US 20120221473A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2012/0221473 A1

(43) Pub. Date: Aug. 30, 2012

Redmann et al.

(54) METHOD AND SYSTEM FOR USING A MOBILE DEVICE FOR SECURE ACCESS TO ELECTRIC VEHICLE SUPPLY EQUIPMENT

(76) Inventors: **William Gibbens Redmann**, Glendale, CA (US); **Chris Outwater**, Santa Barbara, CA (US)

(21) Appl. No.: **13/409,511**

(22) Filed: **Mar. 1, 2012**

Related U.S. Application Data

(63) Continuation-in-part of application No. PCT/US2011/026781, filed on Mar. 2, 2011.

(60) Provisional application No. 61/309,813, filed on Mar. 2, 2010.

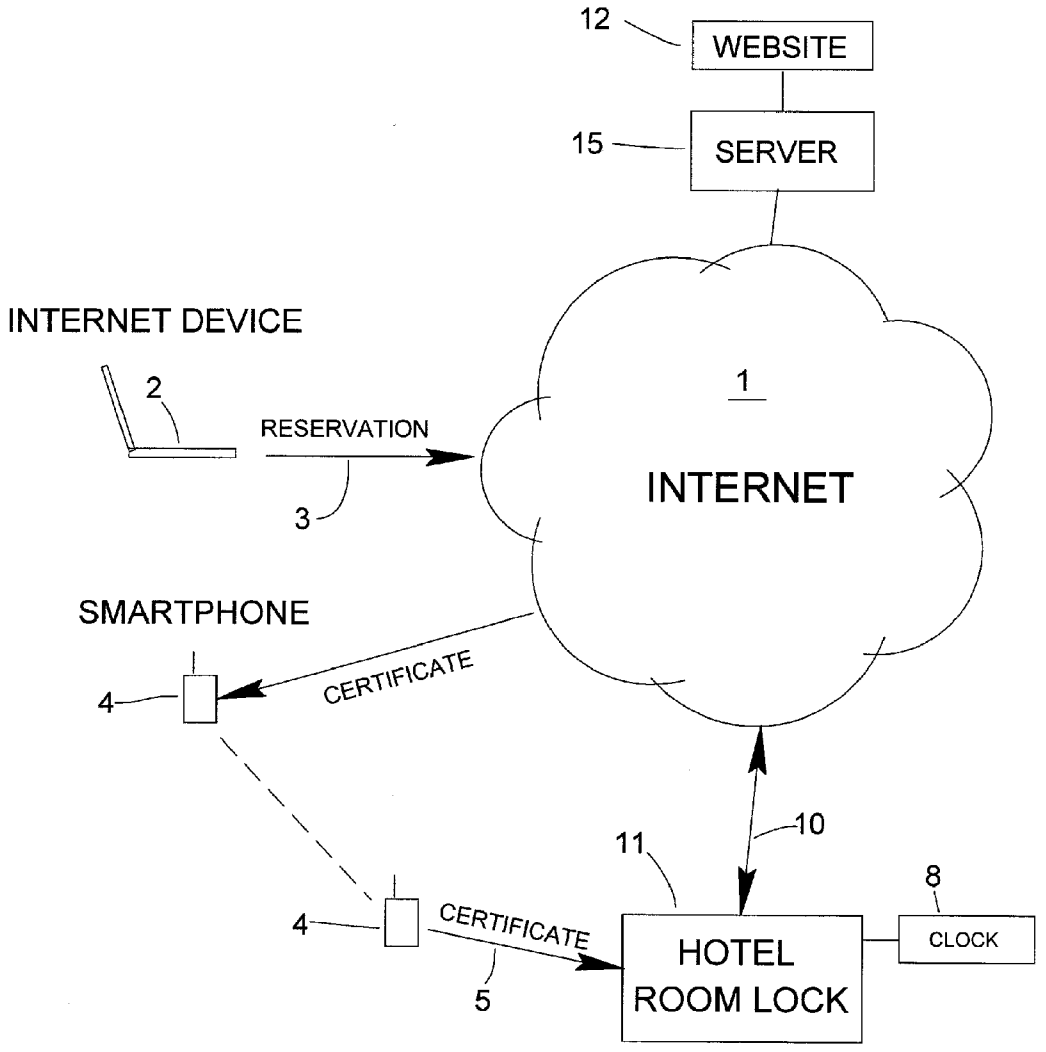
Publication Classification

(51) **Int. Cl.**
G06Q 10/02 (2012.01)
G06F 21/00 (2006.01)

(52) **U.S. Cl.** **705/50**; 705/5

(57) **ABSTRACT**

A systems and method are to allow a wireless telephone or any terminal to reserve and activate an electric vehicle charger using a web site or server computer system. An access control system is provided that includes a server and an access device. The access device includes an electrical vehicle charger. A reservation request is accepted from a first terminal using the server. A reservation certificate is provided to a mobile second terminal in response to the request using the server. The reservation certificate is accepted from the mobile second terminal using the access device and a communications technique like Bluetooth. The reservation certificate is determined to be authentic using the access device. The electric vehicle charger is activated in response to accepting an authentic reservation certificate using the access device.



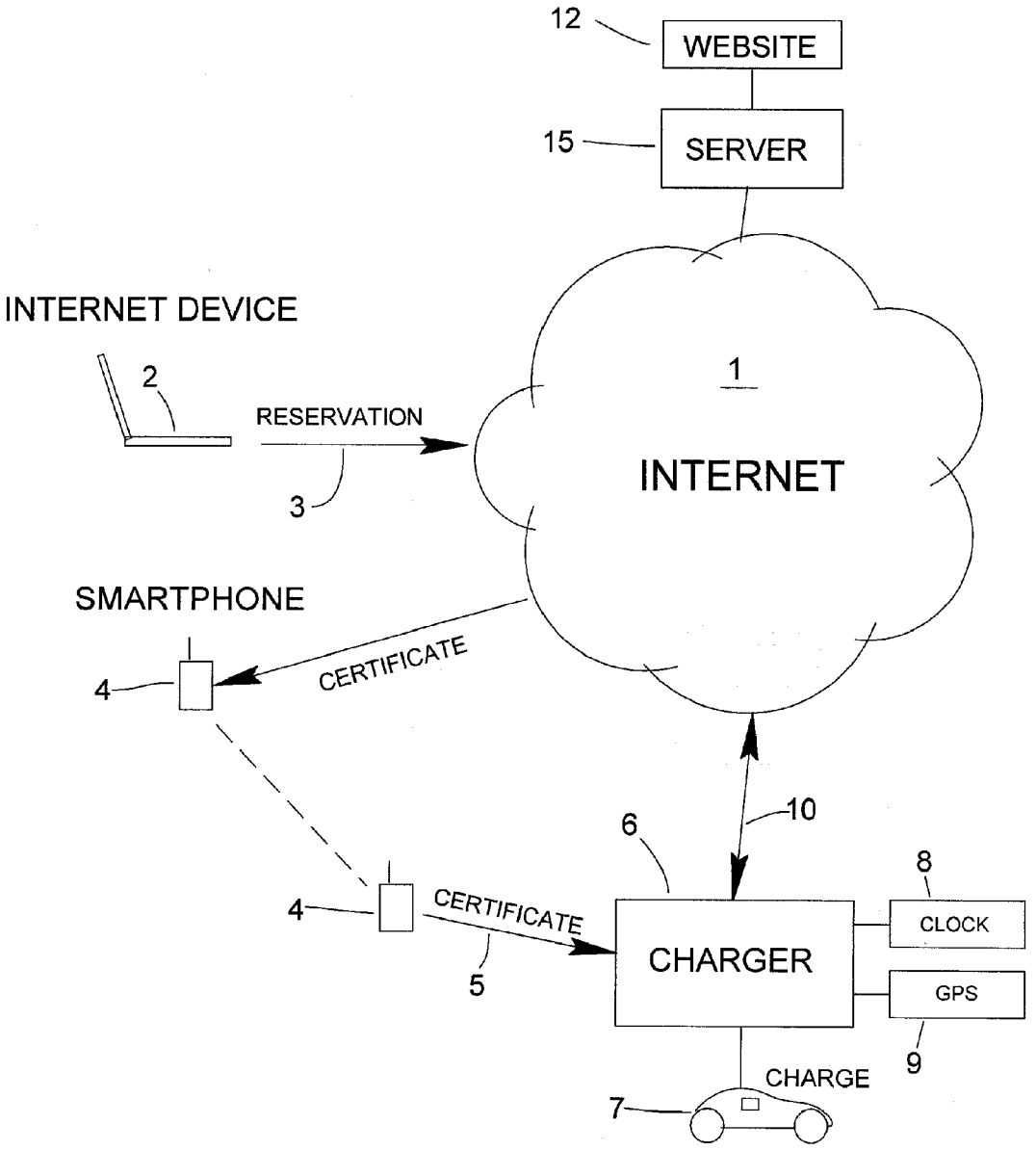

12
WEBSITE
15
SERVER
INTERNET DEVICE
2
RESERVATION
3
1
INTERNET
SMARTPHONE
4
CERTIFICATE
10
6
8
4
CERTIFICATE
5
CHARGER
CLOCK
GPS
9
CHARGE
7

FIG. 1

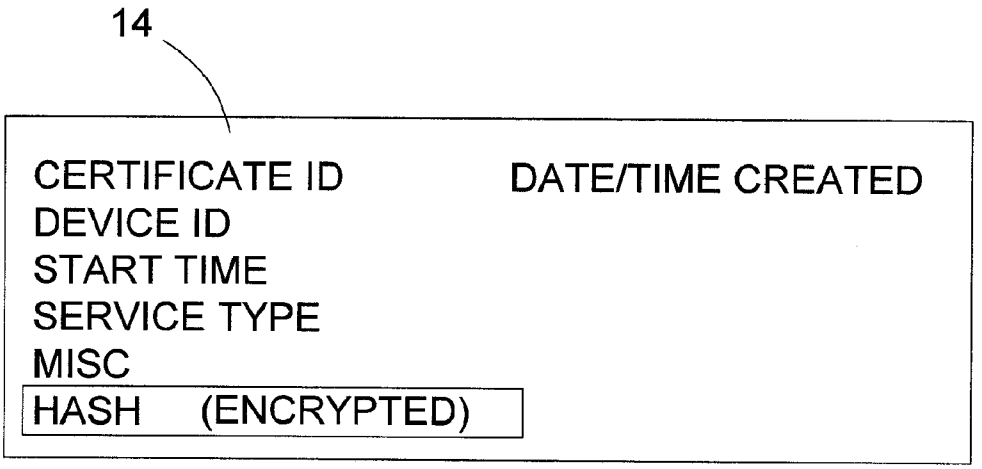

14
CERTIFICATE ID
DATE/TIME CREATED
DEVICE ID
START TIME
SERVICE TYPE
MISC
HASH (ENCRYPTED)

FIG. 2

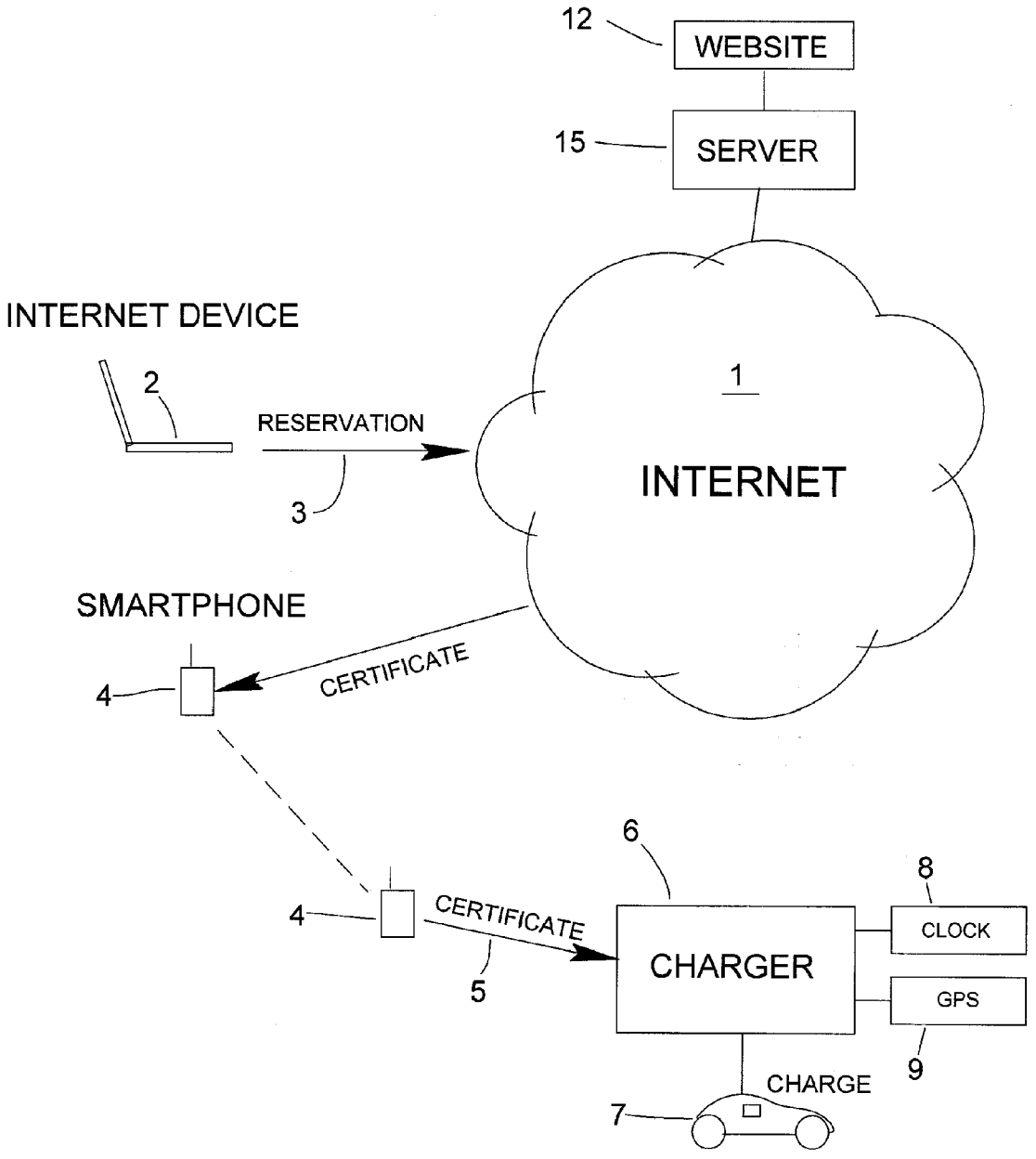

12
WEBSITE
15
SERVER
INTERNET DEVICE
2
RESERVATION
3
1
INTERNET
SMARTPHONE
4
CERTIFICATE
6
8
4
CERTIFICATE
5
CHARGER
CLOCK
GPS
9
CHARGE
7

FIG. 3

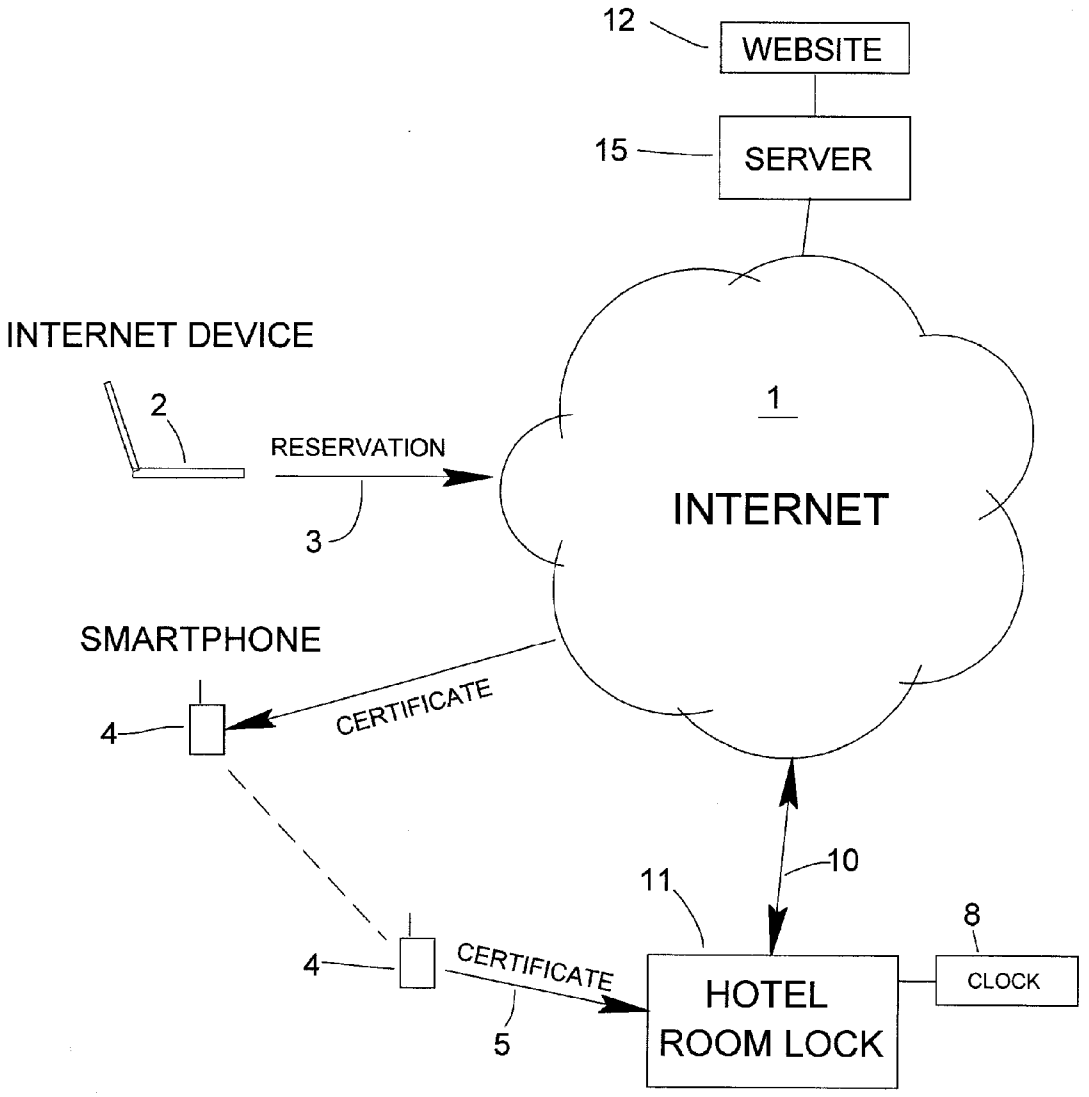

12
WEBSITE
15
SERVER
INTERNET DEVICE
2
RESERVATION
3
1
INTERNET
SMARTPHONE
4
CERTIFICATE
10
11
8
4
CERTIFICATE
5
HOTEL
ROOM LOCK
CLOCK

FIG. 4

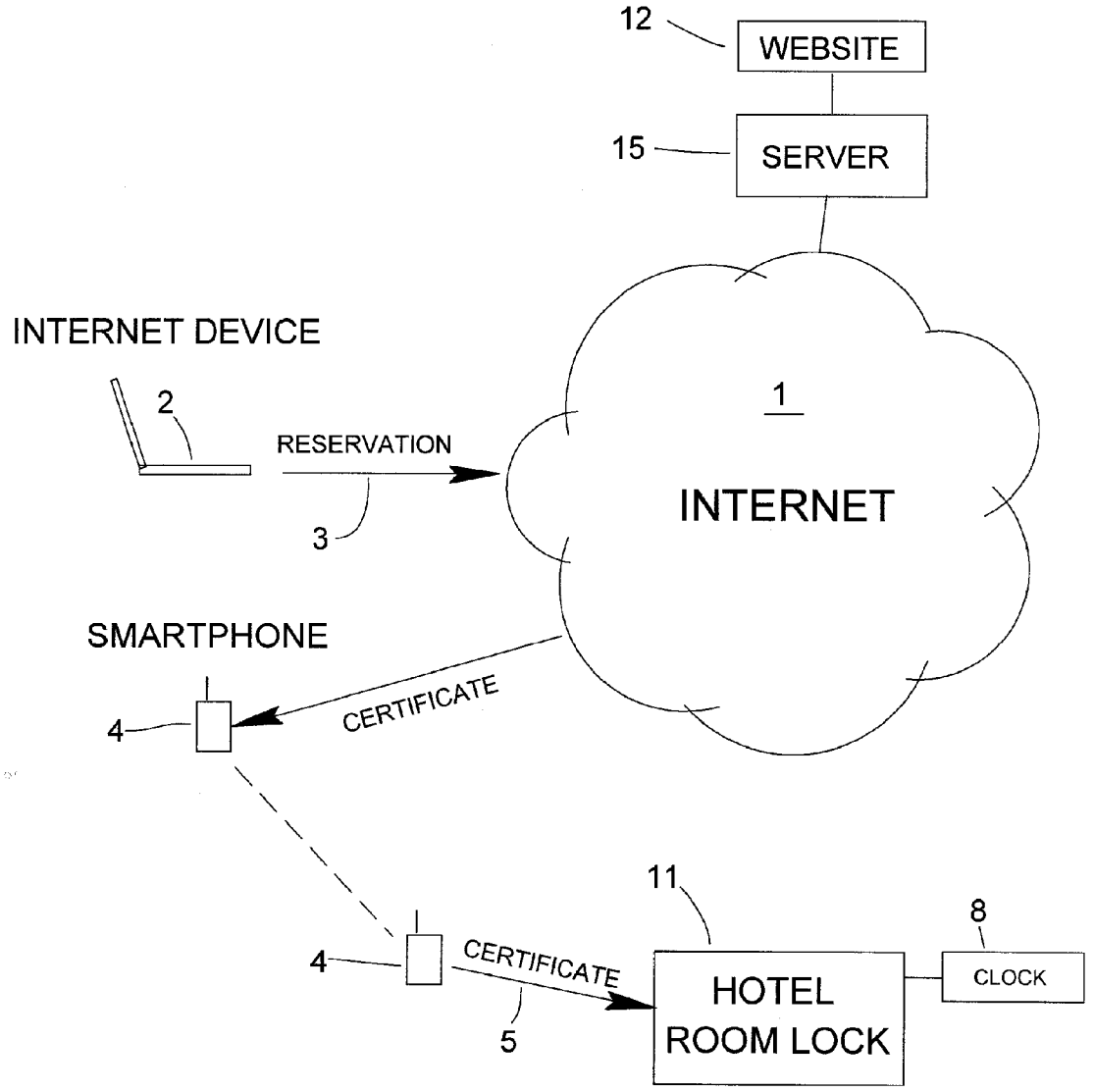

12
WEBSITE
15
SERVER
INTERNET DEVICE
2
RESERVATION
3
1
INTERNET
SMARTPHONE
4
CERTIFICATE
11
8
4
CERTIFICATE
5
HOTEL
ROOM LOCK
CLOCK

FIG. 5

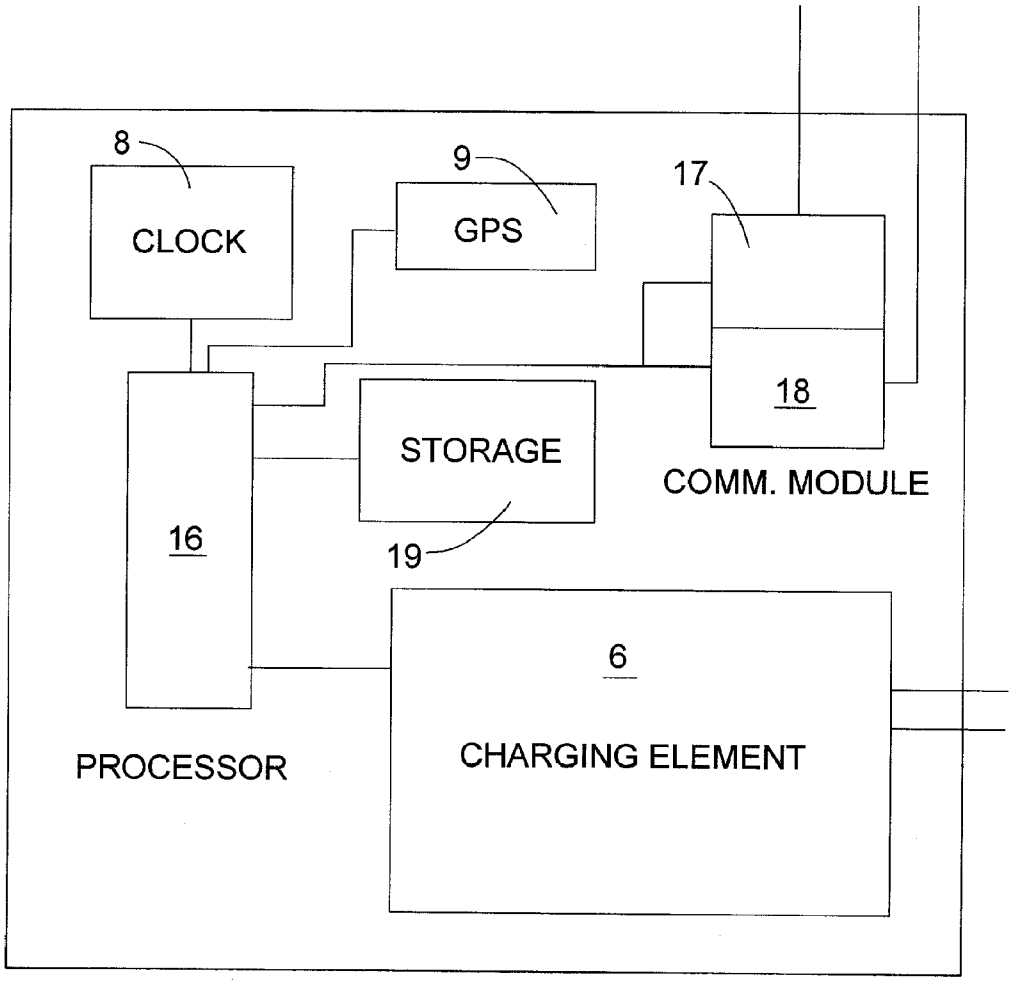

8
CLOCK
9
GPS
17
18
COMM. MODULE
STORAGE
19
16
PROCESSOR
6
CHARGING ELEMENT

FIG. 6

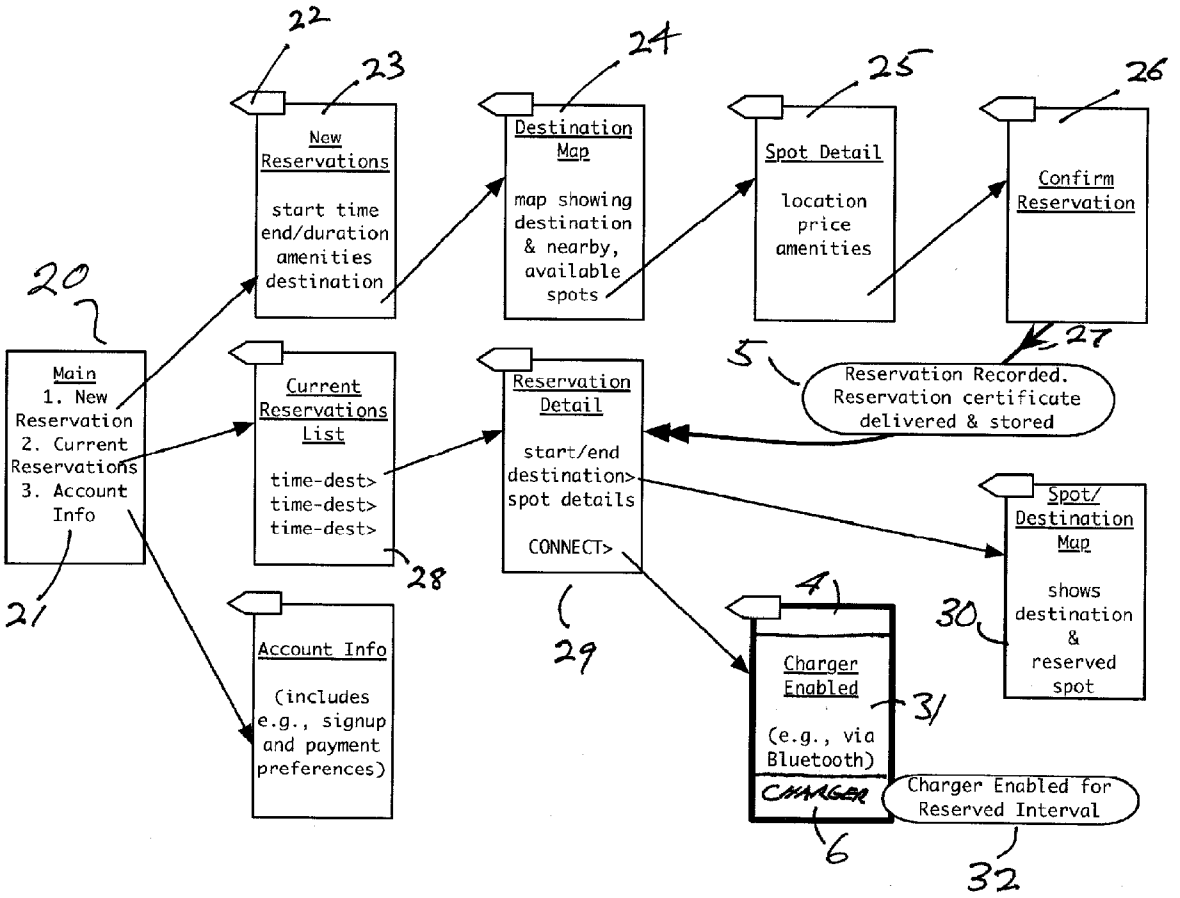

22
23
24
25
26
20
Main
1. New Reservation
2. Current Reservations
3. Account Info
21
New Reservations
start time
end/duration
amenities
destination
Destination Map
map showing destination & nearby, available spots
Spot Detail
location
price
amenities
Confirm Reservation
27
5
Reservation Recorded. Reservation certificate delivered & stored
Current Reservations List
time-dest>
time-dest>
time-dest>
28
Reservation Detail
start/end
destination>
spot details
CONNECT>
29
Spot/ Destination Map
shows destination & reserved spot
30
Account Info
(includes e.g., signup and payment preferences)
4
Charger Enabled
(e.g., via Bluetooth)
31
CHARGER
6
Charger Enabled for Reserved Interval
32

FIG. 7

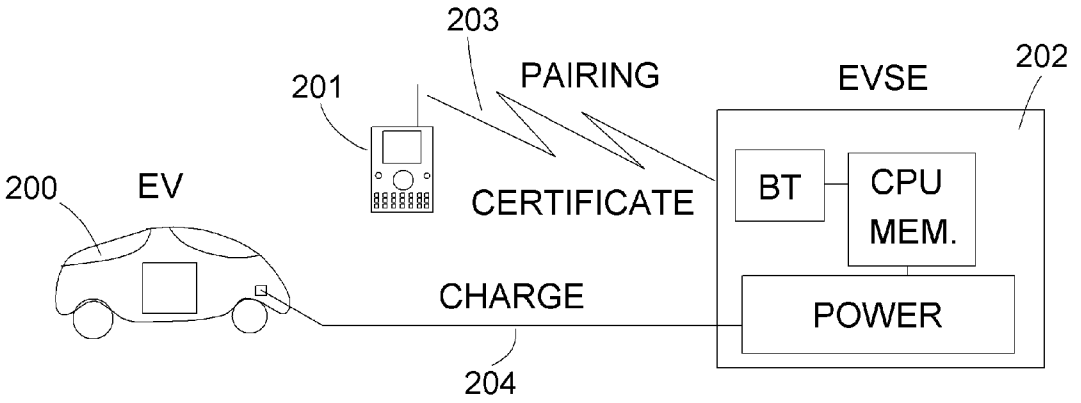

203
201
PAIRING
EVSE
202
200
EV
CERTIFICATE
BT
CPU
MEM.
CHARGE
POWER
204

FIG. 8A

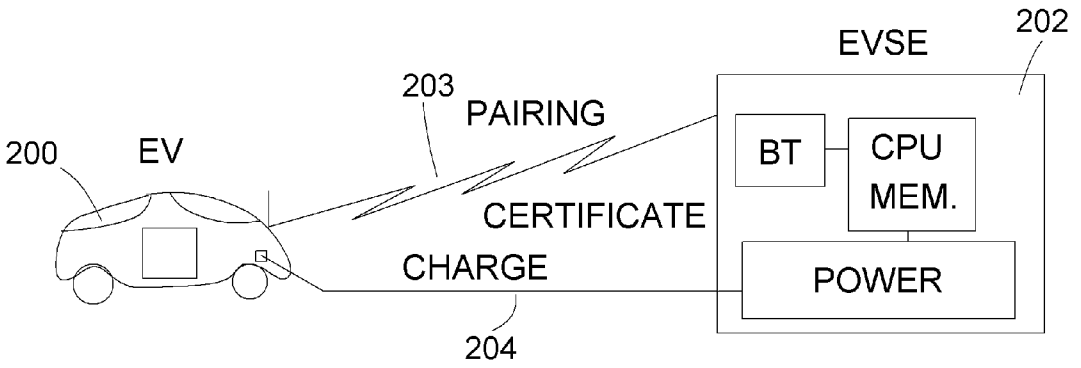

EVSE
202
203
PAIRING
200
EV
BT
CPU
MEM.
CERTIFICATE
CHARGE
POWER
204

FIG. 8B

METHOD AND SYSTEM FOR USING A MOBILE DEVICE FOR SECURE ACCESS TO ELECTRIC VEHICLE SUPPLY EQUIPMENT

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application is a continuation-in-part and claims priority to international application PCT/US11/26781 with international filing date of Mar. 2, 2011 and international priority date of Mar. 2, 2010. That application claimed the benefit of U.S. Provisional Patent Application No. 61/309,813, filed Mar. 2, 2010. Applications PCT/US11/26781 and 61/309,813 are hereby incorporated by reference herein in their entirety.

BACKGROUND

[0002] 1. Field of the Invention

[0003] The present invention relates generally to the field of access to devices such as chargers for electric vehicles and more particularly to a method and system for using a smart phone to allow this access.

[0004] 2. Description of the Prior Art

[0005] Electric vehicles (EVs) are rapidly gaining in popularity. With these electric vehicles, charge points, or Electric Vehicle Supply Equipment (EVSE) and often called "chargers" where the vehicle can charge its batteries, will also become ubiquitous. The simplest charger is simply a kiosk or charge station that a vehicle can plug into and charge. A fee or other access may be required to use this kiosk. In other situations, vehicles will be able to be charged at parking facilities, parking meters and even street lamps. Other electronic access devices such as hotel room locks and the like are also gaining in popularity.

[0006] EVSE can supply the needs of a large number of electric vehicles. A rich environment of EVSE with easy access to an electric charge is key to the growth of the EV industry. And also in certain situations it is important to control access to the EVSE so that only authorized motorists may use the services.

[0007] Given the progress of technology, the confluence of EVSE and wireless telephones such as cellular telephones and smartphones is inevitable. This will entail using communication protocols already in use in the radio frequency (RF) region as well as new ones. The most probable path, at least for the immediate future, is that EVs and wireless telephones will all be Bluetooth (BT) compatible (or compatible with further wireless techniques), so EVSE should also be Bluetooth (or other wireless) compatible to allow access control where needed.

[0008] A major problem with a random collection of charge stations is that a driver needing charge may have no idea exactly where to find a charging station that can charge his vehicle using the correct voltage and current, and may have no convenient way to reserve a place or make payments for this service. Of course, kiosks and the like can accept credit cards much like gas pumps; however, there still remains the problem of reservations and correct charging parameters.

[0009] Use of the Internet for almost everything has also become very common to many people today. A large percentage of fungible goods today are purchased directly from merchants over the Internet. It would be very desirable to have an easily accessed website that could provide reservation services for charges, including directions to the location of a specific charger and could provide correct charging parameters to that charger. This website could interact with a user's wireless telephone to provide an electronic token or certificate that could be temporarily stored in the phone that could be passed on to an access device such as a vehicle charger, hotel room lock or other access system to allow access and provide any necessary parameters.

[0010] Burger in U.S. Published Patent Application number 2010/0031043 teaches a mobile electronic authorization method for enabling a user interface on a computer operated by a user to cause the memory content of an electronic device distinct from the computer to be modified. Burger teaches using RFID tags to replace each typical document found in a person's wallet or purse. Burger fails to teach enabling a charger for an electronic vehicle.

[0011] In US Published Patent Application number 2007/0008181, Rollert et al. teach a "System and Method For Optimizing the Utilization Of Space", primarily parking spaces, by allowing a reservation to be made through the Internet.

[0012] It would be advantageous to have a system and method of reserving an electrical vehicle charger on a web page and then transferring a token or certificate to a wireless telephone which could then further transfer this token to the charger to authorize charging.

[0013] Since there will be a confluence between wireless telephones and EVSE, it would also be very advantageous to have a Bluetooth compatible system in which the EV motorist's phone would "pair" with the target EVSE as the motorist's EV approaches. This would take place in a fashion similar to the way a wireless phone currently pairs with a BT headset. This BT enabled connection will then allow for seamless access based on a secure, token or digital certificate sent via BT to the EVSE.

SUMMARY OF THE INVENTION

[0014] The present invention relates to the use of a web site and a wireless telephone, preferably a smart phone, to reserve and activate an electric vehicle charger or to activate and allow access to any access device such as a hotel room lock or the like. The web site can be general access or restricted access and can allow a user using a browser from a computer, laptop, web-capable wireless telephone, smart phone or any electronic processing device to place a reservation for a particular charger at a particular time window. A server or server computer not hosting a website can also interface directly with a telephone application. The server, or another server, can then transfer a digital token or certificate, which may be wholly or partially encrypted, to the wireless telephone. This certificate may comprise a unique ID and/or a date/time stamp.

[0015] The present invention also relates to a Bluetooth compatible system in which the EV motorist's phone "pairs" with the target EVSE as the motorist's EV approaches. This BT enabled connection then allows for seamless access based on a secure token or digital certificate sent via BT to the EVSE.

[0016] The motorist's phone knows to pair with the target EVSE because the motorist can first locate the EVSE on a map, choose it and reserve or purchase a charge duration on that EVSE. When a request is made for a target EVSE, the database can look to see if that EVSE had previously issued a code that would interfere with the time and charge duration being requested. If no interference is found, a transaction at

that EVSE is allowed. On the other hand, if there is interference, a neighboring EVSE might be offered. After a transaction, a digital certificate and the target EVSE ID #, which is unique to one or a group of EVSE at a specific location, is sent over the wireless network to the motorist's cell phone. Then the code can be sent via BT protocol from the motorist's cell phone to the target EVSE.

[0017] The certificate generally has an ID referring to the final access device (for example, a charger), or is encoded in such a way that only the final access device can read and/or verify the message (e.g., the certificate may be encrypted with or signed with a public key for the final access device); whereby the final access device can recognize that the certificate is intended for it. The certificate generally has a start time and duration (or end time), describing the interval during which the final access device has been reserved. Additional options may also be included.

[0018] The certificate can also contain a digital authorization (for example, a digital signature) so that the final access device can verify that the certificate is genuine. Each charger or other access device in a particular system may have a unique ID, which can be changed for security.

[0019] The certificate can also contain this charger or device ID as well as other information such as approximate time when charging should begin (the reservation time), and the charging parameters.

[0020] If a wireless device, such as a laptop or wireless telephone, is used to carry the certificate, it can be running an application that turns on Bluetooth or other short-range wireless capability as the reservation time approaches. While the term wireless telephone is being used for simplicity of discussion, any type of wireless communication device is envisioned and is within the scope of the present invention. Each such device contains a processor, memory and at least one communication module.

[0021] As the smart phone approaches the charger or access device, a wireless connection is made (e.g., via Bluetooth, Zigbee™, IRDA, or by other wireless means); notification may be provided to the user of the device's proximity; and the wireless device sends the digital token or certificate to the device. The device can be optionally Internet enabled; however, it does not have to necessarily be. In fact, the present invention is particularly useful for devices that may generally be Internet connected, but for which the connection is unreliable, for example, for chargers employing Wi-Fi connection in a garage or private residence. In such cases, an inopportunely placed truck or other obstacle may block communication, or a weakly secured or informally managed modem and/or router may not provide a sufficiently reliable communication. When the device sees its current unique ID on the received certificate or if the device's private key is usable to decrypt at least a portion of the received certificate, and if the reservation time from the certificate approximately agrees with its internal time-of-day/date clock, the device can allow charging. Communication with the smart phone may also include a message as to the smart phone's own clock-calendar, which may be taken into account for adjusting the clock of the device (as the smart phone may have had more recent connection to an authoritative time source.)

[0022] The incoming digital certificate can contain a new, updated unique ID for that charger or access device to assume. Upon assuming the new ID (after charging is complete or access is allowed), the old ID is no longer valid. This prevents hacking or spoofing the device by trying to use the same certificate twice (say by changing the date/time). The certificate can also contain a new encryption decoding key for the next use. This prevents any decoding of an old or used token or certificate. In this case, since the transaction may not take place (for example, the customer could not find the charger), it is possible for the state of the charger to become ambiguous. It is possible to issue reservations with both the old certificate and the new certificate present simultaneously.

[0023] Funds transfer for the access service can be made by the website at the time of reservation from a user's account, from a money transfer service like PAYPAL™ or by receiving funds from a credit card similar to any other e-transaction. In addition, if the charger or access device is web-enabled, the device itself can report back that the charging took place or the access was allowed. Since the digital token or certificate has a reserved charging time, the certificate will generally die automatically a certain number of minutes or hours after that time in that the charger or access device will no longer allow access based on its time-of-day/date clock.

DESCRIPTION OF THE FIGURES

[0024] Attention is now directed to several illustrations that show some of the features of the present invention.

[0025] FIG. **1** shows a flow diagram of a reservation and charge from a web-enabled charger.

[0026] FIG. **2** shows an embodiment of a digital token or certificate.

[0027] FIG. **3** shows a similar flow diagram to that of FIG. **1**, except that the charger is not web-enabled.

[0028] FIG. **4** shows the flow with a web-enabled hotel room lock.

[0029] FIG. **5** shows the flow of FIG. **3** with a hotel room lock that is not web-enabled.

[0030] FIG. **6** shows a block diagram of a charger that might be used with the present invention.

[0031] FIG. **7** shows a block diagram of an embodiment of a smart phone application.

[0032] FIG. **8**A shows an EV pairing and connecting with an EVSE using a wireless telephone.

[0033] FIG. **8**B shows an EV pairing and connecting with an EVSE using Bluetooth on the EV.

[0034] Several illustrations and drawings have been presented to aid in understanding the present invention. The scope of the present invention is not limited to what is shown in the figures.

DESCRIPTION OF THE INVENTION

[0035] The present invention allows reservation and activation of an electric vehicle charger or an access device like a hotel room lock from a website via a digital token or certificate sent to a wireless telephone or smart phone. In this description, the terms mobile or mobile device may be used to describe a cellular telephone, smart phone, enabled vehicle or other device. In this application, mobile can also mean portable; however, not every mobile device must be portable.

[0036] FIG. **1** shows a flow diagram of an embodiment of the present invention. A website **12** is hosted on a server **15** that communicates with the Internet **1**. An Internet terminal device **2** such as a laptop or wireless telephone has communication with the server **15**, browses the site **12** and initiates a reservation request **3** for charging or access. The website can be either open or secure. If secure, then generally a password

is needed to access it. Communications security protocols such as https or IPSec may be used in any part of the system of the present invention.

[0037] The website **12** or server **15** can contain information about different services available including the location of possible vehicle chargers **6**. The website or server will generally have a database which lists all chargers/locations (including possible maintenance closures) and all current reservations along with their status. The user can select where he wants to be charged or can be directed to the nearest charger in the system. The reservation **3** can be let for a certain time when charging will begin on a certain date. The user can also supply any parameters concerning charging necessary such as voltage/current requirements, time needed and the like.

[0038] After all of the information is gathered, the website causes the server **15** to send a particular digital token or certificate (a "reservation certificate" **5**) to a particular mobile terminal, e.g., a wireless telephone or smart phone **4** that the user specifies (which may the phone being used to make the reservation, but it does not need to be). All or part of the digital certificate may be encrypted with a public key for which the private key counterpart is known to only one charger or access device. Similarly, all or part of the digital certificate may be encrypted with a symmetrical key, known to both the server and the charger. All or part of the digital certificate may be encrypted with a private key known only to the server, but for which the public key is known to all compatible chargers, whereby the chargers can authenticate that the encryption was performed by the server. The certificate can contain a unique charger ID code for the target charger **6** or device, the date/time the certificate is issued, the date/time the charging is supposed to take place, the charging parameters, the charging time allocated, a new charger ID code that will replace the old ID, and optionally a new encryption key. Additionally, the certificate can contain communication information necessary to contact the device when in proximity to it, as discussed below. It is also possible that various portions of the message can be in plaintext. This makes it easier for a device to determine if any of many messages is for it without requiring decryption of every message. In this case, part of the certificate can include a hash of portions of the plaintext that would otherwise be exposed to tampering. The hash can then be encrypted by the server (e.g., with the server's private key) so that a charger or device is able to determine the authenticity of the certificate (by decrypting the hash with the server's public key and comparing that hash to one computed from the plaintext).

[0039] The charger **6** (or access device **11**, shown in FIG. **4**) may be Internet capable, having connection **10** to Internet **1**, or optionally it may be unconnected to the Internet **1** (as shown in FIG. **3** and FIG. **5** with no connection **10**). As the wireless telephone **4** approaches the charger **6** (or access device **11**, shown in FIGS. **4** & **5**), a wireless technology such as BLUETOOTH, Wi-Fi, Zigbee, infrared, or other wireless technique can be used to communicate with the charger or access device.

[0040] The charger may use these wireless techniques in a manner that does not advertise its presence, for instance, the BLUETOOTH service may not announce itself. In such cases as these, the application on the smart phone uses a predetermined communication setting, or obtains the appropriate communications settings (such as the network SSID, pass codes, IP addresses, Bluetooth ID, etc.) needed to contact the charger. In fact, with certain information (e.g., the Bluetooth ID) will allow the application to identify and communicate with a specific one of many chargers in proximity.

[0041] After a short communications handshake, the digital token or certificate **5** is sent to the charger or access device by short-range wireless. The charger **6** decrypts the certificate, if encrypted, reads the unique device ID, and decides if it is the correct device. If so, it reads the reservation time. If the reservation time approximately agrees with the time of day read from its internal time-of-day/date clock **8**, it then decodes the charge parameters or access parameters, if any, and allows charging or access to take place. FIG. **1** shows a vehicle **7** being charged, and it shows the charger **6** with a time-of-day/date clock **8** and an optional GPS receiver **9**. If the charger contains a GPS receiver, its identification can be by location, provided the charger has GPS access. This generally requires clear sky. The known coordinates or location of a charger can also be entered during installation, either from a map or predetermined table or from a GPS carried by an installer. If the charger **6** or access device **11** is Internet enabled (i.e., having connection **10**), it can communicate with the website application via long-range wireless such as cellular or by wire access, or it can communicate with an Internet access point by Wi-Fi or the like.

[0042] FIG. **2** shows a sample certificate **14** (one embodiment of certificate **5**) containing several fields of data representative of the reservation:

[0043] In some embodiments, one field is provided that can associate the certificate with the charger, such as a device identification (Device ID) of the charger **6** (so that the charger will have some suggestion that this is a message for it);

[0044] Start Time: this can be in plaintext so that the smart phone application can read it also;

[0045] Duration/End Time: if the reservation is not just for a predetermined time like all day for example;

[0046] Service Type: for example level 1 charging vs. level 2, if the charger supports multiple services.

[0047] For security, in some embodiments, the first portion of the certificate can be hashed, and the hash encrypted using the public key of the charger. Upon receipt by the charger, the hash is decrypted using the private key of the charger, and the hash result compared with the charger's internal hash calculation. If the two match, then nobody has edited the reservation and the certificate may be trusted as authentic. This is safe unless someone cracks the key of the charger. In that case, only one charger **6** is affected. An alternative embodiment may use a signed hash or checksum. Here, the hash is computed as above, then encrypted with a private key held by a trusted authority such as the website. Upon receipt, anyone, including the smart phone and the charger, can use the trusted authority's public key to decrypt the hash and compare that to the hash they run. This method is safe unless someone cracks the private key of the website. In still another embodiment, a Signed-then-Encrypted Hash/Checksum is used. Here the signed hash is encrypted so that only the charger can read it. This way, the private keys of both the charger **6** and the website server **15** need to be compromised, and then only that charger is threatened.

[0048] The certificate **14** can contain a certificate ID that is unique only to this certificate that can be used for tracking and debugging. The date/time the certificate was issued, again for tracking and debugging, a unique device ID of the target device, the reservation start time and duration, any charging

parameters needed, an optional new device ID for the next session and an optional new decryption key for the next session.

[0049] When charging or access is complete, the charger **6** or access device can update its ID to the new ID supplied by the previous certificate and optionally update its decryption key (if encryption is used). If the charger is Internet capable **10**, it can notify the website **12** that the charging is complete or that the changeover has taken place.

[0050] FIG. **3** shows the flow of FIG. **1** with the charger **6** not having Internet access. FIG. **4** shows an Internet capable access device **11**, in this example a hotel room lock, having connection **10** to Internet **1**, while FIG. **5** shows an access device **11** (again a hotel room lock) that cannot communicate over the Internet. In the case of a hotel room, a room reservation can be made using an Internet-enabled wireless telephone **4**, laptop **2**, computer or other Internet device. The room can be paid for in the usual e-commerce way by credit card or by any other payment method. The digital token or certificate is sent to the smart phone **4**, and the user is told the external room number. As the guest approaches the hotel room door, the smart phone **4** sends the certificate **5** to the lock device by way of short-range wireless like Bluetooth. A light on the device might light up or change colors as the authenticated phone comes within range of the device. The user can then unlock the door at any time during the stay period by pressing a particular button on the phone or by other technique. The phone can re-send the unique (and secret) access device ID to the device so that the device knows it is the correct person each time access is requested.

[0051] FIG. **6** shows a block diagram of a charger system **60** that is an embodiment of the charger of the present invention. A processor **16** is tied to a communication module **17** that performs short-range communication with a wireless telephone or smart phone and allows certificate **5** to be transferred from the cellular/smart phone through processor **16** to a storage module **19**. The processor **16** or storage module **19** may comprise the private key for the charger **6** and/or may store a public key (e.g., of server **15**) to verify digital signatures (e.g., those made with the server's private key). The storage module **19** can be any type of disk, memory or mass storage device. A clock **8** and/or GPS receiver **9** are also connected to the processor **16** to provide the current time. The processor **16** directly controls access to a charging element **6**, i.e., enabling charging element **6** when a currently certificate **5** has been presented, and disabling charging element **6** otherwise. An optional long-range communication module **18** can communicate with the Internet either by placing a wireless telephone call or with Wi-Fi or the like.

[0052] Optionally, the application on a wireless telephone **4** can energize short-range communication when the local GPS in the phone indicates that the phone is near the target charger **6**. The smart phone can also optionally signal that the vehicle needs a charge, or that a particular charge reservation time is approaching. The system of the present invention can also optionally track motorists' visits and purchases at retail stores in a mall or shopping center, and have automatic credits that can be added to the smart phone good toward future vehicle charging paid for by merchants as an incentive to purchase from their stores.

[0053] FIG. **7** shows how the present invention represents an improvement to the system and method of Rollert et al. (US Patent Application Publication 2007/0008181 previously mentioned), enabled by a smartphone application that could, for example, run on an iPhone™ by Apple, Inc. of Cupertino, Calif. or other smart phone such as an Android™ based system. Such an application would have a various screen views for performing such functions as making a new reservation, examining current reservations, and maintaining the patron's account. Some portions of the application require connectivity to the Internet to operate, but other portions may operate based on locally stored information. A few related operations, including examining current reservations, should be able to operate without Internet access, as the user may require immediate access to these operations, but be in a location such as in a parking garage where Internet access such as cell communication or Wi-Fi may not be provided.

[0054] In the diagram of FIG. **7**, a main application view **20** is shown to offer three options: New Reservation (for creating a new reservation), Current Reservations (for examining and using reservations already made), and Account Info (for creating and editing appropriate account information). FIG. **7** shows a smart phone application block diagram for an embodiment in which Internet device **2** and smart phone **4** are the same device: In another embodiment, the reservation-making portion of the application may run on Internet device **2** and the current reservation portion of the application may run on the smart phone **4**.

[0055] The patron would have selected the Account Info **21** at least once to create or otherwise associate an account with the patron's smart phone **4**. An account may have associated payment preferences and perhaps acceptance of legal agreements. Payment preferences might include a credit card account, or a bank account. Another payment preference would provide permission to pre-charge a patron's credit card or bank account and subsequently allow the system to operate using micro-payments made against that pre-charge amount. The parking reservation server **15** (or web site **12**) or another server with which it has communication (not shown) would maintain the micro-payment accounts for each patron and apply their funds to charges for parking. The micro-payment accounts would be settled daily or with a different period, or whenever the pre-charged amount has been consumed.

[0056] Once the patron's account has been enabled, the patron can access the views for creating a new reservation.

[0057] The New Reservations **23** screen accepts a start-time, an end-time (or duration), and a destination. Required amenities can be selected, including for the present invention, available charging for an EV (which may further include a selection for Level 1 or Level 2 charging, for instance). The destination may be an actual parking location, but more commonly (and as illustrated herein) it is the patron's destination for which nearby parking is sought.

[0058] As with each screen in this diagram other than the Main view **20**, there is a 'back' arrow **22** atop the screen including the New Reservations screen **23**. The back arrow **22** is a user interface element that permits the patron to move back up the hierarchy to access screens and their interfaces higher up.

[0059] Once a destination has been entered into the New Reservation screen **23**, the user may be presented with the Destination Map screen **24** showing a map with the destination marked and parking spots nearby shown and selectable. The spots shown may be only ones having the stated amenities and that are available to be reserved for the interval entered such as beginning from the start-time and available for the duration or until the end-time. Current information regarding parking spot availability requires communication

with the server responsible for maintaining reservations for that spot, which may be server **15**, web site **12**, or some other server.

[0060] Alternatively, the spots may be shown in a list, which may be sorted by their distance from the indicated destination, or by price, or by available service, whether Level 1 or 2 or DC fast charge, or a combination thereof.

[0061] The patron selects a parking spot, whether from a corresponding marking on the map, or from the spot list (not shown). Once selected, the Spot Detail screen **25** is shown, which includes information such as location, pricing, detailed amenities, and perhaps a picture of the specific parking location (or one representative of it).

[0062] If the patron does not like the parking spot presented, the back buttons allow returning to screens earlier in the interaction to make different selections, e.g., to choose a different spot or alter the start-time, etc.

[0063] If the patron does like the parking spot presented, he can confirm the reservation **26**, which initiates a reservation request to the server. Upon successfully obtaining a reservation for an EV charging enabled parking location, the server in response can provide or authenticate **27** a reservation certificate **5** to be stored in the smart phone **4**. For instance, in one embodiment, reservation certificate **5** comprises data representative of the reservation encrypted with the server's private key. In another embodiment, reservation certificate **5** comprises a digital signature by the server that authenticates data representative of the reservation. The completion of the reservation transitions the patron to a different region of the application screen hierarchy, and instead of being in the 'new reservation' branch (**23**-**26**), the interface jumps to a location in the 'current reservations' branch (**28**-**31**), such as the Reservation Detail page **29**, showing the reservation just made.

[0064] Another way of getting to the Reservation Detail screen **29** begins back on the Main application view **20** when the patron selects the current reservations option. Upon doing this, the Current Reservations List **28** is shown, which lists all pending parking reservations, for example in order of the date and time at which the reservation starts. Besides the start time, each entry in the list should show some additional information to remind the patron of each instance, for example the destination may be presented.

[0065] Upon selecting one of the reservations from the Current Reservations List **28**, the corresponding Reservation Detail screen **29** is shown, listing the same details that were selected and known when the reservation was made. Clicking on the destination entry on this screen can bring up a Spot/Destination Map screen **30**, showing the location of the parking spot with respect to the destination.

[0066] The Reservation Detail screen **29** also presents a connect option to direct the smart phone application to attempt communication with the EV charging system **4** (or other parking spot amenity system or access device **11**, e.g., a hotel room lock) and to provide the reservation certificate **5** to the charger **6** or device (**11**), thereby enabling it **32** for the interval of the reservation.

[0067] The Charger Enabled screen **31** can be used to monitor the connection attempt and confirm activation resulting from a successful connect action, and may also initiate a timer (not shown) on the smart phone to generate an alert as the parking interval is about to expire.

[0068] We have previously disclosed a method for gaining secure access to EVSE based on a keypad and a code that is keyed in to the keypad by the motorist. This method, similar to a car wash, is accepted in the market as a viable approach.

[0069] The approach using Bluetooth (BT) communications frees the motorist from keying in a code and allows us to send a more complex, digital certificate, including date and time and duration information instantaneously to the motorist's wireless phone. Then the code can go securely from the motorist's phone, or from the motorist's EV itself in another embodiment, to the target EVSE.

[0070] This has the added value of allowing usage and reporting back from the EVSE to the wireless phone and in another embodiment directly to the EV. Another feature would be the ability of the EVSE to report a fault, or any service notification through the motorist's wireless network back to a remote database.

[0071] When the EV charge session ends, usage data will be sent via BT to the motorist's phone, or EV, and will automatically be sent up to the network and to a remote database for storage and reporting, as needed. This can be called a "data mule" method.

[0072] At this time many vehicles, not just EV's, have and will have BT connections in the driver and passenger area of the vehicle. This concept can then use the motorist's wireless telephone to make the connection via BT to the BT controller on the EVSE. That range currently is defined by BT and depends on the broadcast power level of the wireless telephone and the EVSE. In the future, EV's and other vehicles may add a more powerful, forward-looking BT system (or other wireless system) that emanates from the vehicle, perhaps in all directions. In the short term, it is also possible to provide a BT amplifier for the dash board of the vehicle to increase BT range.

[0073] While we are describing EVSE at this time; however, embodiments of the present invention can also access various services such as parking lots or spaces with BT enabled gates and utilities meters with BT from a vehicle.

[0074] The following is a use case description give by way of example. The scope of the present invention is not limited by this or any other example.

[0075] A motorist with an EV wishes to find and access EVSE by using his wireless telephone or the dashboard of the EV.

[0076] The present invention unfolds in the following phases:

[0077] Phase 1 uses the motorist's wireless telephone as MASTER and the EVSE or parking meter as SLAVE. The range is limited and defined by BT protocol from the motorist's wireless telephone and the range of the BT transponder in the EVSE. FIG. **8**A shows a block diagram of this embodiment. An EV **200** approaches an EVSE **202**. The motorist uses a wireless telephone **201** to Pair with the EVSE **202** wirelessly **203**. An identification and certificate is sent from the telephone **201** to the EVSE **202**, and upon authentication and checking that the certificate is within the proper date/time, charging **204** is enabled.

[0078] Phase 2, is an intermediate phase in which motorists wish to amplify their wireless telephone's BT signal and there could be a box, similar in size to a radar detector that amplifies the motorist's cell phone BT signal and directs the signal in the direction of travel (or any other direction including omnidirectional).

[0079] Phase 3 is when the EV manufacturers have advanced BT coverage from the EV, and the motorist's BT is internal to the EV so the EV is the MASTER, and the target

EVSE is SLAVE for charging. This also works for secure entry, access, and parking. This embodiment is shown in FIG. **8**B. An EV **200** approaches an EVSE **202**. The EV **200** itself uses its own Bluetooth to Pair with the EVSE **202** wirelessly **203**. An identification and certificate is sent from the EV **200** to the EVSE **202**, and upon authentication and checking that the certificate is within the proper date/time, charging **204** begins.

[0080] The present invention also teaches a device that will allow motorists that have BT capable wireless telephones that run a proprietary application to access a competitors' EVSE. Most competitors' EVSE are fully networked; therefore, such a system would need to supply a BT stack and controller that could accept and pair with BT enabled wireless telephones and also act as a bridge to the cellular modem that is internal to an EVSE system and reaches various competitors' networks for access control and billing. In this situation, BT (or other wireless technique) can act as a unifying, standard protocol for a vast majority of EV motorists that do not want to join a subscription service for fully networked EVSE systems, but still want to access as many EVSE brands and types as possible, especially in an emergency.

[0081] The process starts with the motorist finding and choosing an EVSE for use now, or in the future. Maps of EVSE locations are presently widely available from a websites online, such recargo.com, plugshare.org or carstations.com. In the future, there will be more websites and maps dedicated to EVSE. Alternatively, the motorist might already know the location, which could be a shopping mall or his place of employment.

[0082] It is also possible that the motorist sets up an account with a pay by phone company, such as currently exist like ParkMobile, or MobileNow, or Verrus, now called Payby-Phone. This is important if there is going to be a transaction and payment for access to the EVSE.

[0083] In the BT enabled EVSE process, an access code is sent from a remote database to the motorist's EV or phone via a wireless network. Many new vehicles already have BT inside the vehicle, so the motorist's phone could be in communication with the vehicle itself, or the request and transaction could take place solely via the motorist's wireless device.

[0084] A specific BT ID number is sent to the motorist's wireless telephone or EV, and the motorist will either already be in the general vicinity of the EVSE or on his way. As discussed above, the vehicle and the motorist's wireless telephone are already able to communicate via the BT controller in the phone and in the vehicle.

[0085] The BT enabled EVSE contain a BT controller and host on a logic board that also has the ability to turn the EVSE on or off. This is what allows controlled access to the EVSE. The EVSE can also have some sort of lighting assembly mounted on the EVSE so that the light will be visible from many directions.

[0086] The BT POLLING and PAIRING and connection process is well understood in the art. An approaching BT enabled vehicle and wireless telephone or smartphone will be POLLING for BT enabled devices within range. As the devices come within range, they respond to the host's POLLING by sending a response message and offering their unique ID number. The actively POLLING device, in this case the EV or the wireless telephone will not PAIR with any of the BT devices other than the unique device for which it is POLLING. This is an added advantage if there are a row of EVSEs. They can be designed with a lighting system such that a specific color represents the state of a particular EVSE. In this embodiment, the target EVSE can change color as the EV approaches and pairs with its host thru BT protocol.

[0087] The system might send just one unique BT ID # corresponding to an EVSE, or it might send a plurality of codes meant for a plurality of EVSEs that the system knows are available based on current data from a database. Once the motorist chooses one of the available EVSEs and pairs with it, then the other codes and other ID #'s expire in the EV or wireless telephone memory after a specified period of time. So that if the motorist paid for one code for a specific duration at a specific EVSE or group of EVSEs, he will only be able to use that one code.

[0088] Thus, using the standard protocol of BT allows the motorist to find the corresponding EVSE that he has reserved or purchased. Finding is enhanced by the POLLING process that can optionally initiate an indicative change in color on the target EVSE, thus guiding the motorist to his EVSE. After PAIRING and connecting, BT also allows for the token or secure code to be quickly and securely transferred from the customer's EV or the customer's wireless telephone in a fast, simple and seamless process.

[0089] If the EVSE has internal use metering, BT allows for full reporting of the charge session once it has expired. This ties the USER, LOCATION, TIME, KWH to a charge session. This data can be sent directly or indirectly to the motorist's wireless telephone or EV and also up to the network to a database, if network access is available. If none is available at the moment, then the data is cached until WIFI, cellular or other access is allowed.

[0090] In some embodiments of the present invention, there may be a combination of Near Field Communication (NFC) and BT communication. In this way the motorist can get out of the EV and walk up and tap his phone onto an NFC pad, or similar device, on the EVSE in order to commence the sharing of data, such as the encrypted access code for a charge duration.

[0091] The secure access via BT (or any other wireless communication technique) of the present invention is not limited to accessing EVSE, but can apply to any access point where a code is issued to a wireless device that also has BT capability. For example, in an airport screening line, a BT enabled system could sense the pre-screened traveler's approach by virtue of his BT enabled wireless telephone or smartphone. This system could even direct a pre-registered traveler with BT enabled phone to go into specific lines for speedier priority security inspection.

[0092] Several descriptions and illustrations have been presented to aid in understanding the features of the present invention. One skilled in the art will realize that numerous changes and variations are possible without departing from the spirit of the invention. Each of these changes and variations is within the scope of the present invention.

We claim:

1. A reservation system comprising:

a server able to receive a reservation request from a first terminal and provide a reservation certificate to a mobile second terminal in response to the reservation request; and,

an access device able to receive and validate the reservation certificate from the mobile second terminal and allow access in response.

2. The system of claim **1**, wherein at least one of the first terminal and the second terminal is a wireless telephone.

3. The system of claim **2** wherein said wireless telephone communicates with the access device using a short-range wireless communication technique.

4. The system of claim **3** wherein the short-range wireless communication technique is Bluetooth.

5. The system of claim **1**, wherein the reservation certificate includes at least one of a duration and an end time.

6. The system of claim **1**, wherein the access device has an identification and the reservation certificate includes the identification.

7. The system of claim **6**, wherein the reservation certificate further comprises a digital signature by the server, and the access device is able to authenticate the reservation certificate with the digital signature.

8. The system of claim **1**, wherein the access device has a public key and a private key pair, and at least a portion of the reservation certificate is encrypted with the public key by the server and decrypted with the private key by the access device.

9. The system of claim **1** wherein the access device is an EVSE.

10. The system of claim **9**, wherein the EVSE contains an electric vehicle charger that has an identification, and the reservation certificate includes the identification.

11. The system of claim **1** wherein the reservation certificate further comprises a digital signature by the server of data representative of the reservation.

12. The system of claim **9**, wherein the reservation certificate comprises a digital signature by the server, and the EVSE is able to authenticate the reservation certificate with the digital signature.

13. The system of claim **9**, wherein the EVSE has a public key and a private key pair, and at least a portion of the reservation certificate is encrypted with the public key by the server and decrypted with the private key by the EVSE.

14. A method of reserving electrical vehicle charging comprising:

providing an access control system including a server and an access device, the access device including an electrical vehicle charger;

accepting a reservation request from a first terminal using the server;

providing a reservation certificate to a mobile second terminal in response to the request using the server;

accepting the reservation certificate from the second terminal using the access device;

determining the reservation certificate is authentic; and

activating the electric vehicle charger in response to accepting an authentic reservation certificate using the access device.

15. The method of claim **14**, wherein the reservation certificate includes a duration and the activating is maintained for not longer than the duration.

16. The method of claim **14**, wherein at least a portion of the reservation certificate is encrypted.

17. The method of claim **14** herein the reservation certificate further comprises a digital signature by the server of data representative of the reservation.

18. The method of claim **14** wherein the access device has an identification, and the reservation certificate contains data that includes the identification.

19. The method of claim **14** wherein the mobile second terminal is a wireless telephone that communicates with the access device using a short-range wireless communication technique.

20. The method of claim **14** wherein the mobile second terminal is a Bluetooth enabled EV.

* * * * *