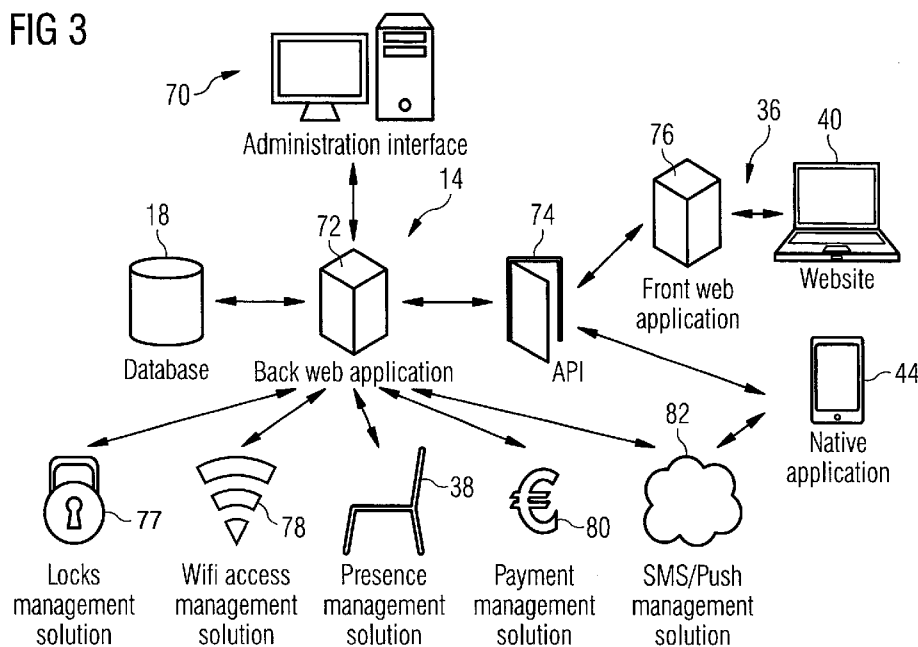




- (51) International Patent Classification:
G07C 9/00 (2006.01)
- (21) International Application Number:
PCT/EP2016/000828
- (22) International Filing Date:
18 May 2016 (18.05.2016)
- (25) Filing Language:
English
- (26) Publication Language:
English
- (71) Applicant: ALSTRIA OFFICE REIT-AG [DE/DE];
Bäckerbreitengang 75, 20355 Hamburg (DE).
- (72) Inventor: ELAMINE, Olivier; Emil-Andresen-Strasse 74,
22525 Hamburg (DE).
- (74) Agent: KRAMER BARSKE SCHMIDTCHEN; Paten-
tanwälte PartG mbB, Landsberger Strasse 300, 80687
München (DE).

- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

(54) Title: CENTRALIZED ACCESS SYSTEM AND METHOD



(57) Abstract: A centralized access system (100) is used for managing access of users to a plurality of distributed facilities, for example, a plurality of shared office spaces provided at geographically different locations. Each user has an access device (16) such as a smartcard including a unique ID associated with the user. A user can subscribe to obtain access to one or more of the plurality of office spaces for a period of time, and each office space may include a plurality of electronic locks that are connected to a central server (14) of the system. The server (14) may then control the respective locks (21) such that the user has access to the office space, and any services provided therein, at the location and the time that has been booked.

WO 2017/198282 A1

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

Description

CENTRALIZED ACCESS SYSTEM AND METHOD

Technical Field

[01] The present invention generally relates to a centralized access system and method, in particular, to a centralized system for controlling user access to a plurality of distributed facilities, for example, office spaces, residential buildings and the like, and the user's authorization to use specific services within these facilities, for example, a WiFi network, printing services, a gym, a swimming pool or the like.

Background

[02] There are a number of existing technologies for providing access and services to building occupants, for example, workers in an office building. Due to the considerable costs associated with leasing office space, many small or medium-sized companies, as well as individuals, sometimes use a shared office space provided in a building owned by a corresponding service provider. This allows for avoiding or limiting inefficiencies associated with leasing office space, as such an office space generally includes facilities such as meeting rooms, a kitchen, recreation rooms, and the like, which are rarely used. Further, in today's global economy, it is common for many employees or businessmen to travel both at home and abroad. Therefore, it is advantageous if the person that is travelling has access to office space also during such travels.

[03] When providing such shared office spaces, several design constraints exist. First of all, the user experience must be as seamless as possible and adapted to any type of user. Further, security and access control are a key factor in an environment with no permanent presence of users. In addition, sometimes it may be cost-effective to design the system such that there is no staff

on site at the respective office spaces. Nevertheless, the office space should feel welcoming and comfortable.

[04] In order to be financially profitable, the system must provide solutions for controlling usage of space and services. In addition, the system should be easy to set up, disassemble and store, without reducing the quality of service.

[05] Therefore, it is desirable to provide a system and method that allow for a flexible, secure and easy user access to a plurality of distributed facilities such as shared office spaces, but not limited to the same.

Summary of the Invention

[06] In a first aspect, a centralized access system for controlling user access to a plurality of distributed facilities comprises a plurality of electronic locks respectively associated with the plurality of distributed facilities, and at least one equipment provided in the plurality of distributed facilities. A central data processing device is in communication with the plurality of electronic locks and the least one equipment. An access device includes a unique ID associated with a user, and a database is configured to store information indicating a period of time during which the user has access to at least part of one or more of the plurality of distributed facilities and the at least one equipment. The data processing device is configured to control the plurality of electronic locks to selectively allow or deny access by the access device based on the information stored in the database. Further, the data processing device is configured to selectively allow or deny access to the at least one equipment by the user based on the information stored in the database, for example, simultaneously to allowing or denying access by the access device based on the information stored in the database.

[07] In a further aspect, a method of controlling user access to a plurality of distributed facilities comprises providing an access device with a

unique ID associated with a user, storing information indicating a period of time during which the user has access to at least part of one or more of the plurality of distributed facilities in a database, controlling a plurality of electronic locks respectively associated with the plurality of facilities to selectively allow or deny access by the access device based on the information stored in the database, and providing at least one service to the user at the plurality of facilities based on the information stored in the database.

[08] With the system and method disclosed herein, a process for providing access and services to building occupants, for example, workers at office spaces is provided. This process could also be used in other areas of real estate, for example, residential buildings or hotels. With the disclosed system and method, it is possible to centralize information concerning a specific user, and to allow the user to access multiple spaces, which can be located in multiple geographical regions, and to offer the user several on site services that are the same in all the different locations. This allows a user having a single access device to be able to access different facilities, for example, different office buildings, connect to a wireless network and use office equipment such as printers and the like. This is because each space will recognize the user and the access rights of the user. These access rights, and the corresponding services, are controlled both in space (the accessible spaces at different locations) and time (the period of time during which the user has access to a given space).

[09] For example, in the hotel world, the disclosed system and method could provide for the ability to book a room online, immediately receive the room number, and be able to access the room at the booked date with an access device that has been provided to the user in advance and can be used to access the room without any further need to register upon arrival at the hotel, and get automatic access to the WiFi network of the hotel, or to the minibar in the room.

[10] In another aspect, a computer program comprises computer-executable instructions that, when executed on a computer, cause the computer to

execute the steps of storing information indicating a period of time during which a user has access to at least part of one or more of a plurality of distributed facilities and to at least one equipment provided in the plurality of distributed facilities in a database, the information including a unique ID associated with the user, and controlling a plurality of electronic locks respectively associated with the plurality of facilities to selectively allow or deny access by an access device including the unique ID associated with the user, and selectively allowing or denying access to the at least one equipment by the user based on the information stored in the database.

- [11] Other features and aspects of this disclosure will be apparent from the following description and the accompanying drawings.

Brief Description of the Drawings

- [12] In the following, embodiments of the present invention are described in detail with reference to the attached drawings, in which:
- [13] FIG. 1 shows an exemplary floor plan of a shared office space in accordance with an embodiment of the present invention;
- [14] FIG. 2 shows a schematic overview of a centralized access system in accordance with an embodiment of the present invention; and
- [15] FIG. 3 shows a system architecture in accordance with an embodiment of the present invention.

Detailed Description

- [16] FIG. 1 shows a floor plan of a shared office space provided in a building 10 as an example of one of a plurality of distributed facilities that can be accessed using the system and method disclosed herein. It will be appreciated that, in the present example, a plurality of buildings 10 may be provided at different locations distributed around a city, or even in different countries. Further, the term “facilities” as used herein is not intended to only designate

different buildings, but may also designate different spaces, for example, floors, apartments or rooms within a building, or other spaces or equipment within an office space that may be accessed using a single access device, preferably at a plurality of different locations (herein referred to as “distributed facilities”).

[17] As shown in FIG. 1, building 10 includes a main entrance 41. Main entrance 41 may comprise one or more doors configured to be opened by using an access device to unlock an electronic or smart lock 42, which will be described in more detail below, or by inputting a code via electronic lock 42, which may also function as a code input device. In some embodiments, a separate code input device may be provided.

[18] As shown in FIG. 1, the shared office space includes a lobby or waiting room 54, a kitchen or recreational area 58, an open office space 60 including a plurality of workplaces (“open desks”) 50, meeting rooms 52, 66, and one or more private offices 22. In addition, the shared office space may include one or more flexible meeting rooms 32 being provided with, for example, a telephone or another communication device. A printer room 62 may include a printer 64 and any other office equipment such as a fax machine and the like, which may be used by the user having the appropriate access rights. Further, a separate room may include technical equipment such as, for example, a wireless or wired communication device 26, for example, a router providing access to the internet. Throughout the office space, a plurality of wireless or wired access points 28 in communication with communication device 26 may be provided.

[19] Waiting room 54 may be openly accessible to any person having entered through main entrance 41. In some embodiments, however, an electronic lock (not shown) that may be opened, for example, by inputting an access code or using an access device may be provided in front of waiting room 54. Inside waiting room 54, a reception terminal 56, for example, a tablet, may be provided. Reception terminal 56 may be configured to be used by a user to, for example, check the availability of one of meeting rooms 52, 66, book one of the meeting

rooms 52, 66, reserve private office 22, reserve a seat at one of workplaces 50, and the like. This will be described in more detail below.

[20] Waiting room 54 may also include an entrance 20 for access to the main area of the shared office space, i.e., open office space 60, the various meeting rooms 52, 66 and the other facilities provided in the shared office space. Entrance 20 is secured by an electronic (door) lock 21. Access via entrance 20 will be described in more detail below.

[21] Each meeting room or private office may be secured by a further electronic lock, for example, a lock 12 in front of private office 22 and a lock 68 in front of meeting room 66. Each meeting room or private office may include a printer 24, a computer 30, a TV, a conference phone, and the like.

[22] Electronic locks 12, 21, 68 and, optionally, lock 42 may form a system of connected locks that are in communication with a central data processing device 14 (for example, a server or the like) shown in FIG. 2. FIG. 2 shows an overview of the general architecture of the access system of the present disclosure. As shown in FIG. 2, a centralized access system 100 in accordance with the present disclosure includes data processing device 14, which is in communication with the plurality of electronic locks provided at a plurality of distributed facilities, for example, a plurality of buildings 10, each including the above-described shared office space. As an example, FIG. 2 shows data processing device 14 being in communication with (connected to) a plurality of electronic locks (smart locks) 21 provided at the entrance 20 to the main area in each shared office space. It will be readily appreciated, however, that this is only an example, and data processing device 14 generally will be in communication with all connected electronic locks provided in the different facilities. Likewise, it will be appreciated that the term “electronic lock” as used herein encompasses any type of electronic or smart lock that has a communication device, a controller and the like enabling remote control of the lock by a central data processing device or control device.

[23] Access system 100 also includes an administration interface 70, for example, a known computer having a display and an input device, and a database 18. In addition, access system 100 includes an access device 16 including an electronic ID that may be uniquely associated with a user of access system 100. Via administration interface 70, an administrator can manage access of the user carrying access device 16 to the respective office spaces. For example, a user may subscribe to a membership program allowing the user access to all open office spaces 50 in the different facilities. In this case, database 18 stores the information that access device 16 may unlock each electronic lock 21 (and, if necessary, electronic lock 42 and any other locks that allow access to entrance 20) at the respective facilities. Therefore, the user travelling, for example, to different cities, each city having a building 10 configured in the above-described manner, may simply enter each building via main entrance 41, for example, by using access device 16, enter open office space 60 via entrance 20 using access device 16 to unlock electronic lock 21, and occupy any available seat at one of open desks 50. In addition, the user's access to the different services (WiFi, printers, and the like) provided in each building 10 may also be managed via administration interface 70 and controlled by central data processing device 14. It should be appreciated, however, that this is merely one example for the access rights that may be given to a user. Further details of the system architecture shown in Fig. 2 will be described in the following.

[24] FIG. 3 shows the system architecture of centralized access system 100 in more detail. As previously mentioned, access system 100 includes administration interface 70 and database 18 associated (in communication) with central data processing device 14. In particular, data processing device 14 may include a back web application 72 running, for example, on a central server of the entity operating distributed access system 100. Back web application 72 is configured to read from and write to database 18, expose administration interface 70, which is used for managing data related to the plurality of distributed

facilities, e.g., shared office spaces, expose an API consumed by a front web application 76 and, for example, a native application running on a mobile device 44 carried by a user, and manage external services such as a locks management solution 77 for controlling the respective electronic locks, a WiFi access management solution controlling WiFi access at the respective facilities, a presence management solution 38 configured for detecting a user presence at each of the plurality of distributed facilities, a payment management solution 80 and an SMS/push management solution 82.

[25] Administration interface 70 may be configured as a website displayed on a computer system used by an administrator to manage data related to the plurality of distributed facilities (for example, creating a space or adding a lock). Administration interface 70 may, for example, be powered by the Rails gem ActiveAdmin, and may offer the following features: administrator authentication, base actions such as create, edit, delete, browsing of records with the help of different filters, and extraction of records into CSV files.

[26] API 74, for example, a JSON API, is the channel through which front web application 76 and the native application running on mobile device 44 get, update, create or delete data. To restrain the access to the data specific to a user, some endpoints require an authentication. This authentication may be powered, for example, by the gem Devise and its plug-in DeviseTokenAuth.

[27] Front web application 76 may provide a user interface 36 including a website that may be displayed on a display of, for example, a personal computer 40 of a user. Using said user interface 36, the user may book access to one or more of the plurality of distributed facilities for a specified period of time. Back web application 72 (central data processing device 14) will then correspondingly update database 18 and store the booked access time therein, together with any associated services to which the user has access.

[28] As previously mentioned, back web application 72 leverages external services for tasks requiring specific know-how. These tasks are the

control of smart locks, the management of access to a WiFi network, the measurement of an occupancy of a given space, the distribution of SMS and push messages, and the processing of payments. All these interactions are performed through HTTP requests on APIs exposed by each of these services.

[29] For example, the plurality of electronic locks may be controlled in the following manner. In particular, the electronic locks may be BRIVO smart locks, and the back web application 72 may interact with the RESTful BRIVO API. The BRIVO system is built around three classes: groups, users and locks. A space such as a particular shared office space will correspond to a group, and users and locks correspond to an entry in the BRIVO system. The back-end (central data processing device 14, i.e. back web application 72) keeps the BRIVO system updated. This happens in the following cases: (i) creation of a space and its locks using administration interface 70, this results in the creation of a BRIVO group with the corresponding BRIVO locks; (ii) creation of a user, (iii) subscription of a user to a space, this results in the addition of the corresponding BRIVO user to the corresponding BRIVO group, (iv) end of a subscription, this results in the BRIVO user being removed from the corresponding BRIVO group. In addition, a guest system may be enabled. To this end, one guest BRIVO group is created per space. This guest group contains only the digicode lock of the space. Each guest invitation creates a user with a daily subscription, with the guest's ID being set to the ID of the user that is sending the invitation. This host ID indicates to the back-end that it needs to add the guest BRIVO user to the guest-dedicated group. Booking of, for example, a meeting room is performed as follows. At the start of a booking, the meeting room corresponding to the BRIVO group is added to the BRIVO users attending the meeting. At the end of the booking, the meeting room is removed from the BRIVO users attending.

[30] Further, back web application 72 manages access to the wireless network, for example, an AEROHIVE WiFi network, through an API such as the ID manager REST API. Through the ID manager, private pre-shared keys

(PPSK) unique to each user are created. Each key may be valid for the whole WiFi network. The back-end (central data processing device 14) creates a new PPSK when a user registers to a space and disables the same when the registration ends. In other words, a service such as, for example, access to a WiFi network may be provided based on the user's registration. Access to such services may be based on access device 16 (for example, a printer or the like may include a contactless reader for reading the ID included in the access device), or it may be based on a code or password generated based on the user's registration (for example, to access a WiFi network or computer, or to be input into a code input device associated with office equipment, doors to specific areas within the facilities, a coffee machine, a video game or other entertainment machine etc.).

[31] To estimate the occupancy of the spaces, data may be gathered using a user detection device 28, for example, chair presence detectors (see Fig. 1), cameras provided at the entrance to each facility, and the like. The back-end may be configured to request information on the detection by the user detection device 28 at regular intervals, for example, every five minutes. The information gathered in this manner may also be displayed to a user, for example, on the display of the user's computer 40. This may assist the user in selecting available facilities and/or available workspaces, meeting rooms or private offices.

[32] Preferably, the back-end may further be configured to store device tokens collected by the native application running on a user's portable smart device 44, and may send a push to the smart device 44 when a guest invited by the user has arrived in the waiting room 54, a booking for a meeting room or private office starts, a booking for a meeting room or private office ends, or send a reminder for a booking via SMS/push management solution 82. In the same manner, the back-end may use the phone number collected during user registration to send a message, for example, an SMS, when an access code to enter a space is received for the first time or when a guest has arrived.

- [33] Payment transactions may be performed using any known electronic billing system, for example, STRIPE or any other appropriate payment management solution. For example, during registration, the mobile and web applications create a customer in the STRIPE system, and send back its ID to the back-end. When a user wishes to subscribe to a space, the mobile and web applications issue a charge corresponding to the duration of the subscription. Once this charge is accepted by the user, the mobile and web applications update the database 18 associated with back web application 72. To prevent fraud, the back-end verifies with the STRIPE service that the charge ID is genuine and the charge is paid. In this manner, no financial information is transmitted through the back-end. All financial transactions are handled by STRIPE. However, invoices can be generated by the back-end, for example, in PDF format.
- [34] Database 18 is the part of the back-end that is responsible for storing persistent data. The database system may be powered by an SQL database such as PostgreSQL. However, collaboration with external services may imply using third party databases. In order to keep data integrity intact, as little data as possible is duplicated to external databases.
- [35] In the following, access device 16 is described in more detail. Access and security play an important role in the centralized access system of the present disclosure. To offer a seamless experience to all members, regardless of their level of technological adoption, access passes in the form of an access device are used as the main access control method in accordance with the present disclosure. Said access passes may use wireless technology to communicate with, e.g., contactless readers (the above-mentioned electronic or connected locks, tablets, smartphones, vending machines, etc.). The access passes can take various forms. For example, access device 16 may be an access card, a sticker, a key chain, and the like. In particular, access device 16 may be a conventional smart card having a standard form, which is relatively cheap and easy to personalize and store.

[36] Access passes are only available for members and visitors, as will be described in more detail below. In the system of the present disclosure, the access passes may be used to unlock main entrance 41 of building 10, entrance 21 to the main area of the office space, unlock and lock meeting rooms, for example, meeting rooms 66, 52, unlock and lock private offices such as private office 22, and use additional services, for example, coffee machines, vending machines, and the like. A unique access pass (ID) is assigned for each member and synchronized with the member's account. The access pass is stored on access device 16. If a member loses access device 16, a new access device can be configured, for example, in any one of waiting rooms 54. To do so, the user must log in via terminal 56 with his login/password, follow a "I lost my access card" process during which the old access card is disabled and can no longer be used, pick up a new access card, which may be stocked inside waiting room 54, bring the new access card into contact with a contactless reader provided, for example, in or at terminal 56 to synchronize the same with the user account, and use the newly configured access card to unlock entrance 20. Access information is stored in central database 18 and not in a local database for security reasons.

[37] As mentioned above, the access pass can take various forms, for example, stickers, cards, and the like. Further, for example, with near field communication (NFC), an NFC-enabled mobile phone can be used by a member as an access device. Contactless access control has the advantage that it does not require a complex hardware installation and is very user-friendly. For instance, with NFC, a member can autonomously program a new access device by using terminal 56 having contactless features. Further, a contactless access control can be set up in a large or small space, and also in a plurality of locations (for example, it is easy to enable/disable access across sites). In addition, access cards are cost-effective, and hardware costs are minimal as the data management is performed on a central server. Therefore, no complex IT infrastructure and maintenance teams are needed.

- [38] In order to control access inside access system 100, door locks play an important role. These door locks only allow access for members, registered visitors and guests. Generally, there can be four types of doors inside the system that require access control. Each door can be unlocked using a valid access pass.
- [39] Main entrance 41 can be entered using an access device or an access code. As previously described, electronic lock 42 may perform both of these functions.
- [40] Inside waiting room 54, entrance 20 controls access to the main area of the office space. From the outside, this door can only be opened with a valid access pass (access device). Guests are not allowed to enter via entrance 20 without being accompanied by their host.
- [41] Meeting room doors can only be locked and unlocked using the access pass of the member who booked it. For example, lock 68 can only be unlocked during the booking period by the user having booked the same. To check out from a meeting room, users must lock the door to the meeting room from the outside.
- [42] Private office doors can only be locked and unlocked using the access pass of the member or members who booked it. It can only be unlocked during the booking period, and checkout must be performed by locking the door.
- [43] Preferably, the above-mentioned locks are electronic locks that can be unlocked using a contactless access device. It should be noted that electronic locks typically work on a battery. Therefore, power shortage must be identified, and batteries need to be replaced periodically. For example, battery control devices may be provided for each lock and generate an alarm that is sent to back web application 72 to alert an administrator that the battery needs to be replaced. Further, for a seamless experience and security reasons, the above-described access control system must be fully integrated with other systems such as access pass creation, the booking system, security systems, invoicing, etc. In

addition, in case a separate building door access control exists for building 10, it must also be integrated into the same.

[44] The plurality of connected locks of the present disclosure allow for a precise access control for each room, giving different rights for different users at different times. Therefore, with no reception and no staff inside the facilities, the strict but flexible access control using access device 16 and, for example, electronic locks 12, 21, 68 is key to managing spaces and making sure that services are provided to the right users at the right time. In addition, to allow for billing for the provided services, for example, with hourly rates, it is necessary to detect when people check in and check out from each facility and the respective rooms provided therein. Using the plurality of connected locks, the exact moment when a user enters an office space, enters and leaves a meeting room or a private office, and the like, can be registered by access system 100. Further, WiFi access logs can be combined with these data, and it can be estimated who is in a space, as well as the total occupancy of each space. This information can again be displayed to other users intending to book a space or reserve a room.

[45] In some embodiments, a mobile application (app) can be used to ensure a high level of services while providing mobility, as well as for controlling the overall experience inside the respective facilities. The mobile application offers different services when logged in and logged out. For example, when logged out, users can use the application to consult a location and an availability of the distributed facilities, for example, the office spaces and their associated open desks, meeting rooms, private offices, and the like. Further, the application can be used for sign up and log in, as well as for getting general information on the services provided by centralized access system 100, such as a user guide, contact information, prices. When logged in, members can use the application to consult/modify their account information, book a desk, a meeting room or a private office, as well as extend/cancel a booking, consult invoices, access

additional services such as a taxi service, food delivery, etc., lock/unlock connected doors in case the associated portable device is NFC-enabled, report issues (loss of access device 16, security issues, etc.), and log out. The application is also used to push notifications to users. For example, for a meeting room, a booking start, a booking info, a booking end, a booking update, and the like can be notified. The same applies to private offices. Further, as previously mentioned, arrival of guests can be notified, booking start and booking end for an open desk can be notified, arrival of a delivery can be notified, and the like.

[46] To compensate for the absence of permanent staff at each facility, it may be advisable to set up a helpline in form of an interactive voice server. This communication channel may provide a solution for users without internet access and a direct link with facility managers for issues and urgent matters. The voice server provides access for users to sign up for the service, manage their account, manage their booking, get an access code for members who forgot their access device, report an issue, and the like. Voice response can be configured in different languages to meet users' preferences. Further, with an interactive voice server, no phone calls are lost, and statistics about most frequent questions and issues can be collected.

[47] The website accessed by the user is the first contact point for all types of users. It provides general information about the service, as well as complete control over member accounts. When used outside access system 100, users can use the website to consult the location and availability of office spaces, sign up and log in, and get general information about the offered services. Once they are logged in, members can use the platform to consult/modify their account information, book a desk, meeting room or private office, and the like, consult invoices, access other services, report issues, and the like.

[48] From within access system 100, users are automatically redirected to a login page where they can log in (members: login/password, guests: access code sent by their contact), sign up, consult availability, get general information,

and the like. Once they are logged in, members can use the platform to consult/modify their account information, book a desk and the like, consult invoices, access all services offered by system 100, i.e., printers, taxi services, any other type of office equipment, etc., report issues, log out, access a collaborative platform that may be provided to chat and share files with other members and guests, and access the internet. Guests and visitors can use the platform to access the available services at the facility, report issues, log out, access the collaborative platform, access the internet and subscribe to a membership. In some embodiments, when a meeting room or a private desk is booked, a private and secure online space is automatically created, allowing participants to share files and chat easily. The creator of the private and secure online space can give temporary access to the created spaces to other members. In other embodiments, system 100 may be configured to store user profiles in database 18 that may, for example, be used to appropriately configure any computers, printers and other equipment in the respective office spaces in an automatic manner when they are used by a particular user.

[49] Inside the web platform, a special interface must be provided for an administrator of system 100. This interface will provide features allowing for the management of member accounts and corporate accounts, consulting analytics, and collecting cumulated invoices. Preferably, the web platform is web based and accessible on any operating system and hardware. Further, being hosted on a central server, the web platform does not require any complex IT infrastructure and is easy to scale if the number of members or facilities grows. Finally, the web platform provides a solution for controlling access to the available services such as printers and the like.

[50] Waiting room terminal 56 is a lightweight tool that can mainly be used for automatically configuring new access passes for members. It includes contactless features that allow for reading and programming an access device 16. Terminal 56 is provided in waiting room 54 to give information to users and

allow users to automatically sign up and configure a unique access pass. A member may create a new access pass. A guest can use terminal 56 to notify a host of its arrival, enter the access code that was received with the invitation, consult general information about the service, or sign up. A visitor can consult general information about the service, complete a subscription and create an access pass and sign up with the service.

[51] Inside each meeting room, for example, meeting room 52, a computer and/or tablet 30 is provided for displaying booking information and configuration of a booking. During a meeting, members may use the tablet to control their booking period and be notified if they exceed their time limit, extend the booking, consult and order services, checkout and control room automation if available (light, air conditioning, etc.). For some features, an ID validation may be necessary (for booking extension, ordering services, etc.). This may be performed using access device 16 containing the unique access pass of a user. To ease the use of meeting rooms, each meeting room may display visual information about its availability. When a member is already inside the office space and immediately needs a meeting room, he or she can simply walk toward a meeting room to unlock it. To make the booking process as seamless as possible, the availability information for the different rooms may also be displayed, for example, at the entrance of waiting room 54 or at any other appropriate location inside the office space by a suitable display device.

[52] As previously mentioned, one or more detection devices 28 may be installed inside the office space to monitor usage of the same. For example, presence detectors may be included in each room, and motion detectors or seating detectors 28 may be provided for each open desk 50. The gathered information will be used to estimate availability of spaces, and to also gather information on how people use the equipment and the respective spaces.

[53] As previously mentioned, there are several possibilities for locks management solution 77. For example, smart locks may be used that are WiFi

connected locks targeting mainly the home automation market. Alternatively, a conventional hotel card lock system may be used that provides an access control solution for hotels, storing access rights inside an access card. Further, real time access control systems can be used, which use wireless updates from a central server. Preferably, a real time access control system is used that is resilient to power shortage, network shortage, and can be updated in real time. Further, the system should be easy to install or remove and compatible with standard door locks. The respective locks may be opened by an access pass, a key, or a smartphone, for example, using NFC. Preferably, each lock should be connected to the central data processing device 14, i.e., the server running back web application 72, and allow for a web-based configuration and management. In particular, the system should allow for a precise configuration inside a building, i.e., assigning different rights for different rooms for different access passes at different times. Finally, the system should allow for the management of connected locks in different buildings within one system. As previously mentioned, an exemplary system that may be used is the BRIVO system.

[54] Concerning access pass solutions, several different technologies may be used. One may be a common contactless RFID smartcard that is compatible with most systems. However, such an RFID smartcard requires a specific reader/writer for configuration. In some embodiments, a secure version of an RFID smartcard can be used. In other embodiments, an NFC communication system may be used, which has the advantage that it may be configured via, for example, smart devices such as a tablet. In some smartphones, NFC communication means are already included. Preferably, an NFC system may be used to ensure future compatibility with smartphones and other connected objects.

[55] For waiting room terminal 56, different solutions can be envisioned. One solution may be a fully integrated system with custom software, while another solution may be use of a standard tablet with a custom app, perhaps

together with a secured enclosure/stand. Using a fully integrated system has the advantage of offering a visible and welcoming experience and a user-friendly interface. Further, the hardware will generally be very reliable. In addition, using a secured enclosure/stand, the hardware can be protected from stealing and damages. Further, the hardware is easy to configure for one facility and may be reconfigured when moving to another facility. In addition, it can provide a user interface for displaying the web platform of the associated service provider. Additionally, some tablets already offer the possibility to read and configure access devices, using an NFC reader and writer.

[56] Concerning contact point solutions, e.g., wireless access point solutions, any secure platform that enables captive portal support with a simple web-based user interface, assigning different rights and roles for different users, automatically disconnecting at the end of the scheduled time, and compatibility with all platforms can be used. Two types of solutions, which may be used, are traditional enterprise class networks and cloud based wireless access solutions. Preferably, cloud based wireless access solutions are used, as they generally fulfil the above-listed requirements. This system architecture may be composed of a router WiFi fiber modem connected to the internet, a WiFi access point with a POE injector, and cloud based network management software.

[57] For the tablet provided in each meeting room, standard tablets can be used. For printer solutions, any solution provided by one of the major printing companies may be used. Further, web-to-print solutions could also be used that allow for a seamless way of printing documents from a web interface.

[58] For the above-mentioned presence sensors, a system that is composed of, for example, activity sensors deployed under desks or seats, network receivers use to collect data via wireless or wired transfer via the internet, and a cloud based management software could be used.

Industrial Applicability

[59] In the following, an operation of centralized access system 100 in accordance with the exemplary embodiment will be described in more detail.

[60] In the exemplary system, a user generally has a particular user status associated with the user. For example, the user may have member status. After registering as a member, the user will generally get access to one or more of the plurality of the distributed facilities, for example, one or more of buildings 10 including the shared office spaces. In other words, the member can enter any building 10 and the associated workspace therein using access device 16. Once a user has subscribed, data processing device 14 updates database 18 accordingly, and controls locks 21 at each of the facilities to which the user has subscribed to allow access by access device 16 during the times covered by the membership. The same applies to lock 42 provided at main entrance 41 of each building 10. Depending on the details of this subscription, the user may also have access to, for example, meeting room 52, private office 22 via lock 12, or meeting room 66 via lock 68. Further, the user may also book a specific open desk 50 in open office space 60. In addition, the subscription may allow the user to access the WiFi network provided at each facility, as well as any other services covered by the subscription, for example, printers or the like. Of course, billing for services such as printing and the like may be based on the actual usage of said services, which may be tracked due to the unique ID of access device 16 that is used for accessing the same.

[61] As a further user status, a visitor status may be provided that allows users to get access to a space for a limited period of time, for example, one day. Finally, a guest may be a user that is invited by a member. A guest does not need to be registered, but gets access to the building by using an access code that is generated, for example, by a code generation device (e.g., the back-end) upon a request by a member. The generated code may be sent to the guest, and the guest may enter the generated code into lock 42 serving as a code input device

provided at main entrance 41 of a facility. After entering the facility, the guest may wait in waiting room 54 to be picked up by the member. The guest may also be allowed to access the wireless network and other services during a limited period of time, for example, from 30 minutes before to 30 minutes after a meeting, using the received code.

[62] A member that has subscribed to one or more office spaces may use its computer to check the availability of a given office space on the website. The user may log in and book a seat in the open office space 60 of the desired facility, for example, for a few hours. When the member arrives in front of building 10, it uses access device 16 to unlock main entrance 41. In some embodiments, the member may also receive a welcome notification on its mobile phone, as well as information on how to find the booked desk. Further, the member will also unlock entrance 20 after passing through waiting room 54 via lock 21, using access device 16. Then, the user may proceed to open office space 60 and sit at any available desk or the specific desk that has been booked. Further, the user may connect to the wireless network and access all services available at the facility.

[63] In a further example, the member that is at the facility, for example, inside open office space 60, may wish to organize a meeting in one of the meeting rooms, for example, meeting room 66. To this end, the user may walk to the closest meeting room and see whether the room is available, for example, by checking a sign that is provided in front of each meeting room and displays whether the meeting room is available or not, or during which times it is not available. When a meeting room is available, the user simply uses access device 16 to unlock the meeting room, for example, by unlocking lock 68 provided at meeting room 66. This may result in the meeting room being booked for the member for the next hour in an automatic manner. Once inside the meeting room, the booking can be confirmed/extended, for example, using a tablet (not shown) provided in the meeting room. After the meeting is over, the

-22-

user leaves meeting room 66 and locks the door using access device 16, thereby ending the booking of the same.

[64] In a further example, a member may set up a meeting with clients or colleagues. To this end, the user may log in on the website and select a meeting room and the period of time for which it should be booked. After confirmation, an access code is generated for the clients or colleagues. The member can send the access code to the clients or colleagues, together with additional information such as the address of the facility, the time of the meeting, and the like. At the time of the meeting, the user accesses the facility in the above-described manner. Further, when the clients or colleagues are entering building 10 using the generated access code, the user may receive a notification, for example, on its mobile phone. Alternatively, the visitors may use terminal 56 provided in waiting room 54 to notify the user. Then, the user picks up the visitors at the waiting room and unlocks the door to the booked meeting room using access device 16. Using the tablet provided inside, for example, meeting room 66, the user can perform various controls such as controlling the temperature, the light, etc. in the meeting room. In addition, a working group can be created on an associated online platform to share files and notes between participants of the meeting.

[65] From a visitor perspective, a code allowing access to a facility may be received via email or SMS, together with the address and the time of the meeting. Upon arrival at building 10, the visitor may enter the code via lock 42 and access building 10. Then, the visitor may proceed to waiting room 54, if necessary, by following signs provided inside building 10. Inside waiting room 54, the visitor may notify the user that has sent the invitation, for example, using terminal 56, and wait until being picked up by the user. After passing through entrance 20, the visitor may use the generated access code to access the provided online platform via the wireless network. After the meeting has ended, the visitor may exit building 10 via main entrance 41.

[66] Further, in case of a visitor, such a user may register for a free limited time pass, for example, a one day pass using the user's email or telephone number. The user receives a confirmation and a generated access code via SMS or email. The code is valid for, for example, one day. Using the code, the visitor enters the building 10 and receives a SMS with a welcome message and advice on how to use the facility. Inside waiting room 54, the visitor may use terminal 56 to complete registration of a profile (name, surname, password, payment details, etc.). The visitor may pick an access device 16, which may be provided in waiting room 54 and synchronize the same with the visitor's account using terminal 56. After synchronization, the visitor may use access device 16 to unlock entrance 20 via lock 21 and enter open office space 60. After accessing the online platform via the wireless network, the visitor may book a seat, a meeting room or a private office for the day.

[67] Although the preferred embodiments of this invention have been described herein, improvements and modifications may be incorporated without departing from the scope of the following claims.

[68] For example, although the exemplary embodiment described herein relates to the use of shared office spaces, it will be readily apparent to the skilled person that the system and method disclosed herein can also be used for hotels, residential buildings, and the like. For example, a user may have a single access device (an access card) that allows access to different hotels, for example, of a hotel chain around the globe. The user may book a room via the website for a specific date, and the system will then automatically program the respective electronic locks provided at the respective hotels to allow the user to access the booked room at the specified date. In this manner, the user does not need to register when arriving at the hotel. Further, checkout can also automatically be performed. In addition, payment may also be handled automatically, for example, as soon as the booking has been confirmed by the user. As described above, additional services may also be included and/or booked by the user, for example,

-24-

access to a wireless network at the hotel, a breakfast room, a gym, or other recreational areas and the like. Further, a tablet or other computer may be provided in each room, which may read in the unique ID stored on the access card or receive any other form of authorization (password, code, etc.) and may be used to order additional services, for example, taxi services, food services, and the like, and also handle electronic billing for the additional services.

[69] In another embodiment, the disclosed system and method can also be used for airport lounges and the like. For example, as soon as a flight is booked, the system can configure the electronic locks associated with the respective lounges or lobbies such that the user having the corresponding access device may enter each lounge a predetermined time before its flight departs. Further, using the above-mentioned presence sensors, the occupancy of each lounge can be determined, and in case of several lounges at a given location, customers may be directed to specific lounges that are not fully occupied. Similarly, access to WiFi copy machines, electronic newspapers, or one or more tablets can be provided in each lounge offering the above-described additional services.

[70] It is explicitly stated that all features disclosed in the description and/or the claims are intended to be disclosed separately and independently from each other for the purpose of original disclosure as well as for the purpose of restricting the claimed invention independent of the composition of the features in the embodiments and/or the claims. It is explicitly stated that all value ranges or indications of groups of entities disclose every possible intermediate value or intermediate entity for the purpose of original disclosure as well as for the purpose of restricting the claimed invention, in particular as limits of value ranges.

Claims

1. A centralized access system (100) for controlling user access to a plurality of distributed facilities (10), comprising:
 - a plurality of electronic locks (12, 21, 42, 68) respectively associated with the plurality of distributed facilities (10);
 - at least one equipment (24, 26, 30) provided in the plurality of distributed facilities (10);
 - a data processing device (14) in communication with the plurality of electronic locks (12, 21, 42, 68) and the at least one equipment (24, 26, 30);
 - an access device (16) including a unique ID associated with a user;and
 - a database (18) configured to store information indicating a period of time during which the user has access to at least part of one or more of the plurality of distributed facilities (10) and the at least one equipment (24, 26, 30),
 - wherein the data processing device (14) is configured to control the plurality of electronic locks (12, 21, 42, 68) to selectively allow or deny access by the access device (16), and configured to selectively allow or deny access to the at least one equipment (24, 26, 30) by the user based on the information stored in the database (18).
2. The system of claim 1, wherein the at least one equipment (24, 26, 30) includes one or more of: a wireless or wired communication device (26) connected to the internet or an intranet; a printer (24); a network or standalone computer (30); a voice communication device (32) such as a telephone; a copier and other types of office equipment; a gym or another service area provided in the plurality of distributed facilities (10).

-26-

3. The system of claim 1 or 2, wherein access to the at least one equipment (24, 26, 30) is based on the access device (16), or on a code which has been generated based on the information stored in the database (18).

4. The system of any one of claims 1 to 3, wherein each electronic lock (12, 21, 42, 68) includes at least a first electronic lock (21, 42) and a second electronic lock (12, 66), each of the plurality of facilities (10) includes an entrance (20, 41) secured by the first electronic lock (21, 42) and a private room or meeting room (22, 66) secured by the second electronic lock (12, 68), and the data processing device (14) is configured to selectively allow or deny access to at least the private room or meeting room (22, 66) by the access device (16) based on the information stored in the database (18).

5. The system of any one of claims 1 to 4, further comprising a user interface (36) in communication with the data processing device (14), the user interface (36) being configured to allow the user to book access to one or more of the plurality of distributed facilities (10) for a specified period of time, wherein the data processing device (14) is configured to store the booked access time in the database (18).

6. The system of claim 5, wherein the data processing device (14) is configured to determine an occupancy of the plurality of distributed facilities (10) based at least in part on information stored in the database (18), and to cause the user interface (36) to display said occupancy to the user.

7. The system of any one of claims 1 to 6, further comprising at least one user detection device (28) configured to detect a user presence at each

-27-

of the plurality of distributed facilities (10), and a display device (40, 44, 56) configured to display said user presence.

8. The system of any one of claims 1 to 7, further comprising a code generation device that is configured to generate at least one access code upon a request by the user, and a code input device associated with one of the plurality of distributed facilities (10), wherein the data processing device (14) is configured to allow access to the one of the plurality of distributed facilities (10) when the code is input via the code input device (42).

9. The system of claim 8, wherein the data processing device (14) is configured to send a notification to the user when the code has been input via the code input device.

10. The system of any one of claims 1 to 9, wherein the plurality of facilities (10) include a plurality of shared office spaces provided at different locations, each shared office space comprising a plurality of public and/or private workspaces (22, 50, 52, 66).

11. The system of any one of claims 1 to 9, wherein the plurality of facilities (10) include a plurality of residential buildings, hotels, airport lounges, recreational facilities, or the like.

12. A method of controlling user access to a plurality of distributed facilities (10), comprising:

providing an access device (16) with a unique ID associated with a user;

storing information indicating a period of time during which the user has access to at least part of one or more of the plurality of distributed facilities (10) in a database (18);

controlling a plurality of electronic locks (12, 21, 42, 68) respectively associated with the plurality of facilities (10) to selectively allow or deny access by the access device (16) based on the information stored in the database (18); and

providing at least one service to the user at the plurality of facilities (10) based on the information stored in the database (18).

13. The method of claim 12, wherein the at least one service includes at least one of: allowing access to the internet or an intranet; providing access to a network or standalone computer; providing access to a voice communication device; allowing use of a copier or any other type of office equipment; providing access to a gym or another service area within the plurality of facilities; providing access to an entertainment system, for example, a video game machine or the like.

14. The method of claim 12 or 13, further comprising:
providing a user interface for booking access to one or more of the plurality of distributed facilities (10) for a specified period of time; and
storing the booked access time in the database (18).

15. The method of any one of claims 12 to 14, further comprising:
detecting a user presence at each of the plurality of distributed facilities (10); and
displaying the determined user presence on a display device (40, 44, 56).

-29-

16. The method of any one of claims 12 to 15, further comprising:

generating at least one access code upon a request by the user, the at least one access code allowing access to one of the plurality of distributed facilities (10); and

notifying the user when the at least one access code is used to access the one of the plurality of distributed facilities (10).

17. A computer program comprising computer-executable instructions that, when executed on a computer system, cause the computer system to execute the steps of:

storing information indicating a period of time during which a user has access to at least part of one or more of a plurality of distributed facilities (10) and to at least one equipment (24, 26, 30) provided in the plurality of distributed facilities (10) in a database, the information including a unique ID associated with the user; and

controlling a plurality of electronic locks (12, 21, 42, 68) respectively associated with the plurality of facilities (10) to selectively allow or deny access by an access device (16) including the unique ID associated with the user, and selectively allowing or denying access to the at least one equipment (24, 26, 30) by the user based on the information stored in the database (18).

18. The computer program of claim 17, further comprising instructions to cause execution of the following steps:

providing a user interface for booking access to one or more of the plurality of distributed facilities (10) for a specified period of time; and

storing the booked access time in the database (18).

19. The computer program of claim 17 or 18, further comprising instructions to cause execution of the following steps:

detecting a user presence at each of the plurality of distributed facilities (10); and

displaying the determined user presence on a display device (40, 44, 56).

20. The computer program of any one of claims 17 to 19, further comprising instructions to cause execution of the following steps:

detecting a user presence at each of the plurality of distributed facilities (10); and

displaying the determined user presence on a display device (40, 44, 56).

21. The computer program of any one of claims 17 to 20, further comprising instructions to cause execution of the following steps:

generating at least one access code upon a request by the user, the at least one access code allowing access to one of the plurality of distributed facilities (10); and

notifying the user when the at least one access code is used to access the one of the plurality of distributed facilities (10).

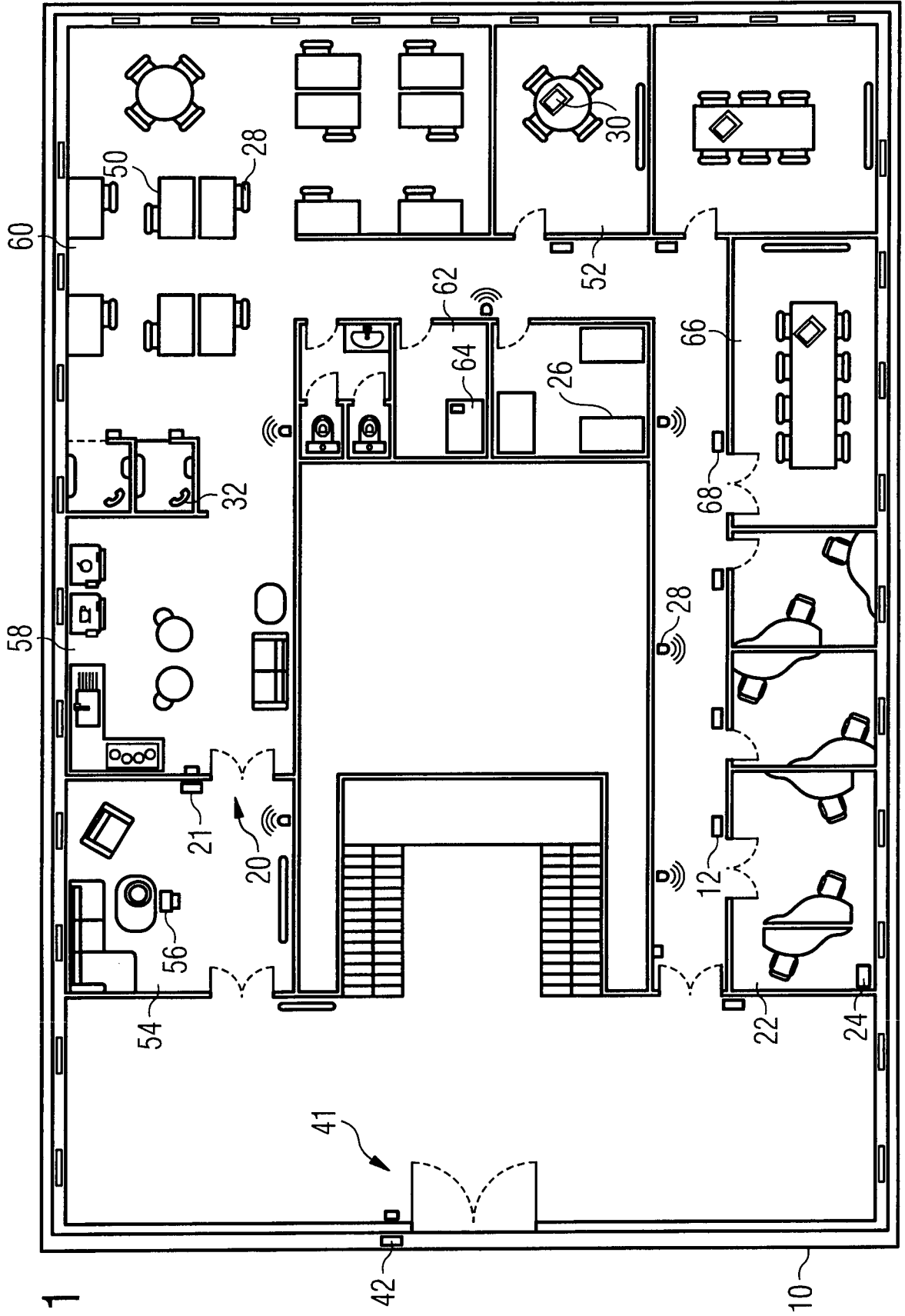
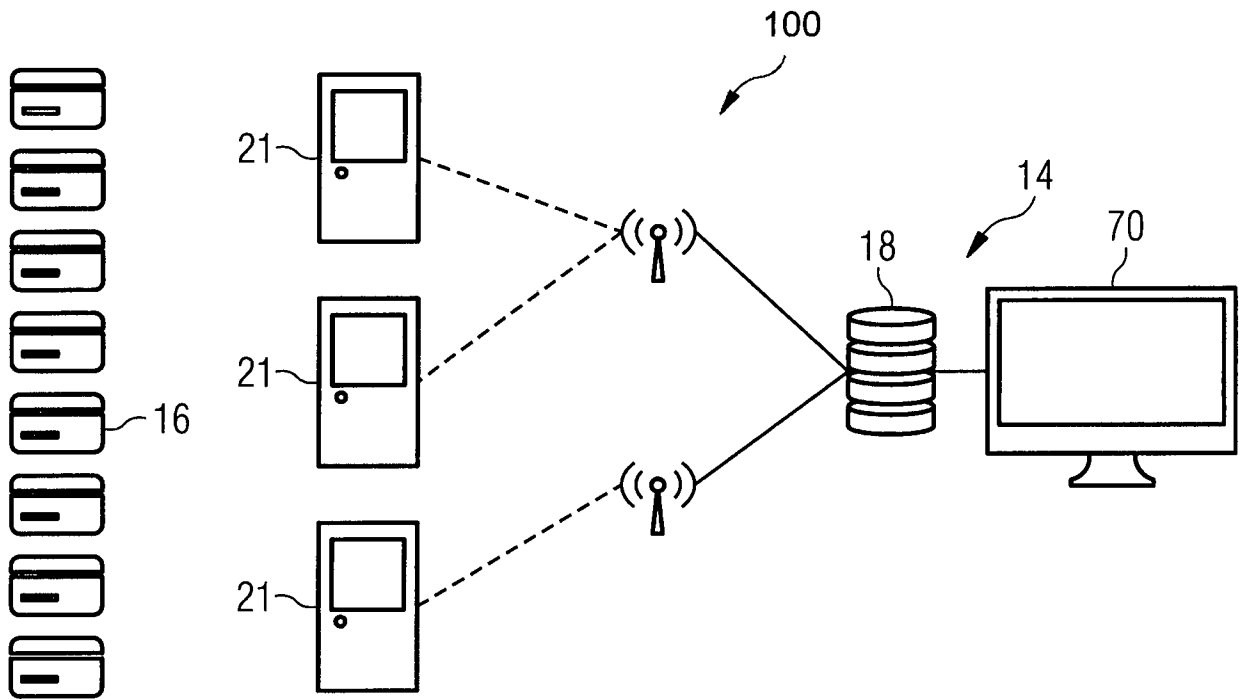


FIG 1

FIG 2



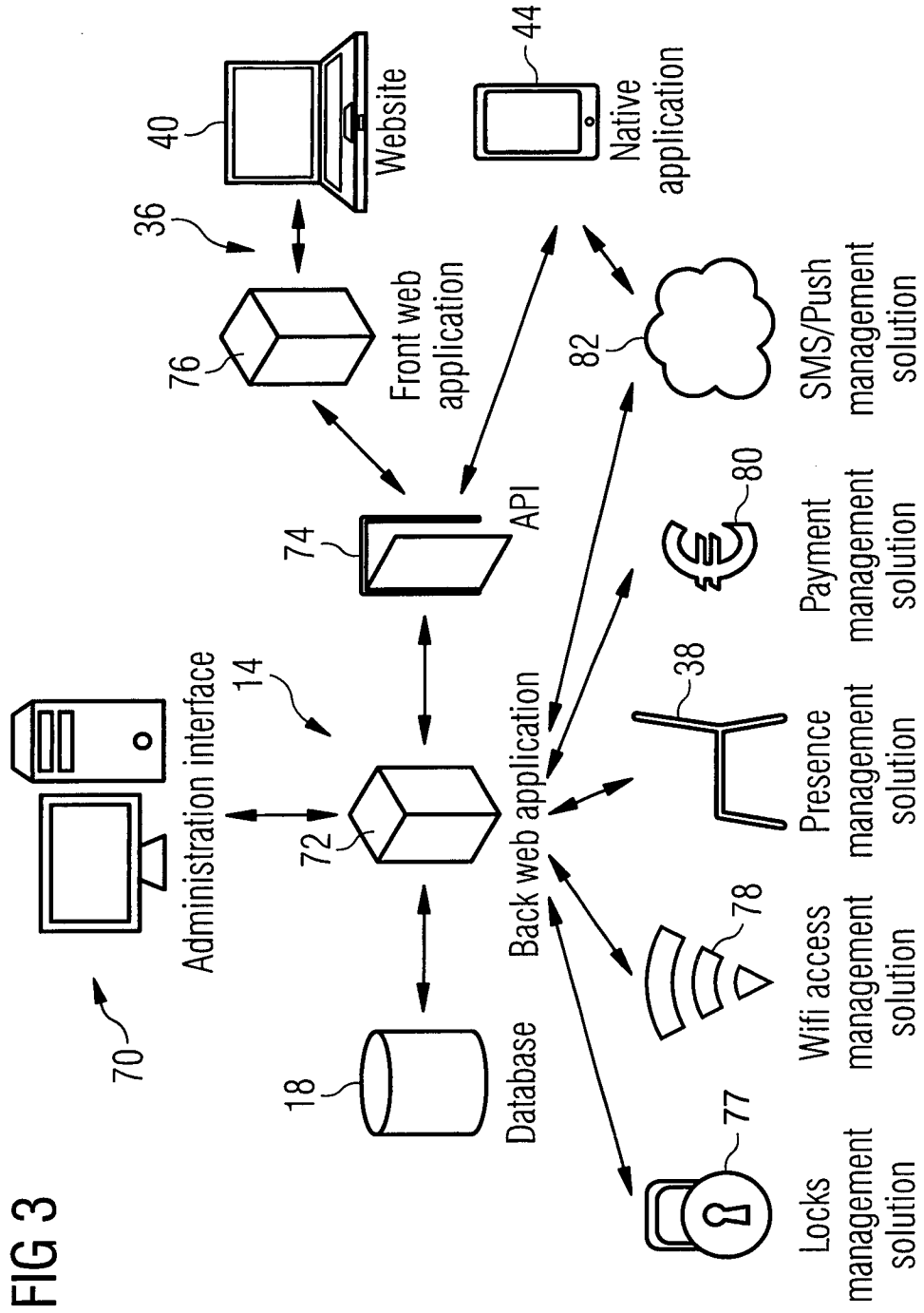


FIG 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/000828

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C9/00
ADD.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
G07C
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/002236 A1 (PINEAU STEPHEN [CA] ET AL) 2 January 2014 (2014-01-02) claim 1 claims 15, 16 paragraph [0054] - paragraph [0066] paragraph [0118] - paragraph [0125] paragraph [0135] - paragraph [0144] paragraph [0179] - paragraph [0182] paragraph [0209] - paragraph [0218] ----- -/--	1-6,8, 10-14, 17,18

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

Date of the actual completion of the international search

20 February 2017

Date of mailing of the international search report

03/03/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Hniene, Badr

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/000828

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/194000 A1 (SCHOENFELDER LUKE ANDREW [US] ET AL) 9 July 2015 (2015-07-09) figures 1b, 3, 5, 8 paragraph [0002] paragraph [0010] - paragraph [0011] paragraph [0026] - paragraph [0028] paragraph [0034] - paragraph [0046] paragraph [0059] - paragraph [0062] -----	1-3,5, 7-9, 11-21
X	US 2010/201536 A1 (ROBERTSON WILLIAM BENJAMIN [US] ET AL) 12 August 2010 (2010-08-12) figure 1 paragraph [0011] - paragraph [0012] paragraph [0017] paragraph [0025] - paragraph [0035] -----	1-5,8, 10-14, 17,18
X	US 2015/150101 A1 (NOVACK BRIAN M [US] ET AL) 28 May 2015 (2015-05-28) figure 2 paragraph [0026] paragraph [0033] - paragraph [0048] paragraph [0062] - paragraph [0068] paragraph [0075] paragraph [0085] - paragraph [0089] -----	1-4, 10-13,17
A	US 2013/024222 A1 (DUNN STEPHEN MARK [AU]) 24 January 2013 (2013-01-24) claims 1, 12 figure 3 paragraph [0063] paragraph [0078] - paragraph [0081] -----	1,3,5,6, 8,9,11, 12,14, 16-18,21

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No PCT/EP2016/000828

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014002236	A1	02-01-2014	NONE
US 2015194000	A1	09-07-2015	NONE
US 2010201536	A1	12-08-2010	NONE
US 2015150101	A1	28-05-2015	US 2015150101 A1 28-05-2015
			US 2016248770 A1 25-08-2016
US 2013024222	A1	24-01-2013	AU 2012222859 A1 10-10-2013
			CN 103548060 A 29-01-2014
			EP 2681387 A1 08-01-2014
			US 2013024222 A1 24-01-2013
			WO 2012116400 A1 07-09-2012