locator" : "JFK-T1-Gate1-WKS-001-LSR1",
        "errorCode" : ""
      },
      "BGR1-LSR" : {
        "Status" : "Online",
        "Locator" : "JFK-T1-Gate1-WKS-001-BGR1-LSR",
        "errorCode" : ""
      },
      "LSR3" : {
        "Status" : "Online",
        "Locator" : "JFK-T1-Gate1-WKS-001-LSR3",
        "errorCode" : ""
      }
    },
    "ReadBagTag" : {
      "LSR2" : {
        "Status" : "Online",
        "Locator" : "JFK-T1-Gate1-WKS-001-LSR2",
        "errorCode" : ""
      },
      "LSR4" : {
        "Status" : "Online",
        "Locator" : "JFK-T1-Gate1-WKS-001-LSR4",
        "errorCode" : ""
      }
    },
    "ReadMagneticCard" : {
      "MSR1" : {
        "Status" : "Online",
        "Locator" : "JFK-T1-Gate1-WKS-001-MSR1",
        "errorCode" : ""
      },
      "BGR1-MSR" : {
        "Status" : "Online",
        "Locator" : "JFK-T1-Gate1-WKS-001-BGR1-MSR",
        "errorCode" : ""
      },
      "MSR2" : {
        "Capability" : "MagneticCard",
        "Locator" : "JFK-T1-Gate1-WKS-001-MSR2",
        "Status" : "Online",
        "errorCode" : ""
      }
    },
    "ReadTravelDocument" : {
      "OCR1" : {
        "MR2" : {
          "Status" : "Online",
          "Locator" : "JFK-T1-Gate1-WKS-001-OCR1",
          "errorCode" : ""
        }
      },
      "FullPage" : {

```

```

        "Status" : "Online",
        "errorCode" : ""
    },
    "ImageOnChip" : {
        "Status" : "Online",
        "errorCode" : ""
    }
},
"BGR1-OCR" : {
    "MRZ" : {
        "Status" : "Online",
        "Locator" : "JFK-T1-Gate1-WKS-001-BGR1-OCR",
        "errorCode" : ""
    },
    "FullPage" : {
        "Status" : "Online",
        "errorCode" : ""
    },
    "ImageOnChip" : {
        "Status" : "Online",
        "errorCode" : ""
    }
},
"PrintBoardingPass" : {
    "ATB" : {
        "Status" : "Online",
        "Locator" : "JFK-T1-Gate1-WKS-001-ATB",
        "mediaStatus" : "OutOfStock,LowStock etc.,",
        "errorCode" : ""
    }
},
"PrintBagTag" : {
    "BTP" : {
        "Status" : "Online",
        "Locator" : "JFK-T1-Gate1-WKS-001-BTP",
        "mediaStatus" : "OutOfStock,LowStock etc.,",
        "errorCode" : ""
    }
},
"PrintDocument" : {
    "DCP" : {
        "Status" : "Online",
        "Locator" : "JFK-T1-Gate1-WKS-001-DCP",
        "mediaStatus" : "OutOfStock,LowStock etc.,",
        "errorCode" : ""
    }
},
"Gate" : {
    "BGR1-Gate" : {
        "Status" : "Online",
        "Locator" : "JFK-T1-Gate1-WKS-001-BGR1-Gate",
        "errorCode" : ""
    }
}
}

```

Table 2: An exemplary JSON location subscribe response message 3050.

- Usually the device capabilities response message 3050 defines the type of shared devices
5 available such as boarding pass reader (BPR), Bag Tag Printer, (BTP), Boarding Pass
Printer (ATB), and each device has an associated location ID.

The cute wrapper API 301 then uses the information received in response message 3050 to produce a device list message 3060 which defines the devices available at a specific location.

- 5 The device list message 3060 may comprise data defining the type of document to be printed or more usually the type of printer required to print a document type. For example, ATP may indicate that a boarding pass printer is required to print a boarding pass. BTP may indicate that a bag tag printer is required to print a bag tag printer. LSR may indicate that a boarding pass reader is required to read a boarding pass.

10

Thus, the application running in the remote airline environment 109 is able to receive a list of available devices in the remote location. This list of available devices is sent to the via communication means 129, or 123, or 125, for example via the web proxy functionality 113 within the API environment. The user is able to select, using the user device 107 one of the

15 available devices to print a particular document type.

15

- In response to the user selecting one of the devices to print a particular document type, the application 141 in the remote environment then sends an open device(s) message 3070 to the CUTE Wrapper application 301 to open one of devices in the device list. If only one
- 20 device is returned in the device list message 3060, then the CUTE Wrapper API 301 generates a single PM Handle associated with the desired device. Usually, the PM Handle uniquely identifies a particular device, within a particular user session.

20

- The Cute Wrapper 301 API 301 returns a PMHandle parameter to the application 141 in the remote application environment 109.
- 25

25

If the device list message 3060 identifies more than one device 108, then usually a different PM Handle parameter is generated for each different device, and usually, each parameter is unique to a particular session.

30

Thus, each device request coming from **LH_APP** 109 is managed as a separate session that is identified by the PM Handle.

35

Message 3070 may be in the form of an XSPMOpen Call for each device based on the device configuration list received (3060). This creates session with device, returns PMHandle. The elements of the call may include any one or more of:

PMRET PMENTRY XSPMOpen (PSZ DevName, PPMHANDLE PPMHandle, ULONG
OpenOption, PSZ AirlineID, SHORT DataWaitTime, ULONG Reserved).

- 5 The CUTE Wrapper API 301 usually creates a PM handle which may be unique to a
specific session. The PM handle may uniquely identify one of the shared devices 108. The
PM Handle is usually returned to the remote API 109 using message 3080.

The message 3080 is usually sent in response to the XSPMOpen call.

- 10 The message may comprise any one or more of the following code elements:
PMSaveHandle, ChangedDataFlag, RequestType, Length, CRC, SequenceNumber,
AppPMHandle, SaveAppBuffer, ChangedDataFlag, ActivityFlag, NotifySem, IPCHandle,
AppBufferAddr, Command, PMHandle, ReturnCode, Status, LocalFlags, Version,
DeviceName, AirlineID, UserName, OpenOption, WksName, ExtStatus,
15 DevDwnFlushTime, DataWaitTime, Reserved

CUTE Functionality of mapping specific PM Handle to device Identifier, ID

- 20 When handling a specific print request, the CUTE Wrapper API 301 includes functionality
to translate the PM Handle defining the particular device which an application 141 is
configured to use, in to a device Identifier ID. In once specific example, the device ID may
comprise a determined location ID and an associated label. The mapping may be
performed by comparing a stored PM handle associated with a particular device, with
stored data defining a location ID and device label.

- 25 As outlined above, message flows 3030, 3060, 3070, 3080 may form part of a single user
session. Thus, the stored PM handle(s) are usually updated each time a new user session
is initiated.

- 30 Messages 3081 and 3082 are schematic in the sense that they show that the subsequent
steps below usually only occur in response to a specific request from the user device 107
to print a specific boarding pass or bag tag for a passenger, or to read a specific passenger
boarding pass. Thus, the subsequent steps may be initiated by a user requesting a specific
action to take place.

35

Messages 3083 are also schematic and show how the application running in the remote airline environment may log in to a remote reservations or departure control system. This is optional as any passenger data, such as PNR data associated with a specific passenger, may be stored within the system 100.

5

Example of printing a boarding pass or bag tag

The following example focuses on the specific example of an agent or passenger using an application running on a device 107 to perform the function of printing a boarding pass or a bag tag at a shared device 108 using an application 141, 143, 145 running in a remote application environment 109 which communicates with the local airport environment 105 via the API environment 103.

10

This assumes that certain passenger data, such as a particular passenger's name has been read, from for example a passport or otherwise entered into an application running on one of the user devices.

15

This information allows a reservations or departure control system, DCS 102 to uniquely identify a passenger's booking and to identify the data to send back to application 141, 143, or 145.

20

Usually in order to uniquely identify a particular booking, the DCS 102 uses the combination of the a credit card number used to make the booking and the passenger's name.

25

For example, the first four and last six digits of a credit card number as well as the associated name may be used to identify a particular booking. Alternatively, passport data, such as a name and date of birth may be used to uniquely identifier a passenger's reservation. Further, a reservation locator such as a reference number may be used to uniquely identify a passenger's reservation.

30

Once a particular passenger's reservation has been identified in the back end DCS 102, this allows data associated with the particular passenger's PNR to be determined. Thus, the system is able to determine which airport the passenger is flying to using an airport identifier, the time of flight, the flight number and seat issued for example. This data allows a boarding pass to be issued for a particular passenger.

35

Further, if the passenger has checked-in baggage, then the DCS creates an identifier in the form of a Licence Plate Number, LPN for that baggage. The DCS returns the baggage information, airport identifier, and flight number and any associated or linked LPN for a
5 baggage to the airline application environment 109.

Thus, the remote application 141, 143, 145 may retrieve a Passenger Name Record, PNR reservation stored in a database. This is usually created when a passenger's booking is created. As a large number of PNR's may be stored in the database, each PNR is identified
10 by a record locator.

Usually, each PNR comprises any one or more of a passenger's name, ticket details such as a ticket number, an itinerary of at least one segment of a journey, and the name of the person providing the information or making the booking. The itinerary may be defined by a
15 departure airport code (such as New York, NYC) (an arrival airport code (such as London Heathrow, LHR), a scheduled departure date and time, and a scheduled arrival date and time.

This allows a boarding pass or bag tag to be issued by a departure control system, for
20 example using scheduled departure flight time and departure airport location.

It will be appreciated that bag tags and boarding passes may be defined in IATA RPS documents such as IATA Resolutions and RPs (Recommended Practices) such Baggage Tag IATA Resolution 740 and RP1740a, and Boarding Pass IATA Resolution 722e and
25 RP1723.

A confirmation is usually provided to the GUI running on user device 107 that a particular passenger record has been located. Further, the data retrieved from the departure control system 102 is returned to one of the applications 141 in the application environment. The
30 API service 111 provides an acknowledgement to one of the applications 141 that the data has been successfully received and performs a routing function to route the data to the correct service within the device service interface.

At step 3090 the particular application 141, selected for use by the user using the user
35 device 107, sends a print boarding pass or bag tag message 3090. This may be done

using XSPMAPI messaging/communications. This defines libraries and communications used by legacy applications.

5 Usually, the data included within the print boarding pass or bag tag message 3090 is based on an AEA format.

10 Usually, the message 3090 defines the type of operation to be performed, such as print a boarding pass or bag tag. Further, the message comprises data allowing the boarding pass or bag tag to be printed. Usually, this data comprises a passenger name, but may comprise any one or more of the information outlined above with reference to defining a boarding pass or bag tag.

15 Usually, the message 3090 for printing a boarding pass or bag tag uses a legacy protocol based on PECTAB to provide a layout for the boarding pass and bag tag. Message 3090 is sent using TCP/IP socket communication based on C-language structure.

20 The payload structure of the message includes data elements which are necessary to print a boarding pass or a bag tag. For example, the message may include passenger name, flight number, gate and seat number in an alpha-numeric format. The message is mapped to a PECTAB template. The data message 3090 is structured in such a way that fields do not need to be identified. The message may include a field defining the particular PECTAB template which should be used.

25 Message 3090 may be in the form of an XSPMWrite call. The call may include details of the document to be printed, such as a boarding pass or a bag tag. The call may include one or more commands, such as Association of European Airline Commands such as PMRET PMENTRY XSPMWrite (PMHANDLE PMHandle, PPMDATABUFFER PPMBuf, ULONG WriteOption, HEV Semaphore, ULONG Reserved) which will be known to the skilled person.

30 The CUTE wrapper API then translates message 3090 in to a format which is suitable for processing by the NGP system to generate message 3100.

35 The message 3100 is based on an html template, boarding pass or bag tag data and a template and the CUTE Wrapper API 301 generates for example a print image message 3100.

Message 3100 is usually based on JSON using key value pairs and is communicated using a web API. The cute wrapper analyses message 3090 to identify particular fields such as fields defining gate number or seat and is able to distinguish between these fields.

5

The cute wrapper API 301 shown in figure 3 maps data from the legacy protocol of message 3090 to the protocol of message 3100. In other words, cute wrapper API 301 translates message 3090 into key value pairs, and may also add information stored by the system 103. The cute wrapper API transforms message 3090 by using an html template for layout of boarding pass for example.

10

The cute wrapper service 301 then creates a print boarding pass or bag tag message 3100 which is sent to the API environment 103, for example using a JSON message. This may be thought of as a translation of a legacy printing command to the new NGP print command and file.

15

An exemplary format of the print BP/BT message 3100 is given below:

PrintDocumentRQ:

20

Parameter	Type	Optional / Mandatory	Description
AirlineId	string	Mandatory	IATA Airline code
LocationId	string	Mandatory	Location Id of the workstation
Locator	String	Mandatory	Device & capability locator FQN
SubscriptionId	string	Mandatory	Unique identifier for each subscriber
TransactionId	String	Mandatory	Unique identifier for airline to track multiple requests under a single business transaction
Timestamp	Datetime	Mandatory	
DocumentType	String	Mandatory	Possible values are: • BagTag, • BoardingPass • BoardingReceipt, • CustomReceipt
TemplateId	String	Mandatory	ID of the template to be used for printing
Params	Object	Mandatory	Contains Key value pairs

Sample JSON Request Format:

```
{
  "AirlineId" : "LH",
  "LocationId" : "LAX-T1-GateB21-WKS-001",
  "SubscriptionId" : "53DE9585-2148-4E66-B5DE-03686F140363",
  "Locator" : "JFK-T1-Gate1-WKS-001-BTP",
  "Timestamp" : "2016-08-12T08:35:49",
  "DocumentType" : "BagTag",
  "TemplateId" : "70CF33E2-B27F-4759-95D6-F061FF932630",
  "Params" : {}
}
```

```

    "TransactionId" : " 868A42EF-EAD2-492D-95C7-FE0011BF98D8",
    "Params" : {
      "Label1" : "Airline",
      "Label1_Value" : "LH",
      "Label2" : "Passenger Name",
      "Label2_Value" : "John",
      "Label3" : "Flight Number",
      "Label3_Value" : "LH117",
      "Label4" : "Departure",
      "Label4_Value" : "LAX"
    }
  }

```

Thus, it will be appreciated that the message 3100 generated by the cute wrapper API may comprise a location identifier, ID (LocationId) and a device label. As previously described, the location identifier may comprise alpha-numeric data such as "LAX-T1-GateB21-WKS-001" or "JFK-T01-GATE03-WKS-002". In the exemplary print message 3100 shown above, the device label is included in the "locator" field. From this, it can be seen that the shared device printer 108 is in fact a bag tag printer, BTP. However, a separate device label field and associated value may be provided in the message 3100 as for example key value pairs. Further the message 3100 may comprise any one or more of the fields shown in the above messages, for example, any of the data required to print a bag tag or boardingpass.

An exemplary print document acknowledge message 3130 is given below. The acknowledgement message 3130 may be sent by one of the applications within the API environment 103 to the cuter wrapper API 301:

PrintDocumentAck:

Parameter	Type	Optional / Mandatory	Description
AirlineId	<i>string</i>	Mandatory	IATA Airline code
LocationId	<i>string</i>	Mandatory	Location Id of the workstation
Locator	<i>String</i>	Mandatory	Device & capability locator FQN
SubscriptionId	<i>string</i>	Mandatory	Unique identifier for each subscriber
MessageId	<i>String</i>	Mandatory	Platform generated MessageId
TransactionId	<i>String</i>	Mandatory	Unique identifier for airline to track multiple requests under a single business transaction
Timestamp	<i>Datetime</i>	Mandatory	

Sample JSON Format:

```

{
  "AirlineId" : "LH",
  "LocationId" : "LAX-T1-GateB21-WKS-001",
  "SubscriptionId" : "53DE9585-2148-4E66-B5DE-03686F140363",
  "Timestamp" : "2016-08-12T08:35:49",
  "MessageId" : "F95DC8D9-FF11-4983-A833-4DC6F64512F7",
  "TransactionId" : "868A42EF-EAD2-492D-95C7-FE0011BF98D8"
}

```

An exemplary document print request message 3110 generated by the one of the API's 131, 132, 117 within the API environment 103 is shown below. Message 3110 is generated based on the information received in message 3100 by one of the applications within the API environment 103. In the example message 3110 a unique device Id is provided which allows a particular device to be uniquely identified by the field "DeviceId". Data associated with the print message 3110 is also included below as "CommandData" and may include any one or more of the data included in message 3100 required in order to print or process the document in question, for example to print the boarding pass or bag tag. The combination of the location identifier, ID and device label may be used to uniquely identify a particular device to which the print document request should be sent.

Document Print Request:

Parameter	Type	Optional/Mandatory	Description
CommandType	String	Mandatory	Print
Command	string	Mandatory	Print, Config, ConfigPrint
TimeStamp	DateTime	Mandatory	Time in UTC
DeviceId	String	Mandatory	IoT Hub DeviceId
CommandData	String	Mandatory	Key/Value Pair, FileData

Exemplary JSON Request Format:

```

5  "deviceCommand": {
      commandType: 'Print',
      command: 'Print',
      timeStamp: '2016-08-11T01:01:43+00:00'
      deviceId: '413dc6c0a03d4d6a9cd2c1==',
      commandData {
10         "File": <FileData>
      }
    }
  }

```

Exemplary JSON Request Format for Configuration:

```

15  "deviceCommand": {
      commandType: 'Print',
      command: 'Config',
      deviceId: '413dc6c0a03d4d6a9cd2c1==',
20      timeStamp: '2016-08-11T01:01:43+00:00'
      commandData {
          "FontName": CourierNew,
          "FontSize": 12
25      }
    }
  }

```

A Globally Unique Identifier may be used as an alternative to using the location ID and
 device label in or der to uniquely identify a shared device 108 to which the print message
 30 311.

For example, during initial system set up, an application within the configuration portal 115
 creates a GUID (Globally Unique Identifier) or in other words deviceId:
 '413dc6c0a03d4d6a9cd2c1=='. An API within the NGP system 103 may be provided which
 35 maps '413dc6c0a03d4d6a9cd2c1==' to Location ID and Device Label. The mapping of the
 device Id to location id and device label may be performed searching, using an API, data
 stored in a database.

Exemplary JSON Request Format with File Data & Configuration:

```

5  "deviceCommand": {
      commandType: 'Print',
      command: 'ConfigPrint',
      timeStamp: '2016-08-11T01:01:43+00:00'
10  deviceId: '413dc6c0a03d4d6a9cd2c1==',
      commandData {
        "FontName": CourierNew,
        "FontSize": 12,
        "File": <FileData>
10      }
    }
  }
}

```

Document Print Response:

Parameter	Type	Optional/Mandatory	Description
MediaType	String	Mandatory	Print
DeviceId	String	Mandatory	IoT Hub DeviceId
TimeStamp	DateTime	Mandatory	FieldGateway Time in UTC
MessageData	String	Mandatory	Key/Value Pair, Message Status & Device Success/Error message

Exemplary JSON Response Format:

5

10

```
"deviceMessage": {
  mediaType: 'Print',
  deviceId: '413dc6c0a03d4d6a9cd2c1==',
  timeStamp: '2016-08-11T01:01:45+00:00',
  messageData {
    "Status": Success
    "MediaStatus": LowStock
  }
}
```

Status	Description
Success	Command Success
Failure	Command Failure

Media Status	Description
LowStock	LowStock Warning
Out of Stock	Out of Stock Error
Paper Jam	Paper Jam Error

15

Thus, alternatively or in addition to the GUID described above, the combination of location ID and device label is used to uniquely identify which shared device the print boarding pass or bag tag message 3110 should be routed to. Thus, this message defines the device to send the print request to in the form of a Device ID. The location ID and label such as ATP

20

may be mapped to the specific device ID.

25

The Field Gateway component, described in further detail below, may therefore store data defining the device ID, such as location ID and label. The field gateway component may also map this information to a specific port number, so that it can correctly determine which device to send the print message 3110 to.

30

The device services interface 117 selects the correct device service, such as printing a boarding pass or bag tag. This is done based on information defining the document to be printed. The selected service within 117 then selects the required template needed to print the data according to a format, such as a boarding pass or bag tag defined by a PECTAB format and encodes the received data according to the format. Thus, the AMQP message

sent to the shared device may be sent with data encoded in a pdf format, also defining the document type such as boarding pass or bag tag.

- In the case of legacy boarding pass printers and bag tag printers, an optional Field Gateway, shown as FR in figure 1, which routes the message to one of the shared locate devices based on the location identifier, and a device label, such as ATP. A certificate is also used. This translates the location ID and label, such as ATP to a unique device identifier.
- 5 Gateway, shown as FR in figure 1, which routes the message to one of the shared locate devices based on the location identifier, and a device label, such as ATP. A certificate is also used. This translates the location ID and label, such as ATP to a unique device identifier.
- 10 In response to receiving a request message 3110 to print a boarding pass or bag tag, the shared device 108 may transmit an optional acknowledgement message 3120. As outlined above, the API 111 may also provide an acknowledgement message 3130 back to the one or more of the applications 141, 143, 145 running in the shared airline environment that a request has been correctly received. The acknowledgements messages may be routed via
- 15 the field gateway which receive acknowledgement message 3130 from the application 111 in the API environment.

- As previously mentioned, the API service(s) 111 perform the function of determine the type of request received from the application 141 in application environment (for example print a
- 20 boarding pass or a bag tag), determine which service in the device service interface 117 will handle the request.

- Finally, the document is printed at one of the shared devices 108 in response to the device receiving the message 3110. The passenger or agent then collects the document for
- 25 subsequent use.

This approach of having different device services within the device services interface 117 allows additional devices, such as payment devices, to be added without impacting system.

- 30 In addition to printing boarding pass and bag tags the other devices such as OCR, LSR, MSR and Boarding gates are supported using same methodology. In this example, the messages structure is shown as 3150, 3160 and 3170 in figure 3 of the drawings.

Closing Applications

- 35 The airlines agent will sign off to their DCS and close the **LH_APP**. This will end the **LH_APP** Citrix session with the **CUTE_Wrapper** service. The airline agent logs out from

NGP and the client device returns to the login screen. **NGP** system then publishes a logout event to the **CUTE_Wrapper** service that allows the **CUTE_Wrapper** service to release all resources associated with the user session and the **LH_App**.

5 Detailed description of router 118 and AMQP protocol messages

Within the API environment 103, a router API 118 may be provided. This may perform a similar function to the API service 111. The router has the function of examining a message received from one of the device services interface 117. This has the function of routing
10 messages 124 to the correct device 108 in the local environment.

The router 118 examines a message 124 received from the device services interface 117. This may be done by examining the message at a header information level which defines the device type. The header may uniquely identify which shared device 108 a particular
15 message should be communicated to.

Each of the shared devices 108 undergo a registration process with the API environment. As part of the registration process, each device 108 is issued a token. The token allows the shared devices 108 to connect the cloud 119.
20

The token is included in the message header of message 124 and by examining the token the router API 118 may determine which device in the local airport environment 108 the message should be sent.

25 The device services interface 117 also processes the information received by message 131 transforms the data into a pdf message format . The particular device services interface 117 transforms the received data into a pdf message format defining either a boarding pass or bag tag defined, for example, according to a PECTAB format.

30 Further, in one specific example the Advanced Message Queuing Protocol, AMQP message protocol is used to send the message from the device service interface 117, via router 118, and usually also via the cloud interface 119 to the shared device 108. This is described in further detail with reference to figure 3 of the drawings. AMQP is an open standard for passing messages between applications. The data unit of AMQP is referred to
35 as a frame. Nine different frames are defined to initiate, control and terminate the transfer

of messages. Messages are sent over a link using the transfer frame. Messages on a link usually only flow in one direction.

5 In the example shown in figure 1 of the drawings a Web Proxy service 113 is provided within the API environment. The Web Proxy service is usually communicatively coupled to both the remote application environment 109 (and hence to one of the applications such as 145 or 143 or 141 in the remote application environment 109) and the one or more user devices 107 shown in the local airport environment 105. The Web Proxy functionality may provide GUI connectivity to the airline applications. The Web Proxy service may also
10 provide GUI connectivity to the tablet, workstation and kiosk display 107 in the airport environment.

However, the Web Proxy functionality 113 is in fact optional and in fact the user devices 107 may be directly coupled to the remote application environment 109 provided the local
15 airport can access, via a communication means 129, the remote application 109 using wired or wireless internet protocols which will be known to the skilled person.

Description of capability services interface

20 A capability services interface, not shown in figure 1 of the drawings, may also be provided. Usually, this functionality is provided within the device services interface 117. Alternatively, the capability services interface may be provided as a separate API service communicatively coupled to the device services API 117.

25 Boarding pass scanners often include capability to show light and emit sound. This provides an audio–visual indication to airline agents regarding whether or not a boarding pass has been accepted or not. This may be done by any illumination means such as an light emitting diode, and a loudspeaker means arrangement. The particular choice as to whether the scanner emits light or sound or both, as well as regarding the particular format
30 of the light or sound emitted, such as the number of beeps and flashes is usually determined by the manufacturer of each device. In any case, these settings may be defined and changed via the configuration portal.

Thus, airlines still have full control of the configuration settings for shared devices, but this
35 is done via the configuration portal 115, rather than via the interface.

This allows for the configuration to be remotely performed by airline for particular airport for a particular user so they can control the number of acknowledgement signals when a boarding pass has been accepted. This allows the device capabilities to be without that coming through interface. Thus, airlines are able to set up the configurations settings for the shared infrastructure via the configuration interface. This avoids the need to put configuration settings in the interface, and also avoids the need for the applications to know how the shared infrastructure interface works.

In a further example, regarding the use of shared infrastructure, when an airline agent scans a boarding pass, the configuration settings may be selected such that the device is locked until the scanning device receives a response from back end systems regarding the validity of the boarding pass.

Thus, the configuration settings may be chosen so that after a boarding pass has been scanned, a visual indication is provided to indicate that additional scans of boarding passes may not be performed. For example, if an LED light is used, this may change to a red colour to indicate that additional scans may not be performed.

The capability service interface determines the type of data and data configurations required by each of the shared devices 108. Usually, a database 112 is provided which stores capability settings and configuration settings associated with each device.

Thus, the device interface 117 can be suitably configured to interact with each of the shared devices by searching the database of physical devices or in other words, a master list of physical devices 112 and their associated capability and configuration settings. Capability or/and configuration settings may vary based on airline preferences and optionally based on location.

Subscriber airlines may view the database of device capabilities and modify it via the configuration portal 115.

To illustrate the above, in one specific example, suppose an airline agent uses a shared boarding pass reader to scan or read a passenger's boarding pass, as the passenger is boarding an aircraft.

Certain data is read from the boarding pass, such as the passenger name. This data will be referred to as boarding pass data. The passenger name, in conjunction with any one or more of the current date and time and airport code may be sufficient for one or more back end systems, such as a departure control system 102 to perform a check that the boarding
5 pass includes data which corresponds to the passenger in a Passenger Name Record, PNR database.

If the boarding pass scanned by the agent is accepted, the departure control system 102 sends a boarding pass acceptance message to the remote application environment 109.
10 This is received by one of the applications 141, 143, 145 in the remote application environment and passed via 121 to the API service 111, and then from the API service via 131 to the device service interface 117. The device service interface 117 then passes this message via 124 to the shared scanner 108 device.

15 The scanner device may indicate that the scanned boarding pass has been accepted by the departure control system by provide one or more indicators. These indicators may take, in principle, any form since device manufacturers and airlines may configure default settings based on their own preferences. However, for example a scanner may indicate that the boarding pass has been accepted by illuminating a green LED, or/and optionally
20 producing a series of beeps or audio indicators.

It is the capability service API, labelled as CS in figure 1 which obtains this device capability data from a database. The capability services API is usually located within device services 117.

25 Usually a list of devices is provided. The list may identify a particular device. Associated information defining the device capability may be provided, for example indicating that the device can read a boarding pass or bag tag. Configuration settings are usually defined for each device. These may relate to specific configuration settings which indicate
30 whether a particular boarding pass has been accepted by a back-end departure control system. In one specific example, the settings may define the number of flashes of and LED or number of sounds emitted by a loudspeaker device to confirm that the boarding pass has been accepted. Usually, specific subscriber airlines will define specific configuration settings they wish to use.

35

The capability services are usually configured as part of initial system configuration when the shared devices 108 are configured for shared use. Part of the configuration process is to list physical shared devices 108 which are available at the local environment 105.

- 5 Once a determination has been made as to which shared devices 108 are available at the local environment 108, then the physical capabilities of each device are determined. Thus, for each device 108 a list of associated physical capabilities is defined. The capability settings and configuration settings associated with each device are usually stored in database 112.

10

For example, suppose the shared device 108 is a DESCO™ VGR device. This device may have any one or more of the following capabilities: passport reading/ scanning, boarding pass reading/scanning, credit or debit card reading/scanning, or a gate function.

- 15 By gate function, we mean the process which is usually performed by an airline agent to check a passenger boarding pass by scanning it with a reader and sending data associated with the boarding pass to a back end system such as departure control system. Thus, data such as a name and seat number may be read from a DCS and sent back to the shared device. The agent may then manually check that the information determined from the DCS
20 matches the information on the boarding pass.

From the above, it will be appreciated that this VGR device has 4 configured capabilities. Thus, for an application which has subscribed to a particular location having such a VGR device, all of the above capabilities are listed.

25

It will be appreciated that the gate function controls access to boarding of the airplane.

As part of the Gate function, the following steps may occur:

- Scan or read a boarding pass;
- 30 • The device is configured to then illuminate a red light which indicates that the device is locked. This prevents others from scanning until the back-end DCS is able to access a database.
- Once the DCS has performed a check that the data read from the boarding pass corresponds to a validly issued boarding pass (for example the
35 passenger name and seat number read from the boarding pass corresponds to the data stored in the DCS), an acceptance command may be issued by

the DCS and communicated to the device. Receipt of an acceptance command may be signalled by a green light, or by one or more audio indicators.

- 5 • These may signal to the agent that the DCS has confirmed that a valid boarding pass with a particular passenger name and seat number has been issued.
- The agent may also perform a cross check to confirm that the boarding pass information shown on the boarding pass matches the passenger data shown on the passport or identity card.

10

As a second example, a device may be an ACCESS™ VGR device. This device only has a single capability, namely to function as a gate function, and it is not able to read a passport or credit card read. Thus, if a particular application in the remote application 141, 143, 145 environment has subscribed to this device at a particular location, then this single capability is listed against this device.

15

For each device shared device 108 associated configuration information is stored. For example, the configuration settings may relate to particular settings chosen to provide an audio or visual confirmation of an acceptance message, such as the particular choice regarding the number of bleeps, such as 1, 2 or 3 to indicate that the boarding pass has been accepted.

20

This configuration information is communicated via the message 124. This is in contrast to known systems in which such device configuration information has to pass through all of the functional components by way of the messages 125, 123, 121, and 131

25

The capabilities services interface provides the individual device services as defined by the device capabilities rather than device make and model. This abstracts the management of the device and any knowledge of physical devices from the airline/airport application. This involves the enumeration and segmentation of a vast number of device capabilities and the individual assignment to a master list of physical devices. Thus a database or list of devices (which may be deployed as one of the shared devices 108 in the airport environment) capabilities) may be provided. The list or database may be stored in storage device 112. Similarly, database 104 may be stored in a storage device.

30

35

Thus, it will be appreciated that the key functionality provided is to integrate future devices with API data without the need of change to applications and utilizing capabilities of future devices to provide rich experience to the user.

- 5 The API's 111 provide managed and controlled access for airport devices 107, 108 to the applications 141, 143, 145 in the remote airport environment 109 based on the interface and configuration settings. Airport administrators may independently configure the devices 107, 108 and airport applications 141, 143, 145 in the API Configuration Portal thus making it available for the airlines, ground handlers and other entities operating in the airport locally
10 or remotely. The airlines administrators may independently configure users and applications and assign them to devices at the airports making it immediately operational. Airlines and airport administrators can create additional administrators and delegate some or all responsibilities.

15 Description of multiple different users at same location sharing the same shared infrastructure

- Embodiments of the invention may handle multiple different users of different user devices which are at the same or similar location, and which may wish to use the same shared
20 device. This is achieved by providing a set of rules regarding how devices are shared between more than one user. In the case of a printer, the rules may simply allow more than one different user to connect to the printer and print jobs are scheduled in the order they are received.

- 25 Regarding shared infrastructure such as a scanner or credit/debit card reader, the rules may need to be more precisely defined. For example, an application requesting use of such a scanner or reader may be required to send a request to the reader to establish if device is available.

- 30 Multiple different users may each share the data channel 124 and Graphical User Interface, GUI channel 125 shown in figure 1.

- Thus, it will be appreciated that a rules engine may be used to govern the rules sharing of devices between different airlines and inter-airlines, as well as between different users
35 belonging to the same or different airline. For example, it will be appreciated that check-in

devices may be shared with different airlines, but however, for a shared kiosk to be accessed by a user, the device must be in an idle state.

Addressing Backward Compatibility

5

A unique feature of the solution outlined above is the ability to accommodate an airline's legacy applications and the standards surrounding legacy devices, and still provide many of the benefits to customers mentioned above. This is achieved by having peripheral communication and airline application delivery following separate paths in the platform.

- 10 • Existing airline applications are delivered to the end station from the Microsoft™ Azure™ cloud using a server-based computing technology, rather than requiring a local installation.
- Calls from legacy applications to the previous system's API are routed through a software translation layer that injects messages into the new platform and delivers
- 15 responses in the correct format. This allows legacy applications to be used without extensive modification.
- Peripheral traffic is therefore separated from the application that generates it, allowing for a more flexible delivery/deployment model.
- Legacy peripherals often require complex PC hardware deployed on site to support
- 20 their operation. Our platform provides for the management of these end stations from Azure-based systems rather than relying on extra equipment deployed at the point of service.
- Customers can access their legacy applications either from a traditional fixed airport position, or from a remote Internet-connected location.

25

When this data is received, it may be parsed.

NGP Interfaces

- 30 The platform exposes the core functionality from two logical perspectives: the customer perspective (airline, airport, operator etc) and the device/location perspective. These interfaces are unique in a way that they provide a complete access for an entity to perform all their processes whilst their operation and implementation is much simpler known systems.

35

Airline/Airport Interface

Embodiments of the invention may have the following advantages: very simple airline interfaces, complete device functionality exposed through this simple interface, roaming and mobile capability, simple ubiquitous web applications, extremely flexible and powerful configurations, smart directly connected devices, no workstations, and high security.

5

The airline and airport interface forms the core services the customers may access and utilize. The interface, through abstraction, provides a simple layer through which the airlines and airports access the device, security, configuration and monitoring services. The platform services in turn implement many checks and balances, some of which are
10 configured by the airline, the airport and others by the platform. The interface, although simple, hides several layers of complex interaction with the platform which ensures authorization, authentication and validation of users, requests and data. The intelligent platform also monitors itself through machine learning technologies to understand the expected behaviour, monitors any deviation and is able to perform corrective actions.

15

Description of Machine learning module

In one specific embodiment, a machine learning or deep learning module may be provided within the API environment 103. The machine learning module may perform stream
20 analytics. This may monitor the communications between the remote application environment 109 or the local airport environment 105 or both. For example, a specific behaviour, such as the number of passport documents being read, by one of the shared devices 108, per minute may be determined. If the number is greater than a predetermined threshold, then, a flag may be provided. This may allow an operator to review the
25 behaviour and decide whether the behaviour should be allowed. Access to the API environment may be denied in response to determine that the number of reads per minute is greater than the threshold. Similarly, the machine learning module may be configured to monitor the number of readers or scanners receiving a message from the API environment. Similarly, if this value is greater than a predetermined threshold, then this may indicate a
30 security breach of the system. S, access to the API environment 103 may be denied based on the determination. Thus, a library of acceptable behaviour patterns may be produced for each shared device 108 and user device 107.

All device functionality is exposed through uniquely designed higher level interfaces. These
35 interfaces are designed for industry wide utilized legacy devices which normally have old interfaces, such as serial, and strict latency and message requirements (link layer).

Platform Interface

The platform exposes several internal interfaces which are utilized in order to implement platform functionality such as: Device services, Location services, Security services,
5 Monitoring services, Logging services, Management services, Configuration services etc. A unique messaging structure has been designed in order to carry the requisite data to and from the platform in either direction either from Cloud to Device (airline to device) or Device to Cloud (device to airline). Built in mechanisms are created in order to calculate message latency for performance measurements and provide corrective actions if the latencies reach
10 a performance limit. Platform interface also abstracts complex monitoring solutions built underneath which provides access to platform wide information on operations, functionality and business processes. This information is available in real time, across the globe to all partners and customers utilizing the platform. The platform makes it possible for airlines to continue to utilize existing business processes, software and hardware and yet still be able
15 to acquire all the flexibility, management and maintenance capability always desired in this environment.

Field Gateway Service

20 A field gateway service, shown as FG in figure 1 of the drawings, download package is usually triggered in response to connecting to the configuration portal 115. As part of the package download, an associated security certificate downloaded with package as well. One the location identifier, ID has been determined as outlined above, the location ID is passed to the field gateway service. The field gateway service connects to the API
25 environment 103 The field gateway uses the downloaded certificate and previously determined location ID. Thus, the field gateway uses the certificate and determined location ID to connect to configuration portal. This allows the configuration portal to determine the particular configuration needed for devices at this location.

30 The configuration service 115 receives a request from the field gateway, and uses the determined location ID to determine what devices are associated with a particular location and the particular configurations needed for those devices.

All device labels are registered in the IOT hub and a token is associated with each label,
35 and thus device.

The field gateway service allows for legacy bag tag printers and boarding pass printers to be remotely connected. The port which a printer is assigned to determines whether the printer is a boarding pass printer or a bag tag printer. For example, bag tag printers are usually assigned to port 07.

5

Thus, the field gateway service may determine the type of printer based on which printing port the printer has been assigned to.

Field gateway used for legacy devices such as custom bag tag and boarding pass.

10

The combination of the field gateway, device certificate, location ID, and device label allows one of the shared devices 108 to be uniquely selected.

15 The following provides further description of how a particular device, such as for example a boarding pass or bag tag printer may be uniquely identified using the location ID and a device label (LocationID.Device_Label). It has particular application for older legacy printers or devices which may need to be compatible with the system, method and device for providing access to shared infrastructure or devices.

20 In this example, the field gateway functionality, FG shown in figure 1 of the drawings may comprise a module or API which may be installed on a work station which may be part of or coupled to one of the shared devices 108 shown in figure 1 of the drawings.

25 During configuration, an agent with suitable credentials launches a portal, usually on the work station. The work station is communicatively coupled with the API environment 103 via wired or wireless communications protocols. A list of possible location identifiers, retrieved from the database 104 is communicated to the portal. The list is usually returned in response to a request for location identifiers. Usually, the location identifiers are associated with particular regions, areas or more particularly zones within particular
30 airports.

The user then selects a particular location identifier which matches their current location, for example, a location identifier "MUM-T1-SBD-001" may be recognised by the user as being associated with Mumbai airport, terminal 1, self bag drop area 001.

35

Another example of a location identifier is "JFK-T1-GATE1-WKS-001" which may be recognised by the user as being associated with US airport, John F Kennedy, Terminal 1, Gate 1, workstation 001.

- 5 Alternatively, the user may scan a beacon 110 which is placed in close proximity to the location where the work station and associated shared device 108 are positioned.

The device_label may take the form of "MSR" may indicate that the device is a Magnetic Swipe Reader used to read a credit card, or loyalty card. Other device types or labels may
 10 be BTP indicating that the device is a Bag Tag Printer or Boarding Pass Printer, referred to as ATP (Automated Ticketing and Boarding Printer) which indicating that the device is a Boarding Pass Printer, as previously described.

The selected location identifier is then communicated to the API environment 103. The API
 15 environment then generates an initialization file which may comprise any one or more of the following fields:

Initialization file contents:

```
{
  "locationId": "JFK-T1-GATE1-WKS-001",
  "authToken": "seyqoeuqwsjfsdkfhdsfuishfs==",
  "configServiceUrl": "https://sita-ngpconfigservice.website.com/"
}
```

20

The initialization file may be encrypted using PGP sign and stored under an Azure Blob storage container ('FgInitFile' container) or storage means or data base 104. Under this container, there may be a sub container for each location ['FgInitFile_<LocationId>.lck']. This file will be usually stored and accessed with an SAS token with an expiry of 4 hrs.

25

The user is then prompted to download the initialization file. The initialization file is also usually copied to USB drive manually. This should be done before token expires.

After launch the Field Gateway component searches for the initialization file which may
 30 be named 'FgInitFile_*.lck'. If the field gateway component successfully finds the Initialization file it sends a request to location service, which may be part of the API environment 103 to obtain the security certificate for each shared device 108 or service running on the work station.

To obtain the security certificate, the Field Gateway component or service calls the Location Configuration service, which may be part of the API environment 103, to get the certificate.

- 5 When the Location service receives the request for security certificate it validates the token (to confirm for example that the token is valid and that it has not expired). The location service may also validate the LocationId or in other words check that the received locationId corresponds to one of the previously stored locationId stored in the database 104.

10

Usually, if both the token and the locationId is valid, then the location configuration service contacts the certificate authority server to obtain the security certificate. Subsequently, the location service sends the public key to the field gateway component.

- 15 Once the certificate is installed on the workstation the field gateway component calls a register certificate API to add this certificate in an active directory or database. The above described process for downloading an initialisation file and obtaining a certificate may be performed for each workstation service or shared device coupled to the work station.
- 20 Once certificate installed in FG it will call the configuration service 'GetDeviceConfiguration' to get the device configuration. Device configuration initially will have only Workstation DeviceId and its key to communicate with IoT, other device details will not be there as device statuses are in 'Not Configured' state.
- 25 Usually, the Filed gateway functionality locally stores or caches the 'LocationId' in a memory for future calls to the configuration service.

From the foregoing, it will be appreciated that the location identifier of a work station (and therefore associated shared devices (108) connected to a work station) as well as a

- 30 Device_Label may be used to uniquely identify a particular shared device to be identified. Thus, this may be used to determine which device particular printing requests should be sent based on the location.

- In some implementations, shared devices, such as bag tag printers or boarding pass
35 printers may be associated with particular ports of a work station. For example, boarding pass printer may be associated with "Port 1" while a bag tag printer may be associated with

“Port 2”. In some implementations, particular device types are always associated with particular port numbers – for example boarding pass printers may always be associated with port 1, while bag tag printers may always be associated with port 2.

5 Thus, it will be appreciated that the shared devices interact with the platform on IoT protocols such as the messaging protocol MQ Telemetry Transport or Message Queue Telemetry Transport (MQTT). In order for this to be possible with existing, legacy devices which may not have any internet based interfaces and higher level messaging protocols, are interfaced with the Field Gateway. The Field Gateway implements device level
10 functionality and manages complex security interaction with the platform to ensure verified devices get to interact by fetching encrypted tokens and applying them to device communications. The Field Gateway also takes several local actions based on device data in order to provide a fast experience based on predetermined configurations.

15 From the foregoing, it will be appreciated that the mobile communication or device may include a computing device, such as a desktop computer, a laptop computer, a tablet computer, a personal digital assistant, a mobile telephone, a smartphone, an internet enabled television, an internet enabled television receiver, an internet enabled games console or portable games device.

20 It will also be appreciated that this invention finds application as a system for processing a user or customer, a device such as a portable device for use by an agent for processing the customer or a device such as a portable device for use by the passenger, as well as a method or computer program for processing the customer or passenger. In addition, this
25 invention finds application as a system for providing services to a customer or user which may be used by an airline agent or other transport services provider agent.

The server may comprise a computer processor running one or more server processes for communicating with client devices. The server processes comprise computer readable
30 program instructions for carrying out the operations of the present invention. The computer readable program instructions may be or source code or object code written in or in any combination of suitable programming languages including procedural programming languages such as C, object orientated programming languages such as C#, C++, Java, scripting languages, assembly languages, machine code instructions, instruction-set-
35 architecture (ISA) instructions, and state-setting data.

The wired or wireless communication s networks described above may be public, private, wired or wireless network. The communications network may include one or more of a local area network (LAN), a wide area network (WAN), the Internet, a mobile telephony communication system, or a satellite communication system. The communications network
5 may comprise any suitable infrastructure, including copper cables, optical cables or fibres, routers, firewalls, switches, gateway computers and edge servers.

The system described above may comprise a Graphical User Interface. Embodiments of the invention may include an on-screen graphical user interface. The user
10 interface may be provided, for example, in the form of a widget embedded in a web site, as an application for a device, or on a dedicated landing web page. Computer readable program instructions for implementing the graphical user interface may be downloaded to the client device from a computer readable storage medium via a network, for example, the Internet, a local area network (LAN), a wide area network (WAN) and/or a wireless
15 network. The instructions may be stored in a computer readable storage medium within the client device.

As will be appreciated by one of skill in the art, the invention described herein may be embodied in whole or in part as a method, a data processing system, or a computer
20 program product including computer readable instructions. Accordingly, the invention may take the form of an entirely hardware embodiment or an embodiment combining software, hardware and any other suitable approach or apparatus.

The computer readable program instructions may be stored on a non-transitory, tangible
25 computer readable medium. The computer readable storage medium may include one or more of an electronic storage device, a magnetic storage device, an optical storage device, an electromagnetic storage device, a semiconductor storage device, a portable computer disk, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), a static random
30 access memory (SRAM), a portable compact disc read-only memory (CD-ROM), a digital versatile disk (DVD), a memory stick, a floppy disk.

Exemplary embodiments of the invention may be implemented as circuit board which may include a CPU, a bus, RAM, flash memory, one or more ports for operation of connected
35 I/O apparatus such as printers, display, keypads, sensors and cameras, ROM, a communications sub-system such as a modem, and communications media.

The flowchart of Figure 3 illustrates the operation of an example implementation of systems, methods, and computer program products according to various embodiments of the present invention. Each block in the flowchart or block diagrams may represent a

5 module comprising one or more executable computer instructions, or a portion of an instruction, for implementing the logical function specified in the block. The order of blocks in the diagram is only intended to be illustrative of an example. In alternative implementations, the logical functions illustrated in particular blocks may occur out of the order noted in the figures. For example, two blocks shown as adjacent one another may be

10 carried out simultaneously or, depending on the functionality, in the reverse order. Each block in the flowchart may be implemented in software, hardware or a combination of software and hardware.