

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been
 filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☐ Patents. (☐ the patent action involves 35 U.S.C. § 292.);

DOCKET NO. 2:22-cv-00318	DATE FILED 8/18/2022	U.S. DISTRICT COURT Eastern District of Texas
PLAINTIFF Liberty Access Technologies Licensing LLC		DEFENDANT Marriott International, Inc.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 US 9,373,205 B2	6/21/2016	Urban Intel, Inc.
2 US 10,657,747 B2	5/19/2020	Urban Intel, Inc.
3 US 11,373,474 B2	6/28/2022	Urban Intel, Inc.
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/034,278	07/12/2018	Chris Outwater	LBT0010-CON3	8554
67050	7590	07/29/2020	EXAMINER	
KASHA LAW LLC 14532 Dufief Mill Road North Potomac, MD 20878			HOFFMAN, BRANDON S	
			ART UNIT	PAPER NUMBER
			2433	
			NOTIFICATION DATE	DELIVERY MODE
			07/29/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JOHN.KASHA@KASHALAW.COM



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

In re Patent No. 10,657,747
Issue Date: May 19, 2020
Application No. 16/034,278
Filing or 371(c) Date: July 12, 2018
Attorney Docket No. LBT0010-CON3

:
:
:
:
:
:
:

DECISION ON PETITION

This is a notice regarding your request filed April 16, 2020, for acceptance of a fee deficiency submission under 37 CFR 1.28(c).

The Office no longer investigates or rejects original or reissue applications under 37 CFR 1.56. **1098 Off. Gaz. Pat. Office 502 (January 3, 1989)**. Therefore, nothing in this Notice is intended to imply that an investigation was done.

The fee deficiency submission under 37 CFR 1.28(c) is hereby **ACCEPTED**.

Accordingly, status as a small entity has been removed and any future fee(s) submitted must be paid at the undiscounted rate.

Inquiries related to this communication should be directed to the undersigned at (571) 272-1058.

/Angela Walker/
Angela Walker
Paralegal Specialist
Office of Petitions



United States Patent and Trademark Office

Office of the Chief Financial Officer

Document Code:WFEE

User :C41722

Sale Accounting Date:07/24/2020

Sale Item Reference Number

16034278

Effective Date

04/16/2020

Document Number

I20207NE04189575

Fee Code

1461

Fee Code Description

1.28(C) SUBMISSIONS - APPLIC
FILE FEE

Amount Paid

\$500.00

Payment Method

Salea



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY.DOCKET NO./TITLE	REQUEST ID
16/034,278	07/12/2018	Liberty PlugIns, Inc.	LBT0010-CON3	111061

Acknowledgement of Loss of Entitlement to Entity Status Discount

The entity status change request below filed through Private PAIR on 04/30/2020 has been accepted.

CERTIFICATIONS:

Change of Entity Status:

☒ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be notification of loss of entitlement to small or micro entity status, as applicable.

This portion must be completed by the signatory or signatories making the entity status change in accordance with 37 CFR 1.4(d)(4).

Signature:	/John Kasha/
Name:	John Kasha
Registration Number:	53100



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/034,278	05/19/2020	10657747	LBT0010-CON3	8554
67050	7590	04/29/2020		
KASHA LAW LLC 14532 Dufief Mill Road North Potomac, MD 20878				

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Chris Outwater, Carpinteria, CA;
Liberty PlugIns, Inc., Santa Barbara, CA;
William Gibbens Redmann, Glendale, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

IR103 (Rev. 10/09)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16034278
	Filing Date	2018-07-12
	First Named Inventor	Outwater
	Art Unit	2433
	Examiner Name	HOFFMAN, BRANDON S
	Attorney Docket Number	LBT0010-CON3

Change(s) applied to document, /C.G./ 4/17/2020	15	20070035381		2007-02-15	Davis	Entire document
	16	20070126562		~~2008-08-15~~ 07/2007	Ku	Entire document
	17	20070176739		2007-08-02	Raheman	Entire document
	18	20070197261		2007-08-23	Humbel	Entire document
	19	20070200665		2007-08-30	Studerus	Entire document
	20	20070290789		2007-12-20	Segev et al.	Entire document
	21	20080024272		2008-01-31	Fiske	Entire document
	22	20090066476		2009-03-12	Raheman	Entire document
	23	20090136035		2009-05-28	Lee	Entire document
	24	20090184801		2009-07-23	Bliding et al.	Entire document
	25	20100141381		2010-06-10	Bliding et al.	Entire document



United States Patent and Trademark Office

Office of the Chief Financial Officer

Document Code:WFEE

User :67142

Sale Accounting Date:04/17/2020

Sale Item Reference Number

16034278

Effective Date

04/16/2020

Document Number

I20204GF45046103

Fee Code

1599

Fee Code Description

MAINTENANCE/PETITION
INTERNAL FEE CODE

Amount Paid

\$500.00

Payment Method

Credit Card

LBT0010-CON3

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of: OUTWATER ET AL. Serial No.: 16/034,278 Filed: July 12, 2018 For: ACCESS CONTROL SYSTEM AND METHOD FOR USE BY AN ACCESS DEVICE	Confirmation No.: 8554 Art Unit: 2433 Examiner: Brandon S. Hoffman
--	---

ISSUE FEE DIFFERENCE PAYMENT DUE TO ENTITY STATUS CHANGE

Sir:

On April 14, 2020, issue fees in the amount of \$500 were paid for this case based on small entity status by mistake. The Applicant is submitting herewith \$500, which is the difference between the issue fees for a large entity (\$1,000) and the issue fees for a small entity (\$500).

	Small Entity	Large Entity	Difference
Issue fees	\$500	\$1,000	\$500

Should the Office have any questions, the Office is encouraged to telephone the Applicant's undersigned representative at the number listed below.

KASHA LAW LLC
14532 Dufief Mill Rd.
North Potomac, MD 20878
Tel. 240-423-8431
Date: April 16, 2020

Respectfully submitted,

By: /Kelly L. Kasha/
Kelly L. Kasha
Registration No. 47,743

Customer No. 67050



Kasha Law LLC
An Intellectual Property Law Firm

14532 Duffer Mill Rd.
North Potomac, MD 20878

Tel. (703) 867-1886
Fax (301) 340-3022
www.kashalaw.com

FAX COVERSHEET

To: Financial Manager Department

To Fax No: 571-273-6500

From: Kelly L. Kasha, Esq.

From Fax No.: (301) 340-3022

Date: 4/16/2020

No. of Pages (including this page): 3

Subject: **Issue fee difference payment due to entity status change**
US Application Serial No: 16/034,278
Attorney Docket No: LBT0010-CON3
Difference in issue fees to be charged: \$500

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

67050 7590 01/21/2020
KASHA LAW LLC
14532 Dufief Mill Road
North Potomac, MD 20878

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/034,278	07/12/2018	Chris Outwater	LBT0010-CON3	8554

TITLE OF INVENTION: ACCESS CONTROL SYSTEM AND METHOD FOR USE BY AN ACCESS DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	04/21/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
HOFFMAN, BRANDON S	2433	713-156000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 John R. Kasha

2 Kelly L. Kasha

3 Kasha Law LLC

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

Liberty PlugIns, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Santa Barbara, CA

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Kelly L. Kasha/

Date April 14, 2020

Typed or printed name Kelly L. Kasha

Registration No. 47,743

Electronic Patent Application Fee Transmittal				
Application Number:		16034278		
Filing Date:		12-Jul-2018		
Title of Invention:		ACCESS CONTROL SYSTEM AND METHOD FOR USE BY AN ACCESS DEVICE		
First Named Inventor/Applicant Name:		Chris Outwater		
Filer:		John Kasha		
Attorney Docket Number:		LBT0010-CON3		
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	500	500

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				500

Electronic Acknowledgement Receipt	
EFS ID:	39148754
Application Number:	16034278
International Application Number:	
Confirmation Number:	8554
Title of Invention:	ACCESS CONTROL SYSTEM AND METHOD FOR USE BY AN ACCESS DEVICE
First Named Inventor/Applicant Name:	Chris Outwater
Customer Number:	67050
Filer:	John Kasha
Filer Authorized By:	
Attorney Docket Number:	LBT0010-CON3
Receipt Date:	14-APR-2020
Filing Date:	12-JUL-2018
Time Stamp:	09:21:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 500
RAM confirmation Number	E20204D021365378
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	LBT0010-CON3_iss_fee_trans. pdf	96137	no	1
			90c0e14107b74135b43baa7c0a02a1692ac3273b		
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30149	no	2
			caf8dff80b0bc6e0dd90ba98dd5194bcf22d3f48e		
Warnings:					
Information:					
Total Files Size (in bytes):			126286		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

67050 7590 01/21/2020
KASHA LAW LLC
14532 Dufief Mill Road
North Potomac, MD 20878

EXAMINER
HOFFMAN, BRANDON S

ART UNIT PAPER NUMBER

2433

DATE MAILED: 01/21/2020

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/034,278	07/12/2018	Chris Outwater	LBT0010-CON3	8554

TITLE OF INVENTION: ACCESS CONTROL SYSTEM AND METHOD FOR USE BY AN ACCESS DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	04/21/2020

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

67050 7590 01/21/2020
KASHA LAW LLC
14532 Dufief Mill Road
North Potomac, MD 20878

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/034,278	07/12/2018	Chris Outwater	LBT0010-CON3	8554

TITLE OF INVENTION: ACCESS CONTROL SYSTEM AND METHOD FOR USE BY AN ACCESS DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	04/21/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
HOFFMAN, BRANDON S	2433	713-156000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

1 _____

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☐ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☐ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/034,278	07/12/2018	Chris Outwater	LBT0010-CON3	8554
67050	7590	01/21/2020	EXAMINER	
KASHA LAW LLC 14532 Dufief Mill Road North Potomac, MD 20878			HOFFMAN, BRANDON S	
			ART UNIT	PAPER NUMBER
			2433	
DATE MAILED: 01/21/2020				

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.** Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 16/034,278	Applicant(s) Outwater et al.	
	Examiner BRANDON S HOFFMAN	Art Unit 2433	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to November 19, 2019.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are 1-14 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
Certified copies:
a) ☐ All b) ☐ Some *c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)	5. ☐ Examiner's Amendment/Comment
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.	6. ☐ Examiner's Statement of Reasons for Allowance
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.	7. ☐ Other _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____.	

/BRANDON S HOFFMAN/ Primary Examiner, Art Unit 2433	
--	--

Issue Classification 	Application/Control No. 16/034,278	Applicant(s)/Patent Under Reexamination Outwater et al.
	Examiner BRANDON S HOFFMAN	Art Unit 2433

CPC						
Symbol					Type	Version
G07C	/	9	/	27	F	2020-01-01
H04W	/	4	/	021	I	2013-01-01
H04W	/	4	/	023	I	2013-01-01
G06Q	/	20	/	045	I	2013-01-01
G06Q	/	20	/	3223	I	2013-01-01
G06Q	/	20	/	38215	I	2013-01-01
G06Q	/	30	/	06	I	2013-01-01
G07F	/	5	/	26	I	2013-01-01
G07F	/	15	/	005	I	2013-01-01
H04L	/	9	/	3247	I	2013-01-01
H04L	/	9	/	3263	I	2013-01-01
H04L	/	63	/	0823	I	2013-01-01
H04W	/	12	/	08	I	2013-01-01
H04L	/	63	/	102	I	2013-01-01
H04W	/	12	/	06	I	2013-01-01
B60L	/	53	/	65	I	2019-02-01
B60L	/	53	/	30	I	2019-02-01
B60L	/	53	/	14	I	2019-02-01
B60L	/	53	/	665	I	2019-02-01
B60L	/	53	/	68	I	2019-02-01
B60L	/	53	/	16	I	2019-02-01
B60L	/	53	/	31	I	2019-02-01
B60L	/	53	/	18	I	2019-02-01
B60L	/	53	/	57	I	2019-02-01
G07C	/	9	/	20	I	2020-01-01
G07C	/	9	/	29	I	2020-01-01
G06Q	/	20	/	32	I	2013-01-01
G06Q	/	10	/	02	I	2013-01-01
G06Q	/	20	/	322	I	2013-01-01
G06Q	/	20	/	3829	I	2013-01-01
G06Q	/	50	/	06	I	2013-01-01

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	14	
/BRANDON S HOFFMAN/ Primary Examiner, Art Unit 2433	07 January 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office

Part of Paper No.: 20200107

Issue Classification 	Application/Control No. 16/034,278	Applicant(s)/Patent Under Reexamination Outwater et al.
	Examiner BRANDON S HOFFMAN	Art Unit 2433

CPC						
Symbol				Type	Version	
H04L	/	9	/	3268	I	2013-01-01
H04M	/	1	/	7253	I	2013-01-01
G06Q	/	20	/	3278	I	2013-01-01
Y02T	/	90	/	162	A	2013-01-01
Y02T	/	10	/	7291	A	2013-01-01
Y02T	/	90	/	128	A	2013-01-01
Y02T	/	90	/	169	A	2013-01-01
Y04S	/	30	/	14	A	2013-01-01
Y02T	/	10	/	7088	A	2013-01-01
Y02T	/	10	/	7005	A	2013-01-01
Y02T	/	90	/	16	A	2013-01-01
Y02T	/	90	/	163	A	2013-01-01
Y02T	/	90	/	121	A	2013-01-01
Y02T	/	90	/	14	A	2013-01-01
B60L	/	2240	/	622	A	2013-01-01
B60L	/	2240	/	72	A	2013-01-01
B60L	/	2240	/	80	A	2013-01-01
B60L	/	2250	/	10	A	2013-01-01
H04L	/	2209	/	56	A	2013-01-01
H04L	/	2209	/	80	A	2013-01-01
H04L	/	2209	/	84	A	2013-01-01
H04L	/	63	/	0442	A	2013-01-01
Y02T	/	90	/	12	A	2013-01-01
G06Q	/	2240	/	00	A	2013-01-01
H04W	/	4	/	40	A	2018-02-01

CPC Combination Sets					
Symbol	Type	Set	Ranking	Version	
/		/			

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	14	
/BRANDON S HOFFMAN/ Primary Examiner, Art Unit 2433	07 January 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Issue Classification 	Application/Control No. 16/034,278	Applicant(s)/Patent Under Reexamination Outwater et al.
	Examiner BRANDON S HOFFMAN	Art Unit 2433

INTERNATIONAL CLASSIFICATION			
CLAIMED			
G07C		9	00
NON-CLAIMED			
G07C		9	00

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS
713	176

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

NONE (Assistant Examiner)		Total Claims Allowed: 14	
/BRANDON S HOFFMAN/ Primary Examiner, Art Unit 2433 (Primary Examiner)		07 January 2020 (Date)	
		O.G. Print Claim(s) 1	O.G. Print Figure 1

Issue Classification 	Application/Control No. 16/034,278	Applicant(s)/Patent Under Reexamination Outwater et al.
	Examiner BRANDON S HOFFMAN	Art Unit 2433

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47															
CLAIMS															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	5	10												
2	2	10	11												
3	3	12	12												
11	4	13	13												
6	5	14	14												
7	6														
8	7														
9	8														
4	9														

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 14	
/BRANDON S HOFFMAN/ Primary Examiner, Art Unit 2433 (Primary Examiner) _____ (Date) 07 January 2020		O.G. Print Claim(s) 1	O.G. Print Figure 1

U.S. Patent and Trademark Office

Part of Paper No.: 20200107

<i>Search Notes</i> 	Application/Control No. 16/034,278	Applicant(s)/Patent Under Reexamination Outwater et al.
	Examiner BRANDON S HOFFMAN	Art Unit 2433

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner
H04L 9/32 - with keyword limiters	08/15/2019	BH

US Classification - Searched*			
Class	Subclass	Date	Examiner
713	176 - with keyword limiters	08/15/2019	BH

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
inventor name search	08/15/2019	BH
see attached EAST search notes	08/15/2019	BH
updated EAST search notes	01/07/2020	BH

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
	searched claim language	01/07/2020	BH

/BRANDON S HOFFMAN/ Primary Examiner, Art Unit 2433	
--	--

EAST Search History**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	1393284	reserv\$5	US-PGPUB; USPAT; USOCR	OR	ON	2020/01/07 12:04
L3	211033	certificate	US-PGPUB; USPAT; USOCR	OR	ON	2020/01/07 12:04
L4	40866	electric with vehicle with charg\$3	US-PGPUB; USPAT; USOCR	OR	ON	2020/01/07 12:04
L5	9404	L4.clm.	US-PGPUB; USPAT; USOCR	OR	ON	2020/01/07 12:04
L6	212752	L2.clm.	US-PGPUB; USPAT; USOCR	OR	ON	2020/01/07 12:04
L7	23829	L3.clm.	US-PGPUB; USPAT; USOCR	OR	ON	2020/01/07 12:04
L8	3	L5 and L6 and L7	US-PGPUB; USPAT; USOCR	OR	ON	2020/01/07 12:04

1/7/2020 12:04:20 PM**C:\Users\bhoffman\Documents\EAST\Workspaces\16034278.wsp**

Electronic Acknowledgement Receipt	
EFS ID:	37794482
Application Number:	16034278
International Application Number:	
Confirmation Number:	8554
Title of Invention:	Access Control System and Method for Use by an Access Device
First Named Inventor/Applicant Name:	Chris Outwater
Customer Number:	67050
Filer:	John Kasha
Filer Authorized By:	
Attorney Docket Number:	LBT0010-CON3
Receipt Date:	19-NOV-2019
Filing Date:	12-JUL-2018
Time Stamp:	17:41:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	LBT0010-CON3_response_11_19_2019.pdf	118015 6e1252bc8c3e345567eb2f150ca48e3eb2d7e8c3	no	9

Warnings:

Information:	
Total Files Size (in bytes):	118015
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of: OUTWATER ET AL. Serial No.: 16/034,278 Filed: July 12, 2018 For: ACCESS CONTROL SYSTEM AND METHOD FOR USE BY AN ACCESS DEVICE	Confirmation No.: 8554 Art Unit: 2433 Examiner: Brandon S. Hoffman
---	--

AMENDMENT**MAIL STOP: AMENDMENTS**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Non-Final Office Action mailed August 19, 2019, please consider the following remarks.

No fees are believed to be due. However, any fee necessary for consideration of this response is hereby authorized to be charged to Deposit Account Number 50-4075.

Amendments to the Specification begin on page 2 of this paper.

Amendments to the Claims begin on page 3 of this paper.

Remarks begin on page 7 of this paper.

Amendments to the Specification:

Please replace paragraph [0001] with the following amended paragraph:

[0001] This application is a continuation of U.S. Patent Application No. 15/609,055, filed May 31, 2017, now U.S. Patent no. 10,049,514, which is a continuation of U.S. Patent Application No. 15/178,849, filed June 10, 2016, now U.S. Patent No. 9,911,258, which is a continuation of U.S. Patent Application No. 14/603,434, filed January 23, 2015, now U.S. Patent No. 9,373,205, which is a continuation of U.S. Patent Application No. 13/582,467, filed September 4, 2012, now U.S. Patent No. 8,996,879, which is a national stage application of PCT Application No. PCT/US11/26781, filed March 2, 2011, which claims the benefit of U.S. Provisional Patent Application No. 61/309,813, filed March 2, 2010. All of the above mentioned applications are incorporated by reference herein in their entireties.

This listing of claims replaces all prior versions and listings of claims in this application.

Amendments to the Claims:

1. (Currently amended) An access control system comprising:
 - a) an access device comprising a communication module connected to a processor having control of a door lock;
 - b) a secure reservation interface to receive a reservation request from a first device for a reservation at a given destination, the reservation interface comprising one or more screens for receiving a selection of a location at the destination and an interval of the reservation;
 - c) a reservation server, in communication with the reservation interface ~~via~~ and a network, to:
 - receive the reservation request for the destination, the reservation request including a selected location at the destination and an interval of the reservation;
 - ~~present a destination map for the destination, the destination map comprising markings for a plurality of selectable locations at the destination;~~
 - ~~receive a request for a given selectable location at the destination;~~
 - issue a reservation certificate describing ~~an~~ the interval of ~~a~~ the reservation based on the reservation request and the selected location; and
 - transmit, via the network, from the reservation server to a second device distinct from the first device, the reservation certificate and a communication setting corresponding to the access device;

d) an application installed on the second device to receive the reservation certificate and the communication setting corresponding to the access device, wherein the application wirelessly transmits the reservation certificate to the access device using the communication setting upon receipt of a command to activate the door lock; and

e) wherein the access device receives the reservation certificate from the application based on use by the application of the communication setting, and the processor activates the door lock based on at least the receipt of the reservation certificate.

2. (Previously presented) The system of claim 1 wherein the access device comprises a unique identifier, and wherein at least the reservation certificate or the communication setting contains the unique identifier.
3. (Currently amended) The system of claim 2 wherein at least a portion of the reservation certificate is encrypted ~~and wherein the access device decrypts the encrypted portion of the reservation certificate.~~
4. (Currently amended) The system of claim + 11 wherein the reservation server receives a request for one or more amenities at the destination.
5. (Previously presented) The system of claim 1 wherein the access device generates a record indicating that the processor activated the door lock.
6. (Previously presented) The system of claim 1 wherein the reservation certificate automatically expires at the end of the interval of the reservation.
7. (Previously presented) The system of claim 1 wherein the second device comprises a smartphone.

8. (New) The system of claim 1 wherein the access device comprises a Bluetooth transceiver.
9. (New) The system of claim 3 wherein the access device decrypts the encrypted portion of the reservation certificate.
10. (New) The system of claim 3 wherein the application installed on the second device decrypts the encrypted portion of the reservation certificate.
11. (New) The system of claim 1 wherein the reservation interface comprises one or more screens for selecting one or more amenities at the destination.
12. (New) The system of claim 1 wherein the reservation detail interface comprises one or more screens for selecting at least a start time and a stop time, or a duration for the reservation.
13. (New) An access control system comprising:
 - a) an access device comprising a communication module connected to a processor having control of a door lock restricting access to a room at a given location, the access device comprising at least a Bluetooth transceiver;
 - b) a reservation interface comprising one or more reservation screens associated with the location, the one or more reservation screens for selecting at least a room and an interval for a reservation at the location;
 - c) a reservation server, in communication with the reservation interface and a network,to:
 - receive a reservation request comprising at least a selected room and an interval for a reservation;

- issue a reservation certificate, the reservation certificate describing an interval of the reservation for the room based on the reservation request; and
- transmit, via the network, from the reservation server to an application installed on a smartphone, the reservation certificate and a communication setting corresponding to the access device;
- d) a smartphone application installed on the smartphone to receive the reservation certificate and the communication setting corresponding to the access device, wherein the smartphone application wirelessly transmits, via Bluetooth, the reservation certificate to the access device using the communication setting upon receipt of a command to activate the door lock; and
- e) wherein the access device receives the reservation certificate from the smartphone application based on use by the smartphone application of the communication setting, and the processor activates the door lock based on at least the receipt of the reservation certificate.
14. (New) The system of claim 13 wherein the reservation interface comprises one or more reservation screens associated with the location, the one or more screens for selecting one or more amenities at the location.

REMARKS

Claims 1-7 are pending in this application. By this amendment, the specification is amended to reflect the patent number of a prior application that has matured into a patent, claims 1, 3 and 4 have been amended, and new claims 8-14 have been added. Claims 1-14 will remain pending herein upon entry of this amendment. No new matter is introduced.

The subject matter of amended claim 1 may be found at, for example, paragraphs [0008], [0033], [0038] and [0048].

The subject matter of amended claim 3 may be found at, for example, paragraphs [0012], [0027], [0030] and [0036-0038].

The subject matter of amended claim 4 may be found at, for example, paragraphs [0049], [0051] and [0053].

The subject matter of new claim 8 may be found at least in the specification, i.e., U.S. Published Application No. 20180336745, at, for example, paragraphs [0012], [0028], [0029] and [0041].

The subject matter of new claim 9 may be found at least in the specification at, for example, paragraphs [0012], [0027], [0030] and [0036-0038].

The subject matter of new claim 10 may be found at least in the specification at, for example, paragraphs [0012], [0027], [0030] and [0036-0038].

The subject matter of new claim 11 may be found at least in the specification at, for example, paragraphs [0048] and [0050-0058].

The subject matter of new claim 12 may be found at least in the specification at, for example, paragraph [0008], [0033], [0038] and [0048].

The subject matter of new claim 13 may be found at least in the specification at, for example, paragraph [0007], [0024], [0027-0030], [0032-0037], [0041], [0058], FIG. 4 and FIG. 5

The subject matter of new claim 14 may be found at least in the specification at, for example, paragraph [0049], [0051] and [0053].

The Applicant believes the instant application is in condition for allowance. Therefore, it is requested that a Notice of Allowance be issued in due course.

Specification Objection

In the Non-Final Office Action mailed August 19, 2019, the “disclosure is objected to because of the following informalities: the CROSS-REFERENCE TO RELATED APPLICATION section needs updated to reflect applications that have matured into patents.” The Specification has been amended to reflect the patent number of a prior application that has matured into a patent. Withdrawal of the Specification objection is respectfully requested.

Non-Statutory Double Patenting Rejections

Claims 1-7 are rejected on the ground of non-statutory obviousness-type double patenting as being unpatentable over claims 1-20 of prior U.S. Patent No. 10,049,514 (hereinafter the “‘514 patent”).

The Applicant files herewith a Terminal Disclaimer over the ‘514 patent. Accordingly, withdrawal of the rejection of the claims based on the judicially created doctrine of double patenting is respectfully requested.

Serial No.: 16/034,278
Art Unit: 2433

Attorney's Docket No.: LBT0010-CON3
Page 9

Conclusion

In view of the foregoing, claims 1-14 are believed to be in condition for allowance.
Should the Examiner have any questions or determine that any further action is desirable to place this application in even better condition for issue, the Examiner is encouraged to telephone the Applicant's undersigned representative at the number listed below.

KASHA LAW LLC
14532 Dufief Mill Rd.
North Potomac, MD 20878
Tel. 240-423-8431
Date: November 19, 2019

Respectfully submitted,
By: /Kelly L. Kasha/
Kelly L. Kasha
Registration No. 47,743

Customer No. 67050

Doc Code: DIST.E.FILE Document Description: Electronic Terminal Disclaimer - Filed		PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce
Electronic Petition Request	TERMINAL DISCLAIMER TO OBTAIN A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	
Application Number	16034278	
Filing Date	12-Jul-2018	
First Named Inventor	Chris Outwater	
Attorney Docket Number	LBT0010-CON3	
Title of Invention	Access Control System and Method for Use by an Access Device	
☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action ☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.		
Owner	Percent Interest	
URBAN INTEL, INC	100%	
The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s) 10049514 as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns. In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later: - expires for failure to pay a maintenance fee; - is held unenforceable; - is found invalid by a court of competent jurisdiction; - is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321; - has all claims canceled by a reexamination certificate; - is reissued; or - is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer. ☒ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.		

☐ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.	
Applicant claims the following fee status: ☒ Small Entity ☐ Micro Entity ☐ Regular Undiscounted	
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.	
THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES I certify, in accordance with 37 CFR 1.4(d)(4) that I am: ☒ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application Registration Number <u>47743</u> ☐ A sole inventor ☐ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application ☐ A joint inventor; all of whom are signing this request	
Signature	/Kelly Kasha/
Name	Kelly Kasha

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
 Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal				
Application Number:		16034278		
Filing Date:		12-Jul-2018		
Title of Invention:		Access Control System and Method for Use by an Access Device		
First Named Inventor/Applicant Name:		Chris Outwater		
Filer:		John Kasha		
Attorney Docket Number:		LBT0010-CON3		
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	2814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				160

Doc Code: DISQ.E.FILE

Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 16034278

Filing Date: 12-Jul-2018

Applicant/Patent under Reexamination: Outwater

Electronic Terminal Disclaimer filed on November 19, 2019

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt	
EFS ID:	37794241
Application Number:	16034278
International Application Number:	
Confirmation Number:	8554
Title of Invention:	Access Control System and Method for Use by an Access Device
First Named Inventor/Applicant Name:	Chris Outwater
Customer Number:	67050
Filer:	John Kasha
Filer Authorized By:	
Attorney Docket Number:	LBT0010-CON3
Receipt Date:	19-NOV-2019
Filing Date:	12-JUL-2018
Time Stamp:	17:42:51
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$160
RAM confirmation Number	E2019AIH42499250
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	33394	no	2
			42d81d9f5d6fcb66cd76ba534b8490fcc945908d		
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30308	no	2
			0eb9b164e2ac06e3776de020f13eaa814b3c1168		
Warnings:					
Information:					
Total Files Size (in bytes):			63702		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/034,278	07/12/2018	Chris Outwater	LBT0010-CON3	8554
67050	7590	08/19/2019	EXAMINER	
KASHA LAW LLC			HOFFMAN, BRANDON S	
14532 Dufief Mill Road			ART UNIT	PAPER NUMBER
North Potomac, MD 20878			2433	
			NOTIFICATION DATE	DELIVERY MODE
			08/19/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JOHN.KASHA@KASHALAW.COM

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

1. Claims 1-7 are pending in this office action.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on October 18, 2018, is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner. However, one reference has not been considered because of copy of the NPL was not included, nor was a date specified.

Specification

4. The disclosure is objected to because of the following informalities: the CROSS-REFERENCE TO RELATED APPLICATION section needs updated to reflect applications that have matured into patents. Appropriate correction is required.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise

extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP §§ 706.02(l)(1) - 706.02(l)(3) for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

1. Claims 1-7 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-20 of U.S. Patent No. 10,049,514. Although the claims at issue are not identical, they are not patentably distinct from each other because both application and patent claim an access device, a reservation interface, a reservation server, an application installed on a second device, wherein the access device receives the reservation certificate from the application. The patent further claims the second device as a smartphone, whereas the instant application claims presenting a destination map comprising markings. It would have been obvious to use a smartphone as the second device since smartphone devices have become so powerful and have the convenience of portability.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRANDON S HOFFMAN whose telephone number is (571)272-3863. The examiner can normally be reached on Monday-Friday 8:30AM-5:00PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Pwu can be reached on (571)272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRANDON S HOFFMAN/
Primary Examiner, Art Unit 2433

<i>Notice of References Cited</i>	Application/Control No. 16/034,278		Applicant(s)/Patent Under Reexamination Outwater et al.	
	Examiner BRANDON S HOFFMAN		Art Unit 2433	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20020100803-A1	08-2002	Sehr, Richard P.	G06Q10/02	235/384
*	B	US-6233577-B1	05-2001	Ramasubramani; Seetharaman	H04L29/06	1/1
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

U.S. Patent and Trademark Office
PTO-892 (Rev. 01-2001)

Notice of References Cited

Part of Paper No. 20190812

<i>Search Notes</i> 	Application/Control No. 16/034,278	Applicant(s)/Patent Under Reexamination Outwater et al.
	Examiner BRANDON S HOFFMAN	Art Unit 2433

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner
H04L 9/32 - with keyword limiters	08/15/2019	BH

US Classification - Searched*			
Class	Subclass	Date	Examiner
713	176 - with keyword limiters	08/15/2019	BH

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
inventor name search	08/15/2019	BH
see attached EAST search notes	08/15/2019	BH

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/BRANDON S HOFFMAN/ Primary Examiner, Art Unit 2433	
--	--

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	7036	(713/176).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:27
L2	190	(OUTWATER near CHRIS REDMANN near WILLIAM).in.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L3	2	"20120331301"	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L4	14245	(G06Q20/32 OR G06Q20/38215 OR G07F15/005 OR H04L9/3263 OR Y02T90/12).CPC.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L5	2	((("20030154169") or ("20050255840"))).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:27
L6	20824	L1 L4	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L7	274	reservation with certificate	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L8	1504335	phone	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L9	77007	digital with signature	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L10	56	L7 and L8 and L9	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L11	21	L6 and L10	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L12	21053	reservation with request	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L13	44	L10 and L12	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L14	99436	vehicle with charg\$3	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L15	1359559	reserv\$5	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L16	205648	certificate	US-PGPUB; USPAT;	OR	ON	2019/08/15 08:27

			USOCR			
L17	717	L14 and L15 and L16	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L18	7036	(713/176).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:27
L19	14245	(G06Q20/32 OR G06Q20/38215 OR G07F15/005 OR H04L9/3263 OR Y02T90/12).CPC.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L20	20824	L18 L19	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L21	274	reservation with certificate	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L22	1504335	phone	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L23	77007	digital with signature	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L24	56	L21 and L22 and L23	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L25	21	L20 and L24	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L26	85	L14 and L15 same L16	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L27	38745	electric with vehicle with charg\$3	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L28	5654	L15 and L27	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L29	188	L16 and L28	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L30	1359559	reserv\$5	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L31	205648	certificate	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L32	38745	electric with vehicle with charg\$3	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L33	5654	L30 and L32	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L34	188	L31 and L33	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L35	7036	(713/176).CCLS.	US-PGPUB; USPAT;	OR	OFF	2019/08/15 08:27

			USOCR			
L36	14245	(G06Q20/32 OR G06Q20/38215 OR G07F15/005 OR H04L9/3263 OR Y02T90/12).CPC.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L37	20824	L35 L36	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L38	274	reservation with certificate	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L39	1504335	phone	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L40	77007	digital with signature	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L41	56	L38 and L39 and L40	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L42	21	L37 and L41	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L43	8987	L32.clm.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L44	207729	L30.clm.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L45	22990	L31.clm.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L46	3	L43 and L44 and L45	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L47	1	("8996876").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:27
L52	1359559	reserv\$5	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L53	205648	certificate	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L54	38745	electric with vehicle with charg\$3	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L55	8987	L54.clm.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L56	207729	L52.clm.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L57	22990	L53.clm.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L58	3	L55 and L56 and L57	US-PGPUB; USPAT;	OR	ON	2019/08/15 08:27

			USOCR			
L59	7036	(713/176).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:27
L60	14245	(G06Q20/32 OR G06Q20/38215 OR G07F15/005 OR H04L9/3263 OR Y02T90/12).CPC.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L61	20824	L59 L60	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L62	274	reservation with certificate	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L63	1504335	phone	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L64	77007	digital with signature	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L65	56	L62 and L63 and L64	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L66	21	L61 and L65	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L71	7036	(713/176).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:27
L72	190	(OUTWATER near CHRIS REDMANN near WILLIAM).in.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L73	2	"20120331301"	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L74	14245	(G06Q20/32 OR G06Q20/38215 OR G07F15/005 OR H04L9/3263 OR Y02T90/12).CPC.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L75	2	((("20030154169") or ("20050255840"))).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:27
L76	20824	L71 L74	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L77	274	reservation with certificate	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L78	1504335	phone	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L79	77007	digital with signature	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L80	56	L77 and L78 and L79	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L81	21	L76 and L80	US-PGPUB; USPAT;	OR	ON	2019/08/15 08:27

			USOCR			
L82	21053	reservation with request	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L83	44	L80 and L82	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L84	99436	vehicle with charg\$3	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L85	1359559	reserv\$5	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L86	205648	certificate	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L87	717	L84 and L85 and L86	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L88	7036	(713/176).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:27
L89	14245	(G06Q20/32 OR G06Q20/38215 OR G07F15/005 OR H04L9/3263 OR Y02T90/12).CPC.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L90	20824	L88 L89	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L91	274	reservation with certificate	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L92	1504335	phone	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L93	77007	digital with signature	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L94	56	L91 and L92 and L93	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L95	21	L90 and L94	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L96	85	L84 and L85 same L86	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L97	38745	electric with vehicle with charg\$3	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L98	5654	L85 and L97	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L99	188	L86 and L98	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L100	1359559	reserv\$5	US-PGPUB; USPAT;	OR	ON	2019/08/15 08:27

			USOCR			
L101	205648	certificate	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L102	38745	electric with vehicle with charg\$3	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L103	5654	L100 and L102	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L104	188	L101 and L103	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L105	7036	(713/176).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:27
L106	14245	(G06Q20/32 OR G06Q20/38215 OR G07F15/005 OR H04L9/3263 OR Y02T90/12).CPC.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L107	20824	L105 L106	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L108	274	reservation with certificate	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L109	1504335	phone	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L110	8987	L102.clm.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:27
L111	1	("8996876").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:27
L112	7036	(713/176).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:28
L113	14245	(G06Q20/32 OR G06Q20/38215 OR G07F15/005 OR H04L9/3263 OR Y02T90/12).CPC.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:28
L114	20824	L112 L113	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:28
L115	274	reservation with certificate	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:28
L124	1	("9373205").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:28
L125	1	("8996876").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:28
L128	250	(("8117125") or ("9607292") or ("20080189212") or ("9064258") or ("20080168270") or ("9531548") or ("20130191269") or ("20110112969") or ("20160119149") or	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:28

("20080022089") or ("8732459") or
("8341397") or ("20130159705") or
("7366677") or ("20100146614") or
("7734527") or ("7873579") or
("7873580") or ("8151336") or
("7933842") or ("8517254") or
("7983992") or ("20150135297") or
("20160241549") or ("7366703") or
("9231944") or ("9325701") or
("8538891") or ("20030061170") or
("7801829") or ("20100306113") or
("20090157554") or ("20090157528")
or ("20150012428") or
("20030034873") or ("20080091602")
or ("7415443") or ("8484134") or
("20090157556") or ("20090157557")
or ("20080217400") or ("7292999") or
("20120089522") or ("20080052183")
or ("20080010220") or
("20080010217") or ("7565297") or
("6938019") or ("20150244534") or
("20060179452") or ("20080215878")
or ("20120041843") or ("7708189") or
("8083130") or ("20020133467") or
("8234189") or ("9245157") or
("20040230489") or ("20120259735")
or ("6516316") or ("RE45131") or
("20010037312") or ("20090265768")
or ("9414230") or ("20100174629") or
("8132012") or ("6233577") or
("6836765") or ("20090144540") or
("20060157563") or ("9070150") or
("20090113205") or ("20090217046")
or ("20120284115") or ("8645708") or
("8069100") or ("8301550") or
("20070219870") or ("9286742") or
("20090100508") or ("20020128977")
or ("20090119159") or
("20130144726") or ("8155710") or
("20020038287") or ("20110301986")
or ("7274931") or ("6957185") or
("20090249478") or ("20080077799")
or ("20050186953") or
("20100036772") or ("20070298776")
or ("20040039709") or
("20060106606") or ("20130093382")
or ("20150271149") or
("20090157558") or ("8245044") or
("20100125737") or ("9060274") or
("20120271768") or ("8898762") or
("7003497") or ("20020178122") or
("20040015406") or ("6571221") or
("9336635") or ("7467099") or
("7315823") or ("20120230490") or
("20150213661") or ("20070213047")
or ("8706627") or ("8433658") or
("20100241494") or ("8489513") or
("20110103586") or ("8423476") or
("20020161723") or ("7308431") or
("20040010472") or ("8856891") or
("6748367") or ("20140157393") or
("20070106897") or ("20060032905")
or ("7107248") or ("20030208386") or
("9367975") or ("8028329")).PN. or

		(("20150279130") or ("20080244714") or ("9654448") or ("20110289314") or ("20040073440") or ("20120259774") or ("20100201536") or ("8996861") or ("8213902") or ("20010045451") or ("7039802") or ("20110140656") or ("9026471") or ("20090036164") or ("20150256521") or ("7103572") or ("7269732") or ("7865731") or ("5850442") or ("8392699") or ("20140258011") or ("20160295411") or ("20030191721") or ("20100250947") or ("20080313457") or ("20130191244") or ("7945959") or ("20060282662") or ("8244636") or ("8718717") or ("20110131406") or ("20120072350") or ("8630933") or ("8452680") or ("20080148059") or ("20130185202") or ("7725928") or ("20090205033") or ("20020198849") or ("20050177843") or ("20030120553") or ("20090187980") or ("20070130617") or ("7970678") or ("7533065") or ("20120150670") or ("20100082492") or ("20140143142") or ("20090132813") or ("20060190353") or ("9361741") or ("9483764") or ("20090287578") or ("20090198618") or ("8791790") or ("8073756") or ("9195982") or ("20110022668") or ("9129450") or ("9026472") or ("20030149662") or ("20160035162") or ("20140292482") or ("20100174598") or ("7565329") or ("20020019811") or ("20070265984") or ("20090113543") or ("8630932") or ("7120603") or ("8214299") or ("20080027814") or ("20110191196") or ("20050261913") or ("20120191491") or ("20040243804") or ("9374362") or ("20130198036") or ("20100201482") or ("20100228405") or ("20110145564") or ("20040103064") or ("9092813") or ("9047634") or ("6675153") or ("20150095640") or ("20130198009") or ("8914628") or ("7680736") or ("20120129577") or ("20150072654") or ("20160104142") or ("8938402") or ("9558604") or ("20110208600") or ("8924310") or ("9519894") or ("7726579") or ("20040098350") or ("8924299") or ("20110119485") or ("20110191248") or ("20110191249") or ("20110191250") or ("20090076966") or ("20160210799") or ("20130191224") or ("20050033692") or ("20030061163") or ("20130252585") or ("9264902") or ("20040107170") or ("20090089366") or ("8949608") or ("20090179078") or ("20050138364") or ("20090265552") or ("20080046734") or ("20100275014")).PN.			
--	--	--	--	--	--

L131	250	("8117125") or ("9607292") or ("20080189212") or ("9064258") or ("20080168270") or ("9531548") or ("20130191269") or ("20110112969") or ("20160119149") or ("20080022089") or ("8732459") or ("8341397") or ("20130159705") or ("7366677") or ("20100146614") or ("7734527") or ("7873579") or ("7873580") or ("8151336") or ("7933842") or ("8517254") or ("7983992") or ("20150135297") or ("20160241549") or ("7366703") or ("9231944") or ("9325701") or ("8538891") or ("20030061170") or ("7801829") or ("20100306113") or ("20090157554") or ("20090157528") or ("20150012428") or ("20030034873") or ("20080091602") or ("7415443") or ("8484134") or ("20090157556") or ("20090157557") or ("20080217400") or ("7292999") or ("20120089522") or ("20080052183") or ("20080010220") or ("20080010217") or ("7565297") or ("6938019") or ("20150244534") or ("20060179452") or ("20080215878") or ("20120041843") or ("7708189") or ("8083130") or ("20020133467") or ("8234189") or ("9245157") or ("20040230489") or ("20120259735") or ("6516316") or ("RE45131") or ("20010037312") or ("20090265768") or ("9414230") or ("20100174629") or ("8132012") or ("6233577") or ("6836765") or ("20090144540") or ("20060157563") or ("9070150") or ("20090113205") or ("20090217046") or ("20120284115") or ("8645708") or ("8069100") or ("8301550") or ("20070219870") or ("9286742") or ("20090100508") or ("20020128977") or ("20090119159") or ("20130144726") or ("8155710") or ("20020038287") or ("20110301986") or ("7274931") or ("6957185") or ("20090249478") or ("20080077799") or ("20050186953") or ("20100036772") or ("20070298776") or ("20040039709") or ("20060106606") or ("20130093382") or ("20150271149") or ("20090157558") or ("8245044") or ("20100125737") or ("9060274") or ("20120271768") or ("8898762") or ("7003497") or ("20020178122") or ("20040015406") or ("6571221") or ("9336635") or ("7467099") or ("7315823") or ("20120230490") or ("20150213661") or ("20070213047") or ("8706627") or ("8433658") or ("20100241494") or ("8489513") or ("20110103586") or ("8423476") or ("20020161723") or ("7308431") or	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:28
------	-----	---	------------------------------	----	-----	---------------------

("20040010472") or ("8856891") or
("6748367") or ("20140157393") or
("20070106897") or ("20060032905")
or ("7107248") or ("20030208386") or
("9367975") or ("8028329").PN. or
(("20150279130") or ("20080244714")
or ("9654448") or ("20110289314") or
("20040073440") or ("20120259774")
or ("20100201536") or ("8996861") or
("8213902") or ("20010045451") or
("7039802") or ("20110140656") or
("9026471") or ("20090036164") or
("20150256521") or ("7103572") or
("7269732") or ("7865731") or
("5850442") or ("8392699") or
("20140258011") or ("20160295411")
or ("20030191721") or
("20100250947") or ("20080313457")
or ("20130191244") or ("7945959") or
("20060282662") or ("8244636") or
("8718717") or ("20110131406") or
("20120072350") or ("8630933") or
("8452680") or ("20080148059") or
("20130185202") or ("7725928") or
("20090205033") or ("20020198849")
or ("20050177843") or
("20030120553") or ("20090187980")
or ("20070130617") or ("7970678") or
("7533065") or ("20120150670") or
("20100082492") or ("20140143142")
or ("20090132813") or
("20060190353") or ("9361741") or
("9483764") or ("20090287578") or
("20090198618") or ("8791790") or
("8073756") or ("9195982") or
("20110022668") or ("9129450") or
("9026472") or ("20030149662") or
("20160035162") or ("20140292482")
or ("20100174598") or ("7565329") or
("20020019811") or ("20070265984")
or ("20090113543") or ("8630932") or
("7120603") or ("8214299") or
("20080027814") or ("20110191196")
or ("20050261913") or
("20120191491") or ("20040243804")
or ("9374362") or ("20130198036") or
("20100201482") or ("20100228405")
or ("20110145564") or
("20040103064") or ("9092813") or
("9047634") or ("6675153") or
("20150095640") or ("20130198009")
or ("8914628") or ("7680736") or
("20120129577") or ("20150072654")
or ("20160104142") or ("8938402") or
("9558604") or ("20110208600") or
("8924310") or ("9519894") or
("7726579") or ("20040098350") or
("8924299") or ("20110119485") or
("20110191248") or ("20110191249")
or ("20110191250") or
("20090076966") or ("20160210799")
or ("20130191224") or
("20050033692") or ("20030061163")
or ("20130252585") or ("9264902") or

		("20040107170") or ("20090089366") or ("8949608") or ("20090179078") or ("20050138364") or ("20090265552") or ("20080046734") or ("20100275014").PN.				
L132	1	("9911258").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:28
L133	7036	(713/176).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:28
L134	190	(OUTWATER near CHRIS REDMANN near WILLIAM).in.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:28
L135	7036	(713/176).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:28
L136	14245	(G06Q20/32 OR G06Q20/38215 OR G07F15/005 OR H04L9/3263 OR Y02T90/12).CPC.	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:28
L137	20824	L135 L136	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:28
L138	274	reservation with certificate	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:28
L141	250	((("20090132813") or ("20070198432") or ("20090265552") or ("20080214111") or ("20080167060") or ("20030149662") or ("20030172090") or ("20040107170") or ("20060179452") or ("20090076966") or ("7426750") or ("20090037388") or ("20010051996") or ("20030055689") or ("20060157563") or ("7349871") or ("20040098350") or ("20070173266") or ("20050027543") or ("20050109841") or ("7213766") or ("20050246292") or ("6941285") or ("20040031856") or ("20070118426") or ("20080022089") or ("6607136") or ("7599847") or ("20090210347") or ("20050216354") or ("20030145205") or ("20080133930") or ("20050085226") or ("20080108324") or ("20050136949") or ("20050114367") or ("20060219776") or ("20050077349") or ("7597250") or ("20090119159") or ("20030097331") or ("20030065805") or ("20040128514") or ("20050017068") or ("20090144624") or ("20080189212") or ("20050040951") or ("7133659") or ("20030220835") or ("20080109370") or ("6609103") or ("20080057935") or ("20080081601") or ("7487112") or ("6771981") or ("7274928") or ("20040030601") or ("7079832") or ("20050170818") or ("6615183") or ("6622124") or	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:28

("6807532") or ("20020029350") or
("7366702") or ("20020073046") or
("20070244811") or ("20090037333")
or ("20090144202") or ("7155199") or
("20040019564") or ("20070083444")
or ("6516316") or ("20070255662") or
("20090198618") or ("6167251") or
("20070293202") or ("20070255652")
or ("20080217400") or ("7010512") or
("7505941") or ("20010000505") or
("6016476") or ("20070179895") or
("6836651") or ("20030061170") or
("20090089581") or ("6233577") or
("7379891") or ("7584149") or
("6938019") or ("7577619") or
("20040172340") or ("20060173781")
or ("20100031043") or ("7577575") or
("7617159") or ("6571221") or
("20080140577") or ("7031945") or
("7222101") or ("20090048975") or
("7599857") or ("7203665") or
("7343350") or ("20090222349") or
("7529713") or ("20050187883") or
("20080215878") or ("20050108096")
or ("6836765") or ("20070233615") or
("6744874") or ("7562051") or
("20010032878") or ("7415424") or
("6601040") or ("7577620") or
("20040210449") or ("20030088781")
or ("20080010220") or ("7280975") or
("20020040346") or ("20070106612")
or ("7627531") or ("7386517") or
("7451921") or ("20090049529") or
("20090157528") or ("6763336")).PN.
or ("20070255620") or
("20070197261") or ("20040210448")
or ("7415443") or ("7013001") or
("20060224470") or ("20080010217")
or ("20060032905") or
("20090157556") or ("20060043164")
or ("20080052183") or ("7162454") or
("7565328") or ("20090157557") or
("20090055315") or ("7013365") or
("20070255653") or ("20020194068")
or ("20030195847") or
("20090157554") or ("20040158532")
or ("20010034720") or
("20040255081") or ("7562028") or
("20020060246") or ("20080006685")
or ("20030200184") or
("20030172044") or ("7613659") or
("20090073965") or ("7343351") or
("20060218091") or ("20050033689")
or ("7340045") or ("20090070260") or
("6736322") or ("20060144925") or
("7565297") or ("20080091602") or
("7292999") or ("20090125429") or
("20030135740") or ("7210620") or
("20080255890") or ("6931382") or
("7103572") or ("7590602") or
("20080048022") or ("6553108") or
("20060153350") or ("20030195846")
or ("20040029566") or
("20020133467") or ("7216109") or

		(("20080207296") or ("20090265768") or ("7107248") or ("7080037") or ("7366703") or ("20020172345") or ("20070198436") or ("20090157558") or ("20040243520") or ("20020188863") or ("20080235108") or ("20050044044") or ("7467099") or ("20030195848") or ("7567934") or ("20030088647") or ("20090100508") or ("20090049528") or ("20020099665") or ("7540015") or ("20040260470") or ("20090113205") or ("20070106892") or ("20040015406") or ("7188110") or ("20090119190") or ("20090144205") or ("20060178994") or ("20070228161") or ("7127236") or ("20010037312") or ("20090187764") or ("20020100802") or ("6565000") or ("7139914") or ("7631193") or ("7555458") or ("7552467") or ("20040029569") or ("20070284434") or ("20090259588") or ("20100036772") or ("20070250920") or ("20090164325") or ("20020156704") or ("20030028481") or ("20080168270") or ("20090217046") or ("20090164329") or ("20050021983") or ("7448538") or ("20050085931") or ("20060076400") or ("20090164326") or ("20080319906") or ("20090164331") or ("20020161723") or ("20020077978") or ("20080319872") or ("20080040265") or ("20020100803") or ("7606401") or ("7308431") or ("20090164328") or ("7472827") or ("20090164327") or ("20090144203")).PN.				
L142	5	L138 and L141	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/08/15 08:28
L143	274	reservation with certificate	US-PGPUB; USPAT; USOCR	OR	ON	2019/08/15 08:28
L146	250	((("20090132813") or ("20070198432") or ("20090265552") or ("20080214111") or ("20080167060") or ("20030149662") or ("20030172090") or ("20040107170") or ("20060179452") or ("20090076966") or ("7426750") or ("20090037388") or ("20010051996") or ("20030055689") or ("20060157563") or ("7349871") or ("20040098350") or ("20070173266") or ("20050027543") or ("20050109841") or ("7213766") or ("20050246292") or ("6941285") or	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:28

("20040031856") or ("20070118426")
or ("20080022089") or ("6607136") or
("7599847") or ("20090210347") or
("20050216354") or ("20030145205")
or ("20080133930") or
("20050085226") or ("20080108324")
or ("20050136949") or
("20050114367") or ("20060219776")
or ("20050077349") or ("7597250") or
("20090119159") or ("20030097331")
or ("20030065805") or
("20040128514") or ("20050017068")
or ("20090144624") or
("20080189212") or ("20050040951")
or ("7133659") or ("20030220835") or
("20080109370") or ("6609103") or
("20080057935") or ("20080081601")
or ("7487112") or ("6771981") or
("7274928") or ("20040030601") or
("7079832") or ("20050170818") or
("6615183") or ("6622124") or
("6807532") or ("20020029350") or
("7366702") or ("20020073046") or
("20070244811") or ("20090037333")
or ("20090144202") or ("7155199") or
("20040019564") or ("20070083444")
or ("6516316") or ("20070255662") or
("20090198618") or ("6167251") or
("20070293202") or ("20070255652")
or ("20080217400") or ("7010512") or
("7505941") or ("20010000505") or
("6016476") or ("20070179895") or
("6836651") or ("20030061170") or
("20090089581") or ("6233577") or
("7379891") or ("7584149") or
("6938019") or ("7577619") or
("20040172340") or ("20060173781")
or ("20100031043") or ("7577575") or
("7617159") or ("6571221") or
("20080140577") or ("7031945") or
("7222101") or ("20090048975") or
("7599857") or ("7203665") or
("7343350") or ("20090222349") or
("7529713") or ("20050187883") or
("20080215878") or ("20050108096")
or ("6836765") or ("20070233615") or
("6744874") or ("7562051") or
("20010032878") or ("7415424") or
("6601040") or ("7577620") or
("20040210449") or ("20030088781")
or ("20080010220") or ("7280975") or
("20020040346") or ("20070106612")
or ("7627531") or ("7386517") or
("7451921") or ("20090049529") or
("20090157528") or ("6763336")).PN.
or ("20070255620") or
("20070197261") or ("20040210448")
or ("7415443") or ("7013001") or
("20060224470") or ("20080010217")
or ("20060032905") or
("20090157556") or ("20060043164")
or ("20080052183") or ("7162454") or
("7565328") or ("20090157557") or
("20090055315") or ("7013365") or

		(("20070255653") or ("20020194068") or ("20030195847") or ("20090157554") or ("20040158532") or ("20010034720") or ("20040255081") or ("7562028") or ("20020060246") or ("20080006685") or ("20030200184") or ("20030172044") or ("7613659") or ("20090073965") or ("7343351") or ("20060218091") or ("20050033689") or ("7340045") or ("20090070260") or ("6736322") or ("20060144925") or ("7565297") or ("20080091602") or ("7292999") or ("20090125429") or ("20030135740") or ("7210620") or ("20080255890") or ("6931382") or ("7103572") or ("7590602") or ("20080048022") or ("6553108") or ("20060153350") or ("20030195846") or ("20040029566") or ("20020133467") or ("7216109") or ("20080207296") or ("20090265768") or ("7107248") or ("7080037") or ("7366703") or ("20020172345") or ("20070198436") or ("20090157558") or ("20040243520") or ("20020188863") or ("20080235108") or ("20050044044") or ("7467099") or ("20030195848") or ("7567934") or ("20030088647") or ("20090100508") or ("20090049528") or ("20020099665") or ("7540015") or ("20040260470") or ("20090113205") or ("20070106892") or ("20040015406") or ("7188110") or ("20090119190") or ("20090144205") or ("20060178994") or ("20070228161") or ("7127236") or ("20010037312") or ("20090187764") or ("20020100802") or ("6565000") or ("7139914") or ("7631193") or ("7555458") or ("7552467") or ("20040029569") or ("20070284434") or ("20090259588") or ("20100036772") or ("20070250920") or ("20090164325") or ("20020156704") or ("20030028481") or ("20080168270") or ("20090217046") or ("20090164329") or ("20050021983") or ("7448538") or ("20050085931") or ("20060076400") or ("20090164326") or ("20080319906") or ("20090164331") or ("20020161723") or ("20020077978") or ("20080319872") or ("20080040265") or ("20020100803") or ("7606401") or ("7308431") or ("20090164328") or ("7472827") or ("20090164327") or ("20090144203")).PN.				
L147	5	L143 and L146	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2019/08/15 08:28

EAST Search History

			EPO; JPO; DERWENT; IBM_TDB			
L148	1	("10049514").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/15 08:28

8/ 15/ 2019 8:41:51 AM
C:\ Users\ bhoffman\ Documents\ EAST\ Workspaces\ 16034278.wsp

Doc code: IDS

PTO/SB/08a (01-10)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16034278
	Filing Date	2018-07-12
	First Named Inventor	Outwater
	Art Unit	2433
	Examiner Name	HOFFMAN, BRANDON S
	Attorney Docket Number	LBT0010-CON3

U.S. PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	3742453		1973-06-26	Poylo	Entire document
	2	5933085		1999-08-03	Holcomb et al.	Entire document
	3	6950808		2005-09-27	Kyojima et al.	Entire document
	4	6975202		2005-12-13	Rodriguez et al.	Entire document
	5	7012503		2006-03-14	Nielsen	Entire document
	6	7114178		2006-09-26	Dent et al.	Entire document
	7	7114179		2006-09-26	Ritter et al.	Entire document
	8	7170998		2007-01-30	McIntock et al.	Entire document

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16034278
Filing Date	2018-07-12
First Named Inventor	Outwater
Art Unit	2433
Examiner Name	HOFFMAN, BRANDON S
Attorney Docket Number	LBT0010-CON3

9	7196610		2007-03-27	Straumann et al.	Entire document
10	7209029		2007-04-24	Coelho et al.	Entire document
11	7315823		2008-01-01	Brondrup	Entire document
12	7457418		2008-11-25	Bunte et al.	Entire document
13	7706778		2010-04-27	Lowe	Entire document
14	8730004		2014-05-20	Elfstrom et al.	Entire document

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS

Remove

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20080148369		2008-06-19	Aaron	Entire document
	2	20090183541		2009-07-23	Sadighi et al.	Entire document
	3	20100201536		2010-08-12	Robertson	Entire document

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16034278
Filing Date	2018-07-12
First Named Inventor	Outwater
Art Unit	2433
Examiner Name	HOFFMAN, BRANDON S
Attorney Docket Number	LBT0010-CON3

4	20020031228	2002-03-14	Karkas et al.	Entire document
5	20020099945	2002-07-25	McIntock et al.	Entire document
6	20020180582	2002-12-05	Nielsen	Entire document
7	20030016828	2003-01-23	Bunte et al.	Entire document
8	20030151493	2003-08-14	Straumann et al.	Entire document
9	20030208386	2003-11-06	Brondrup	Entire document
10	20040025039	2004-02-05	Kuenzi et al.	Entire document
11	20040059815	2004-03-25	Buckingham et al.	Entire document
12	20050241003	2005-10-27	Sweeney et al.	Entire document
13	20060072755	2006-04-06	Oskari	Entire document
14	20070034691	2007-02-15	Davis et al.	Entire document

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16034278
Filing Date	2018-07-12
First Named Inventor	Outwater
Art Unit	2433
Examiner Name	HOFFMAN, BRANDON S
Attorney Docket Number	LBT0010-CON3

15	20070035381	2007-02-15	Davis	Entire document
16	20070126562	2006-08-15	Ku	Entire document
17	20070176739	2007-08-02	Raheman	Entire document
18	20070197261	2007-08-23	Humbel	Entire document
19	20070200665	2007-08-30	Studerus	Entire document
20	20070290789	2007-12-20	Segev et al.	Entire document
21	20080024272	2008-01-31	Fiske	Entire document
22	20090066476	2009-03-12	Raheman	Entire document
23	20090136035	2009-05-28	Lee	Entire document
24	20090184801	2009-07-23	Bliding et al.	Entire document
25	20100141381	2010-06-10	Bliding et al.	Entire document

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16034278
Filing Date	2018-07-12
First Named Inventor	Outwater
Art Unit	2433
Examiner Name	HOFFMAN, BRANDON S
Attorney Docket Number	LBT0010-CON3

26	20100176919	2010-07-15	Myers et al.	Entire document
27	20100191551	2009-10-01	Drance et al.	Entire document
28	20110001603	2011-01-06	Willis	Entire document
29	20110112969	2011-05-12	Zaid et al.	Entire document

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2005080720	WO	A1	2005-09-01	Wilgert	Entire document	
	2	2008076074	WO	A1	2008-06-26	Knutsson et al.	Entire document	
	3	1783694	EP	B1	2011-02-16	Perez et al.	Entire document	
	4	2364202A	GB	A	2002-01-16	Kalle et al.	Entire document	
	5	2002125266	JP		2002-04-26	Watanabe et al.	Entire document	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16034278
Filing Date	2018-07-12
First Named Inventor	Outwater
Art Unit	2433
Examiner Name	HOFFMAN, BRANDON S
Attorney Docket Number	LBT0010-CON3

6	1020020087057	KR	A	2007-03-15	Yanai	Entire document	×
7	1020070012735	KR	A	2005-05-13	Markham	Entire document	☒

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	The Institute of Electrical and Electronics Engineers, Inc., "IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" copyright 2007, printed in the United States of America	
	2	The Institute of Electrical and Electronics Engineers, Inc., "IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 2: Fast Basic Service Set (BSS) Transition" copyright 2008, printed in the United States of America	
	3	LodgingHospitality, "Technically Speaking, How Technology Enhances the Bottom Line, New System Links Cellphones, Lock Systems," LHOnline.com, January 2010	
	4	General Electric, "Supra," http://www.geindustrial.com:80/ge-interlogix/supra/index.html	

If you wish to add additional non-patent literature document citation information please click the Add button

Add

EXAMINER SIGNATURE

Examiner Signature	/BRANDON S HOFFMAN/	Date Considered	08/14/2019
--------------------	---------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16034278
	Filing Date	2018-07-12
	First Named Inventor	Outwater
	Art Unit	2433
	Examiner Name	HOFFMAN, BRANDON S
	Attorney Docket Number	LBT0010-CON3

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Kelly L. Kasha/	Date (YYYY-MM-DD)	2018-10-18
Name/Print	Kelly L. Kasha	Registration Number	47743

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

~~ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /B.S.H/~~

Bibliographic Data

Application No: 16/034,278

Foreign Priority claimed: ☐ Yes ☒ No

35 USC 119 (a-d) conditions met: ☐ Yes ☒ No ☐ Met After Allowance

Verified and Acknowledged: /BRANDON S HOFFMAN/

Examiner's Signature

Initials

Title:

Access Control System and Method for Use by an Access Device

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
07/12/2018	713	2433	LBT0010-CON3
RULE			

APPLICANTS

Liberty PlugIns, Inc., Santa Barbara, CA, UNITED STATES

INVENTORS

Chris Outwater Carpinteria, CA, UNITED STATES

William Gibbens Redmann Glendale, CA, UNITED STATES

CONTINUING DATA

This application is a CON of 15609055 05/31/2017 PAT 10049514

15609055 is a CON of 15178849 06/10/2016 PAT 9911258

15178849 is a CON of 14603434 01/23/2015 PAT 9373205

14603434 is a CON of 13582467 09/04/2012 PAT 8996876

13582467 is a 371 of PCT/US11/26781 03/02/2011

PCT/US11/26781 has PRO of 61309813 03/02/2010

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

08/13/2018

**** SMALL ENTITY ****

STATE OR COUNTRY

UNITED STATES

ADDRESS

KASHA LAW LLC
14532 Dufief Mill Road
North Potomac, MD 20878
UNITED STATES

FILING FEE RECEIVED

\$785



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/034,278	07/12/2018	Chris Outwater	LBT0010-CON3

CONFIRMATION NO. 8554

67050
KASHA LAW LLC
14532 Dufief Mill Road
North Potomac, MD 20878

PUBLICATION NOTICE



Title:Access Control System and Method for Use by an Access Device

Publication No.US-2018-0336745-A1

Publication Date:11/22/2018

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <https://portal.uspto.gov/pair/PublicPair>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16034278
	Filing Date	2018-07-12
	First Named Inventor	Outwater
	Art Unit	2433
	Examiner Name	HOFFMAN, BRANDON S
	Attorney Docket Number	LBT0010-CON3

U.S. PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	
	1	3742453		1973-06-26	Poylo	Entire document	
	2	5933085		1999-08-03	Holcomb et al.	Entire document	
	3	6950808		2005-09-27	Kyojima et al.	Entire document	
	4	6975202		2005-12-13	Rodriguez et al.	Entire document	
	5	7012503		2006-03-14	Nielsen	Entire document	
	6	7114178		2006-09-26	Dent et al.	Entire document	
	7	7114179		2006-09-26	Ritter et al.	Entire document	
	8	7170998		2007-01-30	McIntock et al.	Entire document	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16034278	
	Filing Date		2018-07-12	
	First Named Inventor	Outwater		
	Art Unit	2433		
	Examiner Name	HOFFMAN, BRANDON S		
	Attorney Docket Number	LBT0010-CON3		

	9	7196610		2007-03-27	Straumann et al.	Entire document
	10	7209029		2007-04-24	Coelho et al.	Entire document
	11	7315823		2008-01-01	Brondrup	Entire document
	12	7457418		2008-11-25	Bunte et al.	Entire document
	13	7706778		2010-04-27	Lowe	Entire document
	14	8730004		2014-05-20	Elfstrom et al.	Entire document

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS

Remove

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20080148369		2008-06-19	Aaron	Entire document
	2	20090183541		2009-07-23	Sadighi et al.	Entire document
	3	20100201536		2010-08-12	Robertson	Entire document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16034278	
	Filing Date		2018-07-12	
	First Named Inventor	Outwater		
	Art Unit	2433		
	Examiner Name	HOFFMAN, BRANDON S		
	Attorney Docket Number	LBT0010-CON3		

	4	20020031228		2002-03-14	Karkas et al.	Entire document
	5	20020099945		2002-07-25	McIntock et al.	Entire document
	6	20020180582		2002-12-05	Nielsen	Entire document
	7	20030016828		2003-01-23	Bunte et al.	Entire document
	8	20030151493		2003-08-14	Straumann et al.	Entire document
	9	20030208386		2003-11-06	Brondrup	Entire document
	10	20040025039		2004-02-05	Kuenzi et al.	Entire document
	11	20040059815		2004-03-25	Buckingham et al.	Entire document
	12	20050241003		2005-10-27	Sweeney et al.	Entire document
	13	20060072755		2006-04-06	Oskari	Entire document
	14	20070034691		2007-02-15	Davis et al.	Entire document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16034278
	Filing Date		2018-07-12
	First Named Inventor	Outwater	
	Art Unit	2433	
	Examiner Name	HOFFMAN, BRANDON S	
	Attorney Docket Number	LBT0010-CON3	

	15	20070035381		2007-02-15	Davis	Entire document
	16	20070126562		2006-08-15	Ku	Entire document
	17	20070176739		2007-08-02	Raheman	Entire document
	18	20070197261		2007-08-23	Humbel	Entire document
	19	20070200665		2007-08-30	Studerus	Entire document
	20	20070290789		2007-12-20	Segev et al.	Entire document
	21	20080024272		2008-01-31	Fiske	Entire document
	22	20090066476		2009-03-12	Raheman	Entire document
	23	20090136035		2009-05-28	Lee	Entire document
	24	20090184801		2009-07-23	Bliding et al.	Entire document
	25	20100141381		2010-06-10	Bliding et al.	Entire document

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16034278	
	Filing Date		2018-07-12	
	First Named Inventor	Outwater		
	Art Unit	2433		
	Examiner Name	HOFFMAN, BRANDON S		
	Attorney Docket Number	LBT0010-CON3		

	26	20100176919		2010-07-15	Myers et al.	Entire document
	27	20100191551		2009-10-01	Drance et al.	Entire document
	28	20110001603		2011-01-06	Willis	Entire document
	29	20110112969		2011-05-12	Zaid et al.	Entire document

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2005080720	WO	A1	2005-09-01	Wilgert	Entire document	
	2	2008076074	WO	A1	2008-06-26	Knutsson et al.	Entire document	
	3	1783694	EP	B1	2011-02-16	Perez et al.	Entire document	
	4	2364202A	GB	A	2002-01-16	Kalle et al.	Entire document	
	5	2002125266	JP		2002-04-26	Watanabe et al.	Entire document	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16034278	
	Filing Date		2018-07-12	
	First Named Inventor	Outwater		
	Art Unit	2433		
	Examiner Name	HOFFMAN, BRANDON S		
	Attorney Docket Number	LBT0010-CON3		

6	1020020087057	KR	A	2007-03-15	Yanai	Entire document	×
7	1020070012735	KR	A	2005-05-13	Markham	Entire document	☒

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	The Institute of Electrical and Electronics Engineers, Inc., "IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" copyright 2007, printed in the United States of America	
	2	The Institute of Electrical and Electronics Engineers, Inc., "IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 2: Fast Basic Service Set (BSS) Transition" copyright 2008, printed in the United States of America	
	3	LodgingHospitality, "Technically Speaking, How Technology Enhances the Bottom Line, New System Links Cellphones, Lock Systems," LHOnline.com, January 2010	
	4	General Electric, "Supra," http://www.geindustrial.com:80/ge-interlogix/supra/index.html	

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16034278
	Filing Date		2018-07-12
	First Named Inventor	Outwater	
	Art Unit	2433	
	Examiner Name	HOFFMAN, BRANDON S	
	Attorney Docket Number	LBT0010-CON3	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Kelly L. Kasha/	Date (YYYY-MM-DD)	2018-10-18
Name/Print	Kelly L. Kasha	Registration Number	47743

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

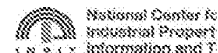
The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



Help desk (9:00-21:00)
 (+81)3-6666-8801
helpdesk@j-platpat.inpit.go.jp

[Japanese](#) [Top page](#) [Help list](#) [Site map](#) [PDF](#)



[Patent & Utility Model](#)

[Design](#)

[Trademark](#)

[Trial & Appeal](#)

[Top page](#)

[Patent & Utility Model](#)

[Patent & Utility Model Number Search](#)

Patent & Utility Model Number Search

[Back](#)

[Help](#)

[Search](#)

[List](#)

[I](#)

You can retrieve a variety of patent and utility model gazettes by their numbers.

Selected Gazette

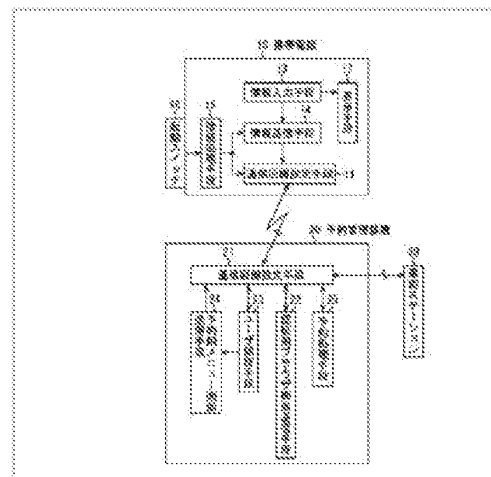
[Previous Document](#) [1/1](#) [Next Document](#)

JP,2002-125266,A

[PAJ](#) [Detail](#) [Image](#)

[Legal](#)

(11)Publication number	2002-125266
(43)Date of publication of application	26.04.2002
(51)Int.Cl.	H04Q 7/38
	G06F 15/00
	G06F 17/60
	G08G 1/00
	H04M 11/00
(21)Application number	2000-313866
(22)Date of filing	13.10.2000
(71)Applicant	SUZUKI MOTOR CORP
(72)Inventor	WATANABE HIROSHI
	SATO KENJI
	INAGAKI MAKOTO
	NISHIGORI HIDETAKA
	KONISHI YASUYUKI
	ASAKAWA YOSHIYUKI



(54)PORTABLE TELEPHONE AND RESERVATION MANAGING DEVICE AND RESERVATION MANAGING SYSTEM AND STORAGE MEDIUM

(57)Abstract

PROBLEM TO BE SOLVED: To easily make a reservation anytime and anywhere by using a portable telephone with a compact browser built-in.
SOLUTION: A reservation control center is provided with a reservation control means for transmitting a browser picture for authentication corresponding to calling performed through a portable telephone network, and for performing authentication processing based on individual information inputted to the browser picture for authentication, and for, when a user who makes a call is a legal user, transmitting a menu picture for reservation to the portable telephone which makes the call, and for judging the validity/invalidity of reservation based on reservation desire information inputted through the menu picture for reservation, and for, when the reservation is valid, transmitting a browser picture in the case of the validity of reservation, and for, when the reservation is invalid, transmitting a browser picture in the case of the invalidity of reservation. Thus, it is possible to easily

[To return to the top of this](#)

[Notice on Usage](#) [Privacy Policy](#) [Questionnaire](#)

Electronic Acknowledgement Receipt	
EFS ID:	34043914
Application Number:	16034278
International Application Number:	
Confirmation Number:	8554
Title of Invention:	Access Control System and Method for Use by an Access Device
First Named Inventor/Applicant Name:	Chris Outwater
Customer Number:	67050
Filer:	John Kasha/Kelly Kasha
Filer Authorized By:	John Kasha
Attorney Docket Number:	LBT0010-CON3
Receipt Date:	18-OCT-2018
Filing Date:	12-JUL-2018
Time Stamp:	15:15:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	KR1020020087057.pdf	23361666	no	20
			27cab1e5698e6d55a3be17f2615465d338945520		

Warnings:

Information:					
2	Foreign Reference	KR1020070012735.pdf	2957389	no	25
			1574ce930eab09506d24021e4e3acfe03cc bc17		
Warnings:					
Information:					
3	Foreign Reference	WO2008076074A1.pdf	484676	no	41
			b30974192dea273a73e8600a3752da8a064 a9a16		
Warnings:					
Information:					
4	Foreign Reference	GB2364202A.pdf	965677	no	27
			1cffc3b6e0d8f87af1c9cdc3c8e54264044b2 43d		
Warnings:					
Information:					
5	Foreign Reference	EP1783694B1.pdf	443693	no	18
			90d51e5c224290a76c8d0ca6c7c3193707c 122aa		
Warnings:					
Information:					
6	Foreign Reference	WO2005080720A1.pdf	318199	no	15
			ca6094c039084cc13ce078b070ae73f16811 3c51		
Warnings:					
Information:					
7	Non Patent Literature	Onity848-1100_1.pdf	8086124	no	253
			0cca0406eed1d44f10430a66a9e8469dc79 4991d		
Warnings:					
Information:					
8	Non Patent Literature	Onity1101-1400_1.pdf	7784252	no	300
			409a58d3f63a33a525c09f1b694c2b2c7050 5efe		
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					

Information:					
9	Non Patent Literature	Onity1401-1700_1.pdf	9120943	no	300
			afc7ec37bb9a72788e50284b4093b366540e7fce		
Warnings:					
Information:					
10	Non Patent Literature	Onity1701-2079_1.pdf	13132209	no	379
			6d3946c0088dee387df7c92b59759a3cce82c72c		
Warnings:					
Information:					
11	Non Patent Literature	Onity2725-2759.pdf	16606360	no	35
			d961a97530556ba0d93c587e763b562175f3c90b		
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
12	Non Patent Literature	Onity2301-2500_2small.pdf	15588806	no	200
			2de2eed58b1fd725b79a225fbcaee7411ef79bc2		
Warnings:					
Information:					
13	Non Patent Literature	Onity2080-2300_2small.pdf	16447330	no	221
			000a823f0c68edbaeaf377c08dba5d00be560fa0		
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
14	Non Patent Literature	Onity2501-2701_2small_shrink.pdf	19166074	no	201
			c86425fc40dad5e1670e2fc521cf1a70995134b7		
Warnings:					
Information:					

15	Information Disclosure Statement (IDS) Form (SB08)	LBT0010- CON3_ids_10_18_2018.pdf	614233	no	8
			2b85511ef06a42c161a3541752cf1bc6568597d2		
Warnings:					
Information:					
16	Foreign Reference	JP2002125266A.pdf	137137	no	1
			4dad8d09a38c256de335d9de1392b66b50925931		
Warnings:					
Information:					
Total Files Size (in bytes):			135214768		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

Bibliographic Data

Int.Cl.	G06Q 10/02 G06Q 50/10 G07B 15/00
Published Date	20070315
Registration No.	1006960540000
Registration Date	20070309
Application No.	1020027011294
Application Date	20010313
Unexamined Publication No.	1020020087057
Unexamined Publication Date	20021121
Priority Claims	JP-P-2000-00068817 20000313 JP
Requested Date of Examination	20041222
Agent.	Kim Myung Shin Park Jang Kyu
Inventor	YANAI,Hiroshi
Rightholder	PiA KoPoReISyeon

발명의 명칭

전자티켓 시스템

Title of Invention

ELECTRONIC TICKET SYSTEM

요약

본 발명은 전자티켓 시스템에 관한 것으로서, 통신수단을 통해 티켓의 권리 정보를 구입하고, 그 권리 정보의 기록이 가능한 기억매체를 이용하여 회장에 입장에 가능한 전자티켓 시스템을 제공하는 것을 목적으로 한다.

티켓의 권리 정보의 기록이 가능한 기록매체(28)를 구비한 데이터 통신 단말(10)과, 그 데이터 통신 단말(10)과 통신수단(16)을 통해 접속하고, 티켓의 권리 정보의 상기 기억매체(28)로의 기록을 실시하는 티켓 판매 센터(12)와, 티켓의 권리 정보가 기록된 기록 매체를 지참하는 입장자가 통과할 때 그 티켓의 권리 정보를 인증하여 입장의 허가를 실시하는 입장 관리 단말(14)을 구비하는 전자티켓 시스템을 이용하여 상기 데이터 통신 단말(10)에서 상기 티켓 판매 센터(12)로 티켓 구입의 신청을 실시하고, 그 신청을 받은 티켓 판매 센터(12)는 티켓의 권리 정보(35)를 발행하고, 그 티켓의 권리 정보(35)가 상기 기록매체(28)에 기록되는 것으로 티켓의 구입을 가능하게 했다.

Abstract

The object of the invention is to provide the electronic ticket system which buys the rights information of the ticket as the invention relating to the electronic ticket system through the communication means and is possible using the storage media in which the register of the rights information is possible in the present in the position.

It connected through data communication terminal (10), equipped with the recording medium (28) in which the register of the rights information of the ticket was possible and data communication terminal (10) and communication means (16) and the Petition of the ticket purchase was performed to the ticket selling center (12) using the electronic ticket system equipped with the ticket selling center (12), performing register to the storage media (28) of the rights information of the ticket and the position management terminal (14) which authenticated the rights information of the ticket when the attendance bringing t

또, 그 기록매체(28)를 지참하고, 상기 입장 관리 단말(1

Bibliographic Abstract Drawing Claims Description

$$0.1(33) \approx 0.024 \approx 0.024(14) \approx 0.024 \approx 0.024 \approx 0.024$$

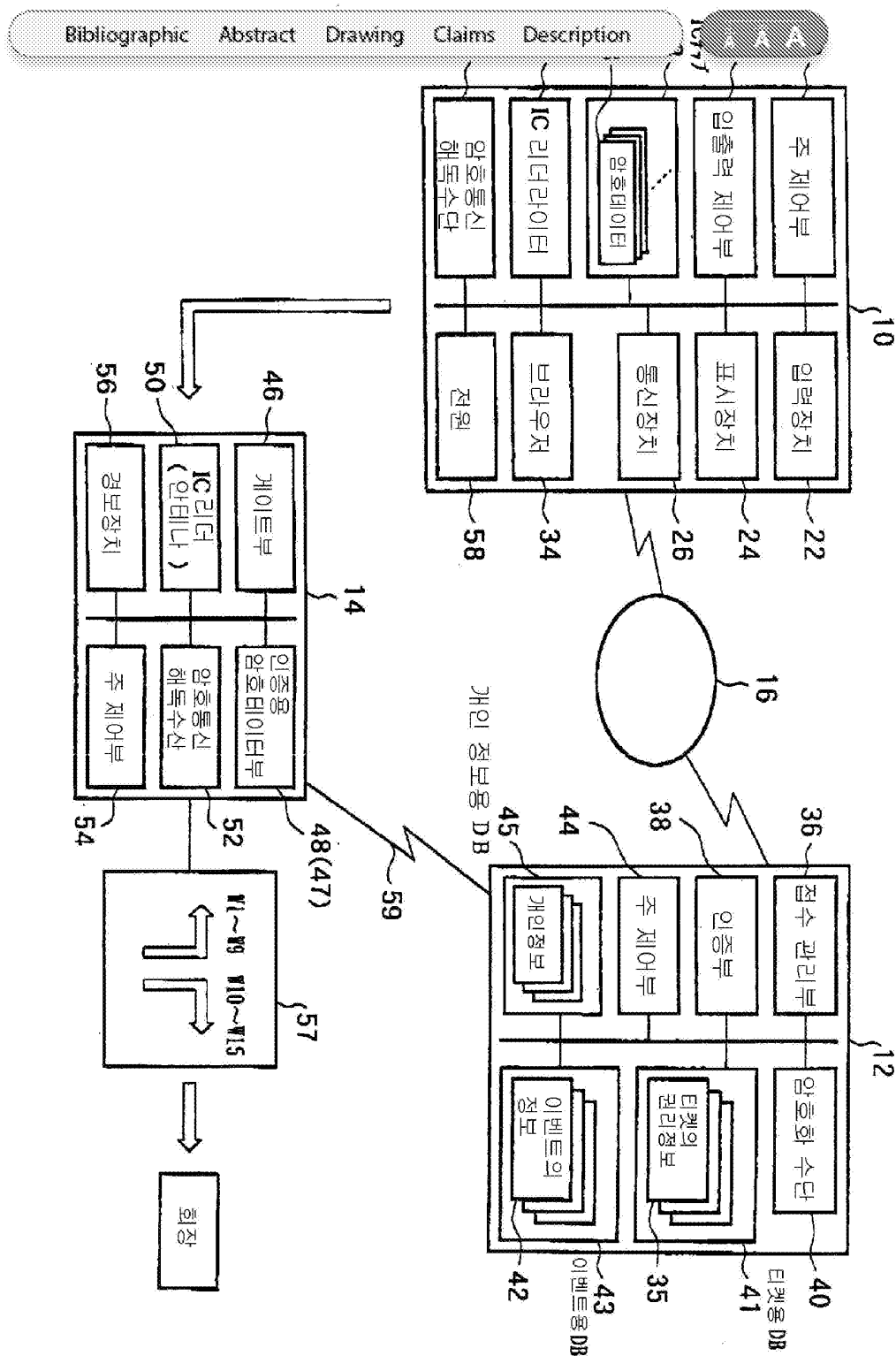
장의 허가를 실시하도록 한 것을 특징으로 한다.

the recording medium in which the rights information
 description is recorded is passed and performed the
 organization of the rights information in data communicatio

n terminal (10) and the ticket selling center (12) which request for the was received published the rights information (35) of the ticket and the rights information (35) of the ticket was recorded in the recording medium (28) and it made the purchase of the ticket possible.

And the recording medium (28) is brought and by a authenticating the rights information (35) of the ticket recorded in the recording medium (28) to the position management terminal (14) when passing the position management terminal (14) the authorization of the position is performed.

대표도면(Representative drawing)



청구의 범위

Scope of Claims

청구 1항:

Claim 1:

컴퓨터 시스템에 의해 티켓을 전자화하여 발행하는 전자

Bibliographic Abstract Drawing Claims Description

티켓 정보를 기억하는 티켓 정보 기억수단, 티켓 신청자에 대해 티켓 신청자의 개인 정보의 입력을 요구하는 한편, 상기 티켓 정보 기억수단에 기억시킨 티켓 정보를 개시하고 상기 티켓 정보의 선택을 요구하는 티켓 신청 접수수단; 상기 입력된 개인 정보를 인증하는 인증수단; 상기 인증수단에 의한 인증후 상기 선택된 티켓 정보로 이루어진 전자티켓을 암호데이터로 암호화하는 암호화수단; 및 상기 암호화수단에 있어서 암호화된 암호데이터를 신청자에 대해 발행하는 전자티켓 발행수단을 구비하는 것을 특징으로 하는 전자티켓 시스템.

The electronic ticket system including the ticket information storage means for memorizing the ticket information; the ticket issuing means for expressing the content of the ticket issuing data to the electronic ticket system which digitalizes the ticket with the computer system and published; the ticket acceptance of application means which demands the input of the personal information of the ticket applicant from the ticket applicant; and it discloses the ticket information which memorizes in the ticket information storage means and demands the selection of the ticket information; the authentication means authenticating the above-mentioned inputted personal information; the encrypting means encoding the e-ticket made of the selected ticket information after the authentication by the authentication means to data encryption; and the e-ticket issuing means publishing data encryption encrypted as to the encrypting means about the applicant.

청구 2항:

제 1 항에 있어서, 상기 전자티켓을 상기 인증된 개인정보와 상기 선택된 티켓 정보로 형성하는 것을 특징으로 하는 전자티켓 시스템.

Claim 2:

As for claim 1, the electronic ticket system forming the e-ticket into the above-mentioned authenticated personal information and selected ticket information.

청구 4항:

제 1 항 내지 제 3 항 중 어느 한 항에 있어서, 상기 전자 티켓 발행수단에 있어서, 상기 암호 데이터를 신청자가 소유하는 기억매체에 기억시키는 것을 특징으로 하는 전자 티켓 시스템.

Claim 4:

As for any one of claim 1 through 3, the electronic ticket system memorized in the storage media in which the applicant possesses data encryption as to the electron ticket issuer.

청구 5항:

제 1 항 내지 제 5 항 중 어느 한 항에 있어서, 티켓을 인증하는 개찰 게이트에 있어서, 상기 기억매체에 기억된 암호 데이터를 인증하는 입장관리단말로서, 상기 전자티켓의 정보를 기억시키는 전자티켓 정보 기억수단; 상기 기억매체에 기억된 암호 데이터를 검지하는 암호 데이터 검지수단; 상기 암호데이터 검지수단에 의해 검지된 암호 데이터의 정보와, 상기 전자티켓 정보 기억수단에 기억시킨 정보를 조합(照合)하는 조합수단; 및 상기 조합수단에 의한 조합을 기초로 개찰 게이트의 개폐를 제어하는 개찰 게이트 제어수단을 구비하는 것을 특징으로 하는 전자티켓 시스템.

Claim 5:

As for any one of claim 1 through 5, the electronic ticket system which comprises the information of the e-ticket information storage means: data encryption detection means: data encryption detected with the data encryption detection means detects the data encryption memorized in the storage media remains the information of the e-ticket it is the position management terminal authenticating the data encryption memorized in the storage media as to the opening of the bids gate authenticating the ticket, the combination means assembling the information memorized in the e-ticket information storage means, and the opening of the bids gate control means controlling opening and shutting of the opening of the bids gate based on the combination by the combination means.

청구 6항:

제 5 항에 있어서, 상기 암호 데이터 검지수단을 상기 기억 매체에 접촉하지 않고 상기 암호 데이터의 검지가 가능하게 하는 것을 특징으로 하는 전자티켓 시스템,

Claim 6:

As for claim 5, the electronic ticket system which does not contact the data encryption detection means in the storage media and in which it makes possible.

청구 7항:

제 4 항 내지 제 6 항 중 어느 한 항에 있어서, 상기 기억매체를 상기 암호 데이터의 기억이 가능한 IC카드로 하는 것을 특징으로 하는 전자티켓 시스템.

Claim 7:

As for any one of claim 4 through 6, the electronic ticket system the storage media to the IC card in which the memory of the data encryption is possible.

Bibliographic	Abstract	Drawing	Claims	Description
---------------	----------	---------	--------	-------------

AAA

제 4 항 내지 제 6 항 중 어느 한 항에 있어서, 상기 기억매체를, 암호데이터의 기억이 가능한 IC칩; 상기 IC칩에 기억된 암호 데이터를 해독하여 복호화하는 암호 통신 해독수단; 및 복호화된 암호 데이터의 정보를 표시하는 표시장치를 구비하는 휴대형 데이터 통신단말로 하는 것을 특징으로 하는 전자티켓 시스템.

As for any one of claim 4 through 6, the electronic ticket system which it is done by the hand-held data communication terminal equipped with the IC chip, the cryptographic communication means of decoding, and the display device indicating the information of the decoded data encryption, and as to the IC chip, the memory of data encryption is the storage media possible; and the cryptographic communication means of decoding decodes data encryption memorized in the IC chip and decoded.

청구 9항:

제 5 항에 있어서, 상기 입장 관리 단말에 상기 조합수단에 의한 조합을 기초로 위법 통과를 알리는 경보장치를 구비하는 것을 특징으로 하는 전자티켓 시스템.

Claim 9:

As for claim 5, the electronic ticket system equipped with the alarm informing the position management terminal of the illegality pass based on the combination by the combination means.

청구 10항:

제 5 항에 있어서, 상기 입장 관리 단말에 상기 티켓 정보에 기초하여 회장(會場)을 안내하기 위한 회장 안내 정보 출력부를 구비하는 것을 특징으로 하는 전자티켓 시스템.

Claim 10:

As for claim 5, the electronic ticket system equipped with the president guidance information output part for guiding the president in the position management terminal based on the ticket information.

청구 11항:

서버 컴퓨터에 의해 티켓을 전자화하여 발행하는 전자 티켓 시스템에 있어서, 발행되는 티켓의 내용을 나타내는 티켓 정보를 기억하는 티켓 정보 기억수단; 티켓 신청자의 컴퓨터 단말에 대해 컴퓨터 네트워크를 통해 티켓 신청자의 개인 정보의 입력을 요구하는 한편, 상기 티켓 정보 기억수단에 기억시킨 티켓 정보를 개시하여 상기 티켓 정보의 선택을 요구하는 티켓 신청 접수수단; 상기 입력된 개인 정보를 인증하는 인증수단; 상기 인증수단에 의한 인증후 상기 선택된 티켓정보로 이루어진 전자티켓을 암호데이터로 암호화하는 암호화수단; 및 상기 암호화수단에서 암호화된 암호 데이터를 신청자의 컴퓨터 단말에 대해 컴퓨터 네트워크를 통해 송신하는 전자티켓 발행수단을 구비하는 것을 특징으로 하는 전자티켓 시스템.

Claim 11:

The electronic ticket system including the ticket information storage means memorizing the ticket information expressing the content of the ticket issuing apparatus to the electronic ticket system which digitalizes the ticket with the server computer and published; the ticket acceptance of application means which demands the input of the personal information of the ticket applicant from the computer terminal of the ticket applicant through the computer network; and it discloses the ticket information which memorizes in the ticket information storage means and demands the selection of the ticket information; the authentication means authenticating the above-mentioned inputted personal information; the encrypting means encoding the e-ticket made of the selected ticket information after the authentication by the authentication means to the data encryption; and the e-ticket issuing means transmitting the data encryption encrypted in the encrypting means about the computer terminal of the applicant through the computer network.

청구 12항:

제 11 항에 있어서, 상기 전자티켓을 상기 인증된 개인 정보와 상기 선택된 티켓 정보로 형성하는 것을 특징으로 하는 전자티켓 시스템.

Claim 12:

As for claim 11, the electronic ticket system forming the e-ticket into the above-mentioned authenticated personal information and selected ticket information.

청구 14항:

제 11 항 내지 제 13 항 중 어느 한 항에 있어서, 상기 암호 데이터에 암호화된 상기 전자티켓의 정보를 기억하는

Claim 14:

As for any one of claim 11 through 13, the electronic ticket system equipped with the e-ticket storage device

전자티켓 기억수단을 구비하는 것을 특징으로 하는 전자 티켓 memorizing the information of the encrypted e
 Bibliographic Abstract Drawing Claims Description d A A A A on.

청구 15항:

제 14 항에 있어서, 티켓을 인증하는 개찰 게이트에 있어서, 상기 기억매체에 기억된 암호데이터를 인증하는 입장 관리 단말로서, 암호 데이터를 해독하여 복호화하는 암호 통신 해독수단; 상기 전자티켓 기억수단에 기억된 전자티켓의 정보의 암호 데이터를 컴퓨터 네트워크를 통해 서버 컴퓨터로부터 전송하고, 암호 통신 해독수단에 의해 복호화하고, 상기 전자티켓의 정보를 기억하는 전자티켓 정보 기억수단; 상기 기억매체에 기억된 암호 데이터를 검지하는 암호 데이터 검지수단; 상기 암호 데이터 검지수단에 의해 검지된 암호 데이터의 정보와, 상기 전자티켓 정보 기억수단에 기억된 정보를 조합하는 조합수단; 및 상기 조합수단에 의한 조합을 기초로 개찰게이트의 개폐를 제어하는 개찰 게이트 제어수단을 구비하는 것을 특징으로 하는 전자티켓 시스템.

Claim 15:

As for claim 14, the electronic ticket system including the cryptographic communication means of decoding which it is the position management terminal authenticating the data encryption memorized in the storage media as to the opening of the bids gate authenticating the ticket ; and it decodes and decodes the data encryption; the e-ticket information storage means which transmits the data encryption of the information of the e-ticket memorized in the e-ticket storage device through the computer network from the server computer ; it decodes with the cryptographic communication means of decoding ; and remembers the information of the e-ticket; the data encryption detection means detecting the data encryption memorized in the storage media; the combination means assembling the information of the data encryption detected with the data encryption detection means and the information memorized in the e-ticket information storage means; and the opening of the bids gate control means controlling opening and shutting of the opening of the bids gate based on the combination by the combination means.

청구 17항:

제 11 항 내지 제 15 항 중 어느 한 항에 있어서, 상기 신청자의 컴퓨터 단말을, 컴퓨터 네트워크를 통해 서버 컴퓨터로 암호 데이터를 수신하는 입출력 제어부; 상기 암호 데이터의 기억이 가능한 기억매체; 상기 기억매체에 기억된 암호 데이터를 해독하여 복호화하는 암호 통신 해독수단; 및 복호화된 암호 데이터의 정보를 표시하는 표시장치를 구비한 휴대형 데이터 통신 단말로 하는 것을 특징으로 하는 전자티켓 시스템.

Claim 17:

As for any one of claim 11 through 15, the electronic ticket system which it is done by the hand-held data communication terminal equipped with the input/output control section receiving data encryption the computer terminal of the applicant through the computer network to the server computer, the storage media, the cryptographic communication means of encoding, and the display device indicating the information of the decoded data encryption, and as to the storage media, the memory of data encryption is possible; and the cryptographic communication means of decoding decodes data encryption memorized in the storage media and decoded.

청구 18항:

제 13 항 내지 제 17 항 중 어느 한 항에 있어서, 상기 기억매체를 상기 암호데이터의 기억이 가능한 IC칩 또는 IC 카드로 하는 것을 특징으로 하는 전자티켓 시스템.

Claim 18:

As for any one of claim 13 through 17, the IC chip in which the memory of data encryption is the storage media possible or the electronic ticket system which it is done by the IC card.

청구 20항:

제 15 항에 있어서, 상기 입장 관리 단말에 상기 티켓 정보에 기초하여 회장을 안내하기 위한 회장 안내 정보 출력부를 구비하는 것을 특징으로 하는 전자티켓 시스템.

Claim 20:

As for claim 15, the electronic ticket system equipped with the president guidance information output part for guiding the president in the position management terminal based on the ticket information.

청구 21항:

서버컴퓨터에 의해 티켓을 전자화하여 발행하는 전자티켓 시스템에 있어서, 발행되는 티켓의 내용을 나타내는 티켓

Claim 21:

The electronic ticket system including the ticket information storage means memorizing the ticket information expressing the content of the ticket issuing a

정보를 기억하는 티켓 정보 기억수단; 티켓 신청자의 컴퓨터
Bibliographic Abstract Drawing Claims Desc
단에 기억시킨 티켓 정보를 개시하여 상기 티켓 정보의 선택을 요구하는 티켓 신청 접수수단; 상기 입력된 개인 정보를 인증하는 인증수단; 상기 인증수단에 의한 인증후 상기 선택된 티켓 정보로 이루어진 전자티켓을 암호 데이터로 암호화하는 암호화 수단; 상기 암호 데이터로 암호화되는 전자티켓의 정보를 기억하는 전자티켓 기억수단; 및 상기 암호화수단에 있어서 암호화된 암호 데이터를 신청자의 컴퓨터 단말에 대해 컴퓨터 네트워크를 통해 송신하는 전자티켓 발행수단을 구비하는 것을 특징으로 하는 전자티켓 시스템.

s to the electronic ticket system which digitalizes th
ption with a computer and published; th
acco application means which dem
ands the input of the personal information of the tic
ket applicant from the computer terminal of the tick
et applicant through the computer network ; and it
discloses the ticket information which memorizes in
the ticket information storage means and demands t
he selection of the ticket information; the authentic
ation means authenticating the above-mentioned in
putted personal information; the e-ticket storage de
vice remembering the information of the encrypting
means: e-ticket encrypted by data encryption of enc
oding the e-ticket made of the selected ticket inform
ation after the authentication by the authentication
means to data encryption; and the e-ticket issuing
mean transmitting data encryption encrypted as to t
he encrypting means about the computer terminal o
f the applicant through the computer network.

청구 22항:

제 21 항에 있어서, 상기 전자 티켓을 상기 인증된 개인 정보와 상기 선택된 티켓 정보로 형성하는 것을 특징으로 하는 전자티켓 시스템.

Claim 22:

As for claim 21, the electronic ticket system forming the e-ticket into the above-mentioned authenticated personal information and selected ticket information.

청구 23항:

제 21 항 또는 제 22 항에 있어서, 상기 암호 데이터를 신청자의 컴퓨터 단말에 구비하는 기억 매체에 기억시키는 것을 특징으로 하는 전자티켓 시스템.

Claim 23:

As for claim 21 or 22, the electronic ticket system memorized in the storage media including data encryption in the computer terminal of the applicant.

청구 24항:

제 23 항에 있어서, 티켓을 인증하는 개찰 게이트에 있어서, 상기 기억매체에 기억된 암호 데이터를 인증하는 입장관리 단말로서, 상기 기억매체에 기억된 암호 데이터를 검지하는 암호 데이터 검지수단; 상기 암호 데이터 검지수단에 의해 검지된 암호 데이터의 정보와 상기 전자티켓 기억수단에 기억시킨 전자 티켓의 정보를 컴퓨터 네트워크를 통해 서버 컴퓨터와 교환함으로써 조합하는 조합수단; 및 상기 조합수단에 의한 조합을 기초로 개찰게이트의 개폐를 제어하는 개찰 게이트 제어수단을 구비하는 것을 특징으로 하는 전자티켓 시스템.

Claim 24:

As for claim 23, as the position management terminal authenticating the data encryption memorized as to the opening of the bids gate authenticating the ticket in the storage media, the electronic ticket system including the opening of the bids gate control means controlling opening and shutting of the opening of the bids gate based on the combination by the combination means which assembles by communicating the information of the e-ticket which memorizes in the information and e-ticket storage device of the data encryption detection means: data encryption detected with the data encryption detection means detects the data encryption memorized in the storage media through the computer network with the server computer and combination means.

청구 26항:

제 21 항 내지 제 25 항 중 어느 한 항에 있어서, 상기 신청자의 컴퓨터 단말을, 컴퓨터 네트워크를 통해 서버 컴퓨터로 암호 데이터를 수신하는 입출력 제어부; 상기 암호 데이터의 기억이 가능한 기억매체; 상기 기억매체에 기억된 암호 데이터를 해독하여 복호화하는 암호 통신 해독수단; 및 복호화된 암호 데이터의 정보를 표시하는 표시장치를 구비하는 휴대형 데이터 통신 단말로 하는 것을 특징으로 하는 전자티켓 시스템.

Claim 26:

As for any one of claim 21 through 25, the electronic ticket system which it is done by the hand-held data communication terminal equipped with the input/output control section receiving the data encryption the computer terminal of the applicant through the computer network to the server computer, the storage media, the cryptographic communication means of decoding, and the display device indicating the information of the decoded data encryption, and as to

the storage media, the memory of the data encryption key is used to decode the cryptographic communication. The receiver uses the same key to decode the data encryption method stored in the storage media and decoded.

청구 27항:

제 23 항 내지 제 25 항 중 어느 한 항에 있어서, 상기 기억매체를 상기 암호데이터의 기억이 가능한 IC칩 또는 IC카드로 하는 것을 특징으로 하는 전자티켓 시스템.

청구 28항:

제 24 항에 있어서, 상기 입장관리단말에 상기 조합수단에 의한 조합을 기초로 위법 통과를 알리는 경보장치를 구비하는 것을 특징으로 하는 전자티켓 시스템.

청구 29항:

제 24 항에 있어서, 상기 입장관리단말에 상기 티켓 정보에 기초하여 회장을 안내하기 위한 회장 안내 정보 출력부를 구비하는 것을 특징으로 하는 전자티켓 시스템.

Claim 27:

As for any one of claim 23 through 25, the IC chip in which the memory of the data encryption is the storage media possible or the electronic ticket system which it is done by the IC card.

Claim 28:

As for claim 24, the electronic ticket system equipped with the alarm informing the position management terminal of the illegality pass based on the combination by the combination means.

Claim 29:

As for claim 24, the electronic ticket system equipped with the president guidance information output part for guiding the president in the position management terminal based on the ticket information.

기술분야

본 발명은 기억매체를 이용하여 티켓의 구입 및 회장으로의 입장을 실시하는 전자티켓 시스템에 관한 것이다.

Technical Field

The present invention relates to the electronic ticket system performing the position to the purchase of the ticket and president using the storage media.

배경기술

종래, 예를 들면 아티스트등의 콘서트에 가는 경우 그 콘서트의 티켓 판매 센터에 해당 티켓의 예약을 전화등으로 신청하고, 티켓 판매 센터에서 발급된 티켓은 지정 기일까지 티켓 판매점에서 건넬받거나 티켓 판매 센터로부터 우송되어 입수했다. 또, 콘서트 회장에서서는 구입한 티켓을 회장의 게이트구에서 담당자에게 제시하여 반으로 자르고 나서 입장했다. 이와 같이 종래는 흥행 티켓의 구입, 그리고 회장으로의 입장은 그 흥행 내용이 기재된 종이 티켓을 통해 실시되었다. 종이 티켓으로의 티켓의 발행이나 회장으로의 입장 절차는 다수의 사람(담당자)을 필요로 한다. 따라서 최근 티켓의 발행 및 입장의 수속을 간소화하기 위해 전자티켓의 발행 및 그 전자티켓을 이용한 입장 시스템이 검토되고 있다.

총래, 티켓의 예약은 인터넷 접속 서비스의 기능을 갖고 있는 휴대전화기등에 의해 가능했지만 티켓의 구입은 할 수 없었다.

Background Art

The reservation of the correspondence ticket was applied for the convention, for example, concert including the artist etc. to case to the ticket selling center of the concert to the telephone etc. and the ticket is sued from the ticket selling center was handed to the designated date in the ticket selling point or it was mailed from the ticket selling center and it obtained. And in the concert stage, after the ticket bought was presented the person in charge in the gate orifice of the president and it cut with half it entered. In this way, the convention was performed through the paper ticket in which the entertainment industry content the position to the purchase of the entertainment industry ticket and president was written. The position procedure to the publication of the ticket to the paper ticket or the president requires multiple humans (the person in charge). Therefore, recently, the position system which uses the publication and e-ticket of the e-ticket in order to streamline the publication of the ticket and convergence of the position is reviewed.

The convention, and the reservation of the ticket were possible with the mobile phone etc. but having the function of the Internet access service the purchase of the ticket could not do.

상술한 휴대전화등으로의 티켓 예약은 해당 티켓의 예약

Bibliographic Abstract Drawing Claims Description

본 발명은 티켓의 권리정보의 기록이 가능한 기억매체를 구비한 데이터 통신이 가능한 데이터 통신 단말을 이용하여 티켓의 구입을 신청하고, 티켓 판매 센터가 티켓의 권리 정보를 송신하고, 그 티켓의 권리 정보를 상기 기억매체에 기록하고, 그 기억매체에 기록된 티켓의 권리정보는 게이트구에서 인증되어 회장에 입장할 수 있도록 하는 것으로 상기 과제를 해결하고 있다.

본 발명은 티켓의 권리정보의 기록이 가능한 기억매체를 구비한 데이터 통신이 가능한 데이터 통신 단말을 이용하여 티켓의 구입을 신청하고, 티켓 판매 센터가 티켓의 권리 정보를 송신하고, 그 티켓의 권리 정보를 상기 기억매체에 기록하고, 그 기억매체에 기록된 티켓의 권리정보는 게이트구에서 인증되어 회장에 입장할 수 있도록 하는 것으로 상기 과제를 해결하고 있다.

The ticket reservation including the mobile telephone reservation number of the corresponding ticket is received in the ticket distributor where in conclusion, the ticket was designated or it was identical with the convention in the point in which it became necessary to receive with the mailing.

The purchase of the ticket is asked for using the data communication terminal in which the data communications in which the invention includes the storage media in which the register of the rights information of the ticket is possible is possible and the ticket selling center transmits the rights information of the ticket and the rights information of the ticket is recorded in the storage media and with the rights information of the ticket recorded in the storage media is authenticated in the gate orifice and it enters the president the subject is solved.

상세설명

상기 목적을 달성하기 위해 본 발명은 컴퓨터시스템에 의해 티켓을 전자화하여 발행하는 전자 티켓 시스템으로서, 발행되는 티켓의 내용을 나타내는 티켓 정보를 기억하는 티켓 정보 기억수단과, 티켓 신청자에 대해 티켓 신청자의 개인 정보의 입력을 요구하는 한편, 상기 티켓 정보 기억수단에 기억시킨 티켓 정보를 개시하여 상기 티켓 정보의 선택을 요구하는 티켓 신청 접수수단과, 상기 입력된 개인 정보를 인증하는 인증수단과, 상기 인증수단에 의한 인증 후 상기 선택된 티켓 정보로 이루어진 전자티켓을 암호 데이터에 암호화하는 암호화수단과, 상기 암호화 수단에 있어서 암호화된 암호 데이터를 신청자에 대해 발행하는 전자 티켓 발행수단을 구비하도록 한 것이다.

제 2 발명은 서버 컴퓨터에 의해 티켓을 전자화하여 발행하는 전자 티켓 시스템에 있어서, 발행되는 티켓의 내용을 나타내는 티켓 정보를 기억하는 티켓 정보 기억수단과, 티켓 신청자의 컴퓨터 단말에 대해 컴퓨터 네트워크를 통해 티켓 신청자의 개인 정보의 입력을 요구하는 한편, 상기 티켓 정보 기억수단에 기억시킨 티켓 정보를 개시하여 상기 티켓 정보의 선택을 요구하는 티켓 신청 접수 수단과, 상기 입력된 개인 정보를 인증하는 인증 수단과, 상기 인증수단에 의한 인증 후 상기 선택된 티켓 정보로 이루어진 전자티켓을 암호 데이터로 암호화하는 암호화수단과, 상기 암호화 수단에 있어서 암호화된 암호 데이터를 신청자의 컴퓨터 단말에 대해 컴퓨터 네트워크를 통해 송신하는 전자 티켓 발행수단을 구비하도록 한 것이다.

Detailed Description

To accomplish the above objects, as for the encrypting means, digitalizing the ticket with the computer system and encodes the e-ticket consisting of the ticket information storage means, the ticket acceptance of application means demanding the input of the personal information of the ticket applicant from the ticket applicant and discloses the ticket information, the authentication means authenticating the above-mentioned inputted personal information, and the selected ticket information after the authentication by the authentication means in the data encryption and encrypting means of the invention, the electronic ticket issuer publishing the encrypted data encryption about the applicant is included. The ticket information storage means is the electronic ticket system published and memorizes the ticket information expressing the content of the ticket issuing. The ticket acceptance of application means demanding the input of the personal information of the ticket applicant from the ticket applicant and discloses the ticket information memorizes in the ticket information storage means and demands the selection of the ticket information.

The encrypting means encoding the e-ticket to data encryption, and the electronic ticket issuer transmitting data encryption encrypted as to the encrypting means about the computer terminal of the applicant through the computer network consisting of the ticket information storage means memorizing the ticket information expressing the content of the ticket issuing, the ticket acceptance of application means demanding the input of the personal information of the ticket applicant from the computer terminal of the ticket applicant through the computer network and of disclosing the ticket information memorized in the ticket information storage means and demanding the selection of the ticket information, the authentication means of authenticating the above-mentioned inputted personal information, and the selected ticket information.

제 3 발명은 서버 컴퓨터에 의해 티켓을 전자화하여 발행하는 전자 티켓 시스템에 있어서, 발행되는 티켓의 내용을 나타내는 티켓 정보를 기억하는 티켓 정보 기억수단과, 티켓 신청자의 컴퓨터 단말에 대해 컴퓨터 네트워크를 통해 티켓 신청자의 개인 정보의 입력을 요구하는 한편, 상기 티켓 정보 기억수단에 기억시킨 티켓 정보를 개시하여 상기 티켓정보의 선택을 요구하는 티켓 신청 접수수단과, 상기 입력된 개인 정보를 인증하는 인증수단과, 상기 인증수단에 의한 인증후 상기 선택된 티켓 정보로 이루어진 전자 티켓을 암호데이터로 암호화하는 암호화수단과, 상기 암호 데이터에 암호화되는 전자티켓의 정보를 기억하는 전자 티켓 기억수단과, 상기 암호화 수단에 있어서 암호화된 암호 데이터를 신청자의 컴퓨터 단말에 대해 컴퓨터 네트워크를 통해 송신하는 전자 티켓 발행수단을 구비하도록 한 것이다.

The encrypting means encoding the e-ticket to data encryption, the e-ticket storage device memorizing the information of the encrypted e-ticket in data encryption, and the electron ticket issuer transmitting data encryption encrypted as to the encrypting means about the computer terminal of the applicant through the computer network consisting of the ticket information storage means memorizing the ticket information expressing the content of the ticket issuing, the ticket acceptance of application means demanding the input of the personal information of the ticket applicant from the computer terminal of the ticket applicant through the computer network and discloses the ticket information, the authentication means authenticating the above-mentioned inputted personal information, and the selected ticket information after the authentication by the authentication means are included as to the electronic ticket system in which the third invention digitalizes the ticket with the server computer and published. The ticket acceptance of application means demanding the input of the personal information of the ticket applicant from the computer terminal of the ticket applicant through the computer network and discloses the ticket information memorizes in the ticket information storage means and demands the selection of the ticket information.

산업상 이용 가능성

이상과 같이, 본 발명에 따른 전자티켓 시스템에 의하면 신용정보인 티켓의 권리 정보 그 자체가 유통되고, 종이 티켓으로 주고 받는 것이 불필요해진다. 이 때문에 종래와 같이 티켓의 발행에 필요했던 일손은 불필요해진다. 또 티켓 용지에 이벤트 정보를 인쇄할 필요도 없어지고, 신속한 티켓의 발행이 가능해진다.

또, 본 발명에 따른 전자티켓 시스템에서는 IC칩과 같은 매립 가능한 기억매체에 티켓의 권리 정보를 기록하는 방식을 채택하기 때문에 휴대전화기 이외에도 IC칩의 매립이 가능한 매체나 부정형의 카드의 사용도 가능해지고, 사용자가 희망하는 매체로 티켓의 권리 정보를 소지할 수 있다.

또, 입장 관리 단말을 비접촉으로 통과할 수 있도록 기억 매체에 비접촉 IC칩을 사용하고, 회장을 안내하기 위한 회장 안내 표시판 또는 회장 안내 작성 프린터를 입장 관리 단말에 구비하는 것에 의해 입장이 원활하게 되어 게이트 구에서의 혼잡을 피하는 것이 가능해진다. 상기 개찰이나 회장 안내에 요하는 일손도 불필요해진다.

Industrial Availability

As described above, according to the electronic ticket system according to the present invention, the rights information itself of the ticket which is the credit information is circulated and it is unnecessary to give and take for the paper ticket. For this reason, the necessary help is unnecessary like the convention in the publication of the ticket. And the need to print the event information on the ticket paper is removed and the publication of the ticket which is quick becomes possible.

And in the electronic ticket system according to the present invention, the use of the card of the media or the irregular in which the padding of the IC chip is possible besides the mobile phone because it adopts the mode recording the rights information of the ticket in the storage media which can reclaim like the IC chip becomes possible and it can have the rights information of the ticket to the media which the user hopes.

And the noncontingence integrated circuit chip is used in the storage media in order to pass the position management terminal to the contactless and it becomes possible that the position is smooth and the congestion at the gate orifice is avoided by including the president introduction post or the president quid

line preparation printer for guiding the president in
option for a terminal. The help needed
the bids or the president inside
is unnecessary.

도면에 대한 간단한 설명

도 1은 본 발명에 따른 전자티켓 시스템의 블록도.

도 2는 본 발명에 따른 전자티켓 시스템에 의해 실행되는 티켓 발행 처리의 플로우차트의 일례,

도 3은 도 2의 티켓 발행 처리에 의한 휴대전화기의 디스플레이의 표시 화면.

도 4는 도 2의 플로우차트의 순서에 따라서 구입된 티켓의 권리정보가 기록된 상태의 IC칩을 나타내는 도면,

도 5는 도 2의 티켓 발행 처리에 의한 휴대전화기의 디스플레이의 표시 화면 및

도 6은 입장 관리 단말의 인증용 암호 데이터부에 기억되는 인증용 암호 데이터의 일례를 나타내는 도면이다.

Brief explanation of the drawing

Figure 1 is a block diagram of the electronic ticket system according to the invention

Figure 2 is an example of the flowchart of the ticket issue processing performed by the electronic ticket system according to the invention

Fig. 3 is the display screen of the display of the mobile phone by the ticket issue processing of 2.

Figure 4 is drawing showing the IC chip of the state where the rights information of the purchased ticket is recorded according to the order of the flowchart of fig. 2

With fig. 5 is the display screen of the display of the mobile phone by the ticket issue processing of fig. 2.

Figure 6 is drawing showing an example of the data encryption for the authentication being memorized in the cipher data part for the authentication of the position management terminal.

실시예

본 발명에 따른 전자티켓 시스템을 도면에 기초하여 설명한다. 도 1은 본 발명에 따른 전자티켓 시스템의 블록도이다.

도 1에 있어서, 도면부호 “10”은 티켓 구입을 희망하는 신청자가 소유하는 휴대형 데이터 통신 단말(컴퓨터 단말)인 휴대전화기, “12”는 신청자가 구입한 티켓에 관한 티켓의 권리 정보(전자티켓)를 발행(송신)하는 티켓 판매 센터인 서버(서버 컴퓨터), “14”는 회장의 입구에 설치되는 입장 관리 단말, “16”은 통신수단이 되는 인터넷이다.

상기 티켓의 권리 정보는 본원에 있어서의 「전자티켓」을 의미하는 것이다. 또, 상기 티켓의 권리 정보를 암호화한 것, 즉 「전자티켓」을 암호화한 것을 이하 「암호 데이터」라고 한다.

휴대전화기(10) 및 서버(12)는 이 인터넷(16)을 통해 접속되어 있으며, 서로 정보의 송수신이 가능한 환경에 있다. 또, 본인의 통신수단으로 이동형 휴대 전화 통신 사업자 회선, 네트워크 전용 회선등의 디지털 통신망등의 다른 컴퓨터 네트워크를 이용해도 좋다.

Example(s)

The electronic ticket system according to the present invention is illustrated based on drawing. Figure 1 is a block diagram of the electronic ticket system according to the invention.

The reference numeral "10" as to fig. 1 is the mobile phone which is the hand-held data communication terminal (computer terminal) which the applicant desiring the ticket purchase possesses, and "12" are the position management terminal in which the server (server computer) , and "14" which is the ticket selling center doing the rights information (E-ticket) of the ticket about the ticket which the applicant buys with the publication (transmission) are installed at the entrance of the president, and the internet in which in "16", the communication means is.

The rights information of the ticket means 「E-ticket」 in the present application. And it is hereinafter called 「data encryption」 encoding the , in other words, 「E-ticket」 encodes the rights information of the ticket.

The mobile phone (10) and server (12) are connected through this internet (16) and it is in the environment in which transmission and/or reception of the information are possible. And it may be acceptable that the digital communication network, including, the dissimilar computer network including mobile telephone communication common carrier the circuit, the network common carrier leased line etc. is used as the communication means of the present application.

Bibliographic Abstract Drawing Claims Description

양자간에서 주고 받는 전부 또는 그 일부의 정보로 구성되는 것이다. 예를 들면 신청자로부터의 주요 정보로서는 신청자의 ID넘버, 성명#183#성별#183#생년월일#183#현주소#183#연락처(휴대전화의 전화번호)#183#결제구좌 또는 크레디트의 번호 등 신청자의 특징이 가능한 개인 정보가 있다. 또, 상기 ID넘버는 상기 각종 개인정보가 입력된 후 해당 입력자(신청자)에 대해 서버(12)가 부여되는 식별번호이다.

서버(12)로부터의 정보로서는 흥행명#183#공연일#183#회장명#183#개연시간#183#좌석번호#183#티켓요금(티켓 구입 대금) 등 신청자가 구입한 티켓의 내용을 명확히 하는 이벤트 정보(티켓 정보)가 있다.

신청자 등으로부터의 정보나 서버(12)로부터의 정보는 이에 한정되지 않지만 적어도 이벤트 정보는 포함되어 있는 것으로 한다.

휴대전화기(10)는 티켓의 권리 정보를 수취하기 위한 단말(매체)이다. 티켓의 권리 정보는 상기 서버(12)에 있어서 암호화되며, 그 암호 데이터가 휴대전화기(10)에 대해 송신된다. 이 때문에 실제로는 휴대전화기(10)는 티켓의 권리 정보를 암호화한 암호 데이터를 수신하게 된다. 본 발명에서는 이 암호 데이터를 티켓의 주고 받는 수단으로 하고 있다.

휴대전화기(10)는 본기(本機)의 각부의 제어나 데이터의 처리를 도시하지 않은 프로그램에 따라서 실행하는 장치인 주 제어부(18)와, 입출력 데이터를 제어하는 입출력 제어부(20)와, 버튼 조작에 의해 데이터의 입력이 가능한 입력장치(22)와, 암호 데이터(23)의 내용을 표시하는 표시장치(디스플레이)(24)와, 암호 데이터(23) 등의 정보 데이터의 송수신을 실시하는 통신장치(26)와, 암호 데이터(23)의 기억매체(메모리)인 IC칩(28)과, 암호 데이터(23)를 해독하여 복호화하기 위한 암호 통신 해독수단(32)과, 상기 서버(12)의 홈페이지의 열람이 가능한 브라우저(34)를 구비한다. 이 휴대전화(10)는 인터넷(16)을 통해 서버(12)에 액세스할 수 있고, 상기 브라우저(34)에 의해 서버(12)가 제공하는 정보를 디스플레이(24)의 표시화면에 표시할 수 있다.

여기서 말하는 IC칩(28)은 통신수단에 의해 수신되는 암호 데이터(23)의 기억(기록)이 가능한 매체이다. 따라서 IC칩(28)에는 수신되는 정보 데이터의 기억, 즉 티켓의 권

partial information. For example, the ID number of the applicant, and the specific of the number-plate lamp applicant of the name · sex · date of birth · current state · address (the telephone number of the mobile telephone) · payment account or credit are possible as the critical information from the applicant. And it is the identification number in which the server (12) is given about the target input person (applicant) after the ID number all kinds of the personal information is inputted.

It has the event information (ticket information) making the content of the ticket which the applicant including the entertainment industry life · performance date · location name · raising of the curtain time · seat number · ticket charge (ticket purchase cost) etc. buys as the information from the server (12) clear.

It does that the information from the information or the server (12) including the applicant etc. is not thus restricted but at least event information is included.

It is the terminal (media) in which the mobile phone (10) receives the rights information of the ticket. The rights information of the ticket is encrypted as to the server (12) and the data encryption is transmitted about the mobile phone (10). For this reason, the mobile phone (10) receives the data encryption encoding the rights information of the ticket in fact. In the present invention, this data encryption is to the means of giving and taking of the ticket and the means has.

According to the program in which the mobile phone (10) does not show the processing of the control of each part of this or data, the main controller (18), the input/output control section (20) controlling input/output data, the input unit (22), the display device (display) (24) indicating the content of data encryption (23), the communication device (26) performing transmission and/or reception of information data including data encryption (23) etc, the IC chip (28), the cryptographic communication means of decoding (32) for decoding data encryption (23) and decoding, and the browser (34) are included. The main controller (18) is the apparatus for executing. As to the input unit (22), the input of data is possible with the button operation. The IC chip (28) is the storage media (memory) of data encryption (23). As to the browser (34), the browse of the home page of the server (12) is possible. This mobile telephone (10) can access in the server (12) through the internet (16) and the information which the server (12) provides can be indicated in the display screen of the display (24) with the browser (34).

Here, it is the media in which the memory (register) of the data encryption (23) in which the IC chip (28) referred is received with the communication means i

리 정보의 기록이 실시된다. 따라서 휴대전화기(10)는 암

Bibliographic Abstract Drawing Claims Description

3)의 판독 및 기록을 실시하기 위해 IC리더라이터(30)를 구비해도 좋다. 티켓의 신청자는 이 IC리더 라이터(30)를 통해 티켓의 권리 정보의 내용을 상기 표시장치(24)에 표시하고, 그 내용을 확인할 수 있다. 또, 상기 티켓의 이벤트 회장에서 담당자에게 그 내용을 제시할 수 있다.

도 1에서는 상기 IC칩(28)을 내장시키거나 또는 매립하는 매체를 휴대전화(10)로 하고 있지만, 다른 데이터 통신 단말을 사용해도 좋다. 예를 들면 인터넷(16)을 통해 서버(12)에 접속 가능한 PC, 전자수첩, 게임기, 편의점 등에 설치되는 컴퓨터 네트워크 전용 단말등을 이용하여 IC칩에 티켓의 권리 정보를 기록하고, 그 IC칩을 플라스틱 카드나 손목시계, 전자수첩에 매립해도 좋다. 또, 상기 예의 데이터 통신 단말에 IC리더라이터를 접속하고, IC카드 등에 티켓의 권리 정보를 기록해도 좋다.

서버(12)는 티켓의 신청에 대해 티켓의 권리 정보를 발행하고, 그 티켓의 권리 정보를 신청자의 IC칩(28)에 기록을 실시하는 것이다. 이 서버(12)는 신청자의 개인 정보의 입력이나 신청하는 티켓(티켓 정보)의 선택을 요구하고, 그 티켓 권리 정보를 신청자에게 발행(송신)하는, 티켓의 신청의 수리를 실시하는 티켓 신청 접수수단 및 티켓의 권리 정보의 발행을 실시하는 전자티켓 발행수단으로서의 접수 관리부(36)와, 티켓의 신청에 있어서 입력된 개인 정보를 인증하여 티켓의 권리 정보의 발행의 여부를 인증하는 인증수단으로서의 인증부(38)와, 티켓의 권리 정보의 발행이 인증된 상기 티켓의 권리 정보를 암호화하는 것을 가능하게 하는 암호화수단(40)과, 인증된 티켓의 권리정보(35)를 기억하는 전자티켓 기억수단으로서의 티켓용 데이터베이스(41)와, 티켓의 권리정보의 발행(판매)이 가능한 흥행의 정보(이벤트의 정보)(42)를 기억하는 티켓 정보 기억수단으로서의 이벤트용 데이터베이스(43)와, 서버(12)에 있어서 출입력되는 각종 정보의 처리의 실행을 제어하는 주 제어부(44)를 구비한다. 또, 신청자의 개인정보를 기억하는 개인 정보 기억수단으로서의 개인 정보용 데이터베이스(45)를 구비해도 좋다. 개인 정보용 데이터베이스(45)에는 본 발명의 전자 티켓 시스템을 이용하는 등록 회원의 개인 정보를 기억한다. 단, 본 발명의 전자티켓의 발행은 개인 정보의 입력이 있으면 가능하게 하는 것이며, 개인 정보용 데이터베이스(45)에 기억된 등록 회원만을 대상으로 하는 것이 아니다.

s possible. Therefore, in the IC chip (28), the memo information data, in other words, its information of the ticket is performed. Therefore, the storage media in which the applicant memorizing possesses the data encryption, in other words, the e-ticket becomes the mobile phone (10). And it may be acceptable that the IC reader writer (30) is included in order to perform the read of the data encryption (23) of the IC chip (28) and register. The applicant of the ticket indicates the content of the rights information of the ticket through this IC reader writer (30) in the display device (24) and the content can be confirmed. And in the event hall of the ticket, the content can be presented to the person in charge.

It may be acceptable that in fig. 1, the IC chip (28) is built or the media reclaiming is decided on to the mobile telephone (10). However the dissimilar data communication terminal is used. For example, it may be acceptable that the rights information of the ticket is recorded in the IC chip using the computer network special purpose terminal etc. and installed at PC, the electronic note, the game console, the convenience store etc which are connectable with the server (12) through the internet (16) the IC chip is reclaimed to the plastic card or the wrist watch, and the electronic note. And it may be acceptable that the IC reader writer is connected to data communication terminal of the example and the rights information of the ticket is recorded in the IC card etc.

The server (12) publishes the rights information of the ticket about the Petition of the ticket and the rights information of the ticket register is performed to the IC chip (28) of the applicant. This server (12) includes the ticket acceptance of application means which demands the selection of the input of the personal information of the applicant or the ticket (ticket information) applied and performs the repair of the Petition the ticket rights information to the applicant the publication (transmission) of the ticket and the database (43), for the event as the database (41), for the ticket as the authenticator (38), as the receipt administration unit (36), as the e-ticket issuing means performing the publication of the rights information of the ticket and the authentication means which authenticates acceptance and rejection of the publication of the rights information of the ticket it authenticates the personal information inputted as to the Petition of the ticket and the encrypting means (40), which makes it possible the rights information of the ticket in which the publication of the rights information of the ticket is authenticated is encoded and the e-ticket storage device memorizing the rights information (35) of the authenticated ticket and the ticket information storage means memorizing the information (the information of the event) (42) of the entertainment industry in which it is possible to the publication (sale) of the rights information of the ticket and the main controller (44) controlling the execution of the processing of the various information inputted

and outputted as to the server (12). And it may be possible to use the database (45) for the personal information of the individual information storage means memorizing the personal information of the applicant is included. In the database (45) for the personal information, the personal information of the registered member using the electronic ticket system of the invention is memorized. However, it makes it possible if the input of the personal information has the publication of the e-ticket of the invention and it does not do only the registered member memorized in the database (45) for the personal information.

티켓의 권리 정보 발행의 여부는 인증부(38)에서 판단된다. 인증부(38)는 티켓의 권리 정보를 판매해서 좋은지 여부를 판단한다. 예를 들면 인터넷(16)을 통해 액세스해온 자에 대해 "귀하에게는 티켓을 발행할 수 없습니다"등의 비매 통지를 배신(配信)한다. 개인 인증이라는 점에서 필요한 것이다. 또, 비매 통지와 함께 "티켓의 구입에는 IC 칩(또는 IC카드)의 구입 및 ID넘버의 취득이 필요합니다"등의 구입 절차의 안내 통지를 실시해도 좋다.

The ticket is necessary in that acceptance and rejection of the rights information publication of the ticket judge whether it is determined the rights information of the ticket the authenticator (38) sells in the authenticator (38) and it is good or not because it is vacant about the person has been access through for example, the internet (16) of "the ticket cannot be published to you" etc. the notification is betrayed it is the personal authentication. And it may be acceptable that the guideline notification of the purchase procedure including "in the purchase of the ticket, the purchase of the IC chip (or, the IC card) and captured of the ID number are necessary" etc. is performed with the notification because it is vacant.

또, 이 인증부(38)는 도시하지 않은 티켓 요금을 징수하는 결제기능을 구비하며, 티켓의 발행이 허가된 경우, 인증후 지불 계약이 있는 은행구좌, 크레디트카드 등에 의해 티켓 요금의 결제처리를 실시한다.

And the payment function collecting the ticket charge which this authenticator (38) does not show is included and in case the publication of the ticket is permitted the payment processing of the ticket charge is performed after the authentication with the bank account, in which it has the contract of payment the credit card etc.

인증된 티켓의 권리 정보(35)는 티켓용 데이터베이스(41)에 등록(기억)된다. 또, 상기 암호화수단(40)에 의해 암호화되고, 암호 데이터(23)로서 신청자들에게 발행(송신)된다.

It becomes the authenticated rights information (35) of the ticket in the database (41) for the ticket with the registration (memory). And it is encrypted with the encrypting means (40) and it becomes as the data encryption (23) to applicants with the publication (transmission).

발행(송신)된 암호데이터(23)는 상기 휴대전화기(10)의 IC칩(28)에 기억되고, 티켓의 권리정보(35)가 IC칩(28)에 기록된다. 또, 암호데이터(23)의 내용을 디스플레이(24)로 확인하는 경우는 IC칩(28)의 암호 데이터(23)를 암호 통신 해독수단(32)에 의해 해독하여, 디스플레이(24)에 표시할 수 있다. 암호 데이터(23)는 상기 암호 통신 해독수단(32)에 의해 해독이 가능하게 하고, 암호 해독수단(32)을 갖지 않은 자에게는 해독되지 않는다. 따라서, 비록 암호데이터(23)가 타인에게 잘못해서 송신된 경우라도 부정하게 사용되지 못한다.

The data encryption (23) which becomes with the publication (transmission) is memorized in the IC chip (28) of the mobile phone (10) and the rights information (35) of the ticket is recorded in the IC chip (28). And the case of confirming the content of the data encryption (23) as the display (24) decodes the data encryption (23) of the IC chip (28) with the cryptographic communication means of decoding (32) and it can indicate in the display (24). The data encryption (23) makes it possible with the cryptographic communication means of decoding (32) and it is not decoded to the person without the encryption translation means (32). Therefore, in case of the data encryption (23) doing wrong to the others and being transmitted it is unable to be foully used.

입장 관리 단말(14)은 티켓을 인증하는 개찰 게이트에 있어서 상기 휴대전화기(10)에 기억된 암호 데이터(23)를 인증하는 것으로 휴대전화기(10)의 IC칩(28)에 기록된

It is the apparatus in which the rights information of the ticket, which with authenticates data encryption (23) memorized as to the opening of the bids gate in which the position management terminal (14) aut

의 정보를 서버(12)의 티켓의 권리 정보(35)와 조합하는 the registration information of the database (41) for Bibliographic Abstract Drawing Claims Description to (12) and is authenticated en 또, 이 경우 서버(12)의 게이트용 데이터베이스(41)에 트 line circuit (59) is to the high speed communication 러블이 발생하면 인증이 불가능해지지만, 전술한 바와 같 circuits processing mutual massive data of the serve 이 입장자가 소지하는 휴대전화기(10)의 디스플레이(24) r (12) and position management terminal (14) at hi gh speed. The authentication at the position manag ement terminal (14) can be made quick by assembli ng the information of the bulk data encryption (23) of the position management terminal (14) through t 란은 피할 수 있다. his high speed communication circuits with the right

이상과 같이 본 발명에서는 티켓의 권리 정보(35)를 암호화한 암호 데이터(23)를 휴대전화(10)나 입장 관리 단말(14)에서 해독하게 된다. 따라서 본 발명에서는 적어도 IC칩(28)을 가진 데이터 통신 단말이 필요해진다. 그 데이터 통신단말 중에서도 휴대용 데이터 통신 이동 단말인 휴대전화기(10)(PHS를 포함)는 입력장치(키 버튼)(22)와 표시장치(디스플레이)(24) 및 통신장치(26)를 표준으로 갖기 때문에 이벤트의 정보(42)등의 표시, 데이터의 입력, 통신수단(16)으로의 접속이 가능한 매체로서 가장 유망한 것이다.

또, 휴대 가능한 데이터 통신 단말에 매립하는 기억매체에 비접촉 IC칩을 사용하면 비접촉으로 회장의 입퇴장이 가능해진다. 또, 티켓의 권리 정보의 기억매체로서 IC카드를 사용하는 경우는 비접촉형 IC카드를 사용하는 것에 의해 비접촉으로 입퇴장이 가능해진다.

계속해서 본 발명에 따른 전자티켓 시스템에 의해 실행되는 티켓의 권리 정보를 구입하는 경우의 처리 동작의 일례를 나타낸다. 도 2는 본 발명에 따른 전자티켓 시스템에 의해 실행되는 티켓 발행 처리의 플로우차트이다.

도 2에 나타내는 본 발명에 따른 전자티켓 시스템에 의해 실행되는 전자티켓 발행 처리의 플로우차트는 통신수단으로서 인터넷(16)을 사용하여, 서버(12)의 홈페이지상에서 티켓의 신청#183#발행의 절차를 실시하는 경우를 예로 채택한 것이다. 이 플로우차트는 휴대전화기(10)의 전원(58)을 온으로 하고, 휴대전화(10)의 디스플레이(24)

the registration information of the database (41) for the ticket of the server (12) and is authenticated encryption (12). It may be acceptable that the on-line circuit (59) is to the high speed communication circuits processing mutual massive data of the server (12) and position management terminal (14) at high speed. The authentication at the position management terminal (14) can be made quick by assembling the information of the bulk data encryption (23) of the position management terminal (14) through this high speed communication circuits with the right information (35) of the ticket of the server (12) and the authentication becomes possible to prevent the delay at the gate orifice. And in this case, the authentication is impossible if the trouble occurs in the database (41) for the gate of the server (12). However because the person in charge can authenticate by showing the information of data encryption (23) memorized in the IC chip (28) in the display (24) of the mobile phone (10) in which the attendance holds the disruption by the trouble of the database (41) for the ticket of the server (12) can avoid.

As described above, in the present invention, the data encryption (23) encoding the rights information (35) of the ticket is decoded in the mobile telephone (10) or the position management terminal (14). Therefore, in the present invention, the data communication terminal having at least IC chip (28) becomes necessary. Because the mobile phone (10) (the inclusion PHS) which is the portable data communications mobile terminal has the input unit (key button) (22), the display device (display) (24) and communication device (26) in the standard among the data communication terminal it is most promising as the media in which the display, the input of data, the connection to the communication means (16) including the information (42) of the event etc. is possible.

And if the noncontingence integrated circuit chip is used in the storage media reclaimed to the portable data communication terminal, entrance and exit of the president become possible to the contactless. And by the result of that the case of using the IC card as the storage media of the rights information of the ticket uses the non contact type IC card entrance and exit become possible to the contactless.

And then, an example of the process operation of the case of buying the rights information of the performed ticket is shown with the electronic ticket system according to the present invention. Figure 2 is a flowchart of the ticket issue processing performed by the electronic ticket system according to the invention.

For example, the flowchart of the e-ticket issue treatment performed by the electronic ticket system according to the present invention shown in fig. 2 adopts the case of performing the procedure of the Petition publication of the ticket on the home page of the server (12) as the communication means using the

또, 본 실시예에서는 도 1의 신청자의 개인 정보를 기억하는 개인 정보용 데이터베이스(45)를 구비하는 것으로 한다.

서버(12)의 홈페이지 화면중에 신청자의 ID넘버의 입력란이 나타난다(단계(S1)). 이 입력란에 자기의 ID넘버를 입력하면 계속해서 등록 완료된 개인 정보의 등록 내용이 표시된다(단계(S2)). 등록 내용에 상위 또는 변경이 없으면 이벤트용 데이터베이스(43)에 기억되어 있는 몇개의 이벤트의 정보(42)가 티켓 안내 정보로서 디스플레이(24)에 화면 표시된다(단계(S3)). 이 티켓 안내 정보로부터 희망하는 흥행, 예를 들면 "WorldCup2002 JAPAN-KOR EA 《결승》"의 표시 화면60(제 3 도)을 선택하고(단계(S4)), 계속해서 좌석, 예를 들면 "1F메인스탠드"를 지정한다(단계(S5)). 다음으로 희망하는 흥행 및 좌석을 확정한다(단계(S6)). 선택한 흥행을 변경한 경우는 단계(S3)의 처리로 복귀한다.

또, 단계(2)의 처리에 있어서 아직 개인 정보의 등록이 되어 있지 않은 경우는 입력란이 표시된다(단계(S7)). 또, 개인 정보에 변경이 있는 경우도 이 단계(7)에서 재입력을 할 수 있다. 입력후 단계(S3)이후의 처리가 실시된다.

신청을 받은 서버(12)(또는 접수 관리부(36))는 신청의 내용을 수신하고(단계(S8)), 인증부(38)에 조회한다(단계(S9)). 인증된 신청은 과금처리가 실시되고(단계(10)), 그 후 신청자의 ID넘버, 개인정보 및 이벤트 정보를 티켓의 권리 정보로서 티켓용 데이터베이스(41)에 등록(기억)한다(단계(S11)). 그 등록(기억)처리가 종료 후, 암호화수단에 의해 티켓용 데이터베이스(41)에 등록(기억)된 발행해야 하는 티켓의 권리 정보(35)를 암호 데이터(23)로 암호화하고(단계(S12)), 암호 데이터(23)는 신청자의 휴대전화(10)에 송신된다(단계(S13)). 수신된 암호 데이터(23)는 IC칩(28)에 기억되고, 4에 나타내는 티켓의 권리 정보(35)가 IC칩(28)에 기록된다(단계(S14)). 이에 의해 신청자에 의한 티켓의 구입이 완료된다. 또, 동시에 디스플레이(24)에 도 5에 나타내는 티켓의 내용이 표시된다(단계(S15)). 한편, 티켓 발행의 인증을 얻을 수 없었던 신청자에 대해서는 비매 통지를 송신한다(단계(16)).

the display (24) of the mobile telephone (10) if the only accesses in 「the display screen (60) box」 at the server (12) using the browser (34).

And in the present preferred embodiment, it does th at the database (45) for the personal information m emorizing the personal information of the applicant of fig. 1 is included.

If the input section of the ID number of the applicant shows up among the homepage screen of the server (12) (the step (S1)) the ID number of magnetism is input to this input section as many, the registration content of the personal information which and the registration is completed is indicated (the step (S2)) if it there is no high position or the change in the registration content, it is shown on screen in the display (24) (the step (S3)) the information (42) of the several events memorized in the database (43) for the event selects the desired entertainment industry, for example, the display screen 60 (third) of "the WorldCup2002 JAPAN-KOREA<< final game >>" as the ticket guiding information from this ticket guiding information and the case it and then designates the seat, for example, "1F main stand" (the step (S5)) of changing the desired entertainment industry next and the entertainment industry which it fixes the seat (the step (S6)) it choose (the step (S4))s returns to the processing of the step (S3).

And the unregistered in that case of the personal information the input section is yet indicated as to the processing of the step (2) (the step (S7)) even in case of the change being in and, the personal information it can re-input in the two-step (7). The processing of the step (S3) after is put into effect after the input.

The server (12) (or, the receipt administration unit (36)) which the Petition is received receives the content of the Petition (the step (S8)) and as to the Petition, which inquires to the authenticator (38) (the step (S9)) is authenticated accounting is performed (the step (10)) and it is the ID number of the applicant, and the personal information and event information at the database (41) for the ticket as the rights information of the ticket with the registration (memory) (the step (S11)) the registration (memory) processing thereafter encodes the rights information (35) of the ticket which becomes in the database (41) for the ticket with the registration (memory) and which it has to publish after the termination with the encrypting means to the data encryption (23) (the step (S12)) and the data encryption (23) which the data encryption (23) is transmitted to the mobile telephone (10) of the applicant (the step (S13)) is received is memorized in the IC chip (28) and the rights information (35) of the ticket shown in fig. 4 is recorded in the IC chip (28) (the step (S14)) the purchas

for the IC card. And the cost of the correspondence ticket is paid at the convenience store etc. and the e-ticket is issued by the purpose terminal as to the case of being the nonmember is installed by buying the IC card in which it is recorded only the event information the purchase of the ticket becomes possible.

상기 실시예에는 이벤트정보(홍행에 따른 티켓의 내용을 나타내는 것)를 전자화하는 전자 티켓 시스템이지만, 본 발명의 전자 티켓 시스템은 해당 이벤트 정보에만 이용되는 것은 아니다. 그외의 티켓, 예를 들면 승차권, 승선권, 식권, 보관증, 여권등에 따른 정보를 전자 티켓으로 발행해도 좋다. 즉, 본 발명의 전자 티켓 시스템은 종래 종이등을 매체로 하여 발행 판매되었던 모든 티켓에 관계된 「티켓 정보」에 대해 이용할 수 있는 것이다.

It is the electronic ticket system in which the embodiment digitalizes the event information (the content of the ticket according to the entertainment industry is expressed). However the electronic ticket system of the invention is not used to the correspondence event information. It may be acceptable that the other tickets, for example, the information according to the passenger ticket, the passage ticket, the meal-ticket, the deposit receipt, the passport etc is published to the e-ticket. That is, the electronic ticket system of the invention decides on the conventional paper etc. to the media and it can use about "the ticket information" connected to all tickets sold with publication.

Disclaimer

본 문서는 특허 및 과학기술문헌 전용의 첨단 자동번역 시스템을 이용해 생성되었습니다. 따라서 부분적으로 오역의 가능성이 있으며, 본 문서를 자격을 갖춘 전문 번역가에 의한 번역물을 대신하는 것으로 이용되어서는 안 됩니다. 시스템 및 네트워크의 특성때문에 발생한 오역과 부분 누락, 데이터의 불일치등에 대하여 본원은 법적인 책임을 지지 않습니다. 본 문서는 당사의 사전 동의 없이 권한이 없는 일반 대중을 위해 DB 및 시스템에 저장되어 재생, 복사, 배포될 수 없음을 알려드립니다.

(The document produced by using the high-tech machine translation system for the patent and science & technology literature. Therefore, the document can include the mistranslation, and it should not be used as a translation by a professional translator. We hold no legal liability for inconsistency of mistranslation, partial omission, and data generated by feature of system and network. We would like to inform you that the document cannot be regenerated, copied, and distributed by being stored in DB and system for unauthorized general public without our consent.)



Unexamined Patent Publication(A)

Bibliographic Data

Int.Cl.	G07C 9/00 H04W 12/06
Application No.	1020067025703
Application Date	20050513
Unexamined Publication No.	1020070012735
Unexamined Publication Date	20070126
Priority Claims	10/846,388 20040513 US
Agent.	C&S Patent and Law Office
Inventor	MARKHAM,ThomasR.
Applicant	HONEYWELL INTERNATIONAL INC.

발명의 명칭

무선 전화 인증 시스템

Title of Invention

AUTHENTICATING WIRELESS PHONE SYSTEM

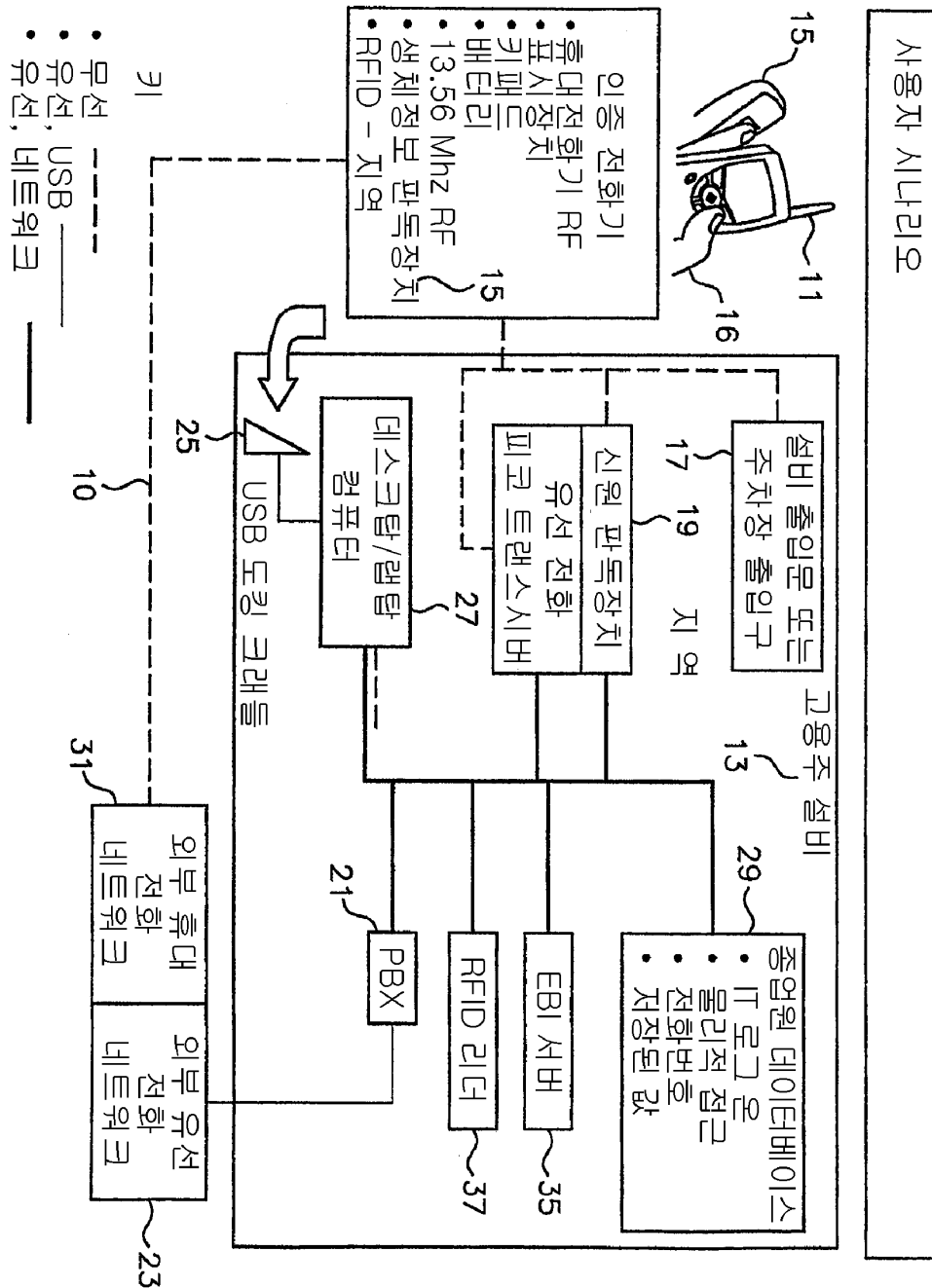
요약

무선 주파수 전송 능력, 배터리 전력 및 키패드를 갖는 휴대 전화기와 같은 인증 휴대 전자 장치를 제공한다. 상기 장치는 상기 장치의 사용자를 인증하기 위하여 상기 장치의 키패드에 인접하는 지문 판독 장치와, 상기 사용자의 신원을 판별하기 위해 원격 지역과 인증 신호를 통신하기 위하여 상기 장치 내의 트랜스시버를 포함하다. 또한, 상기 장치는 구조물 내의 유선 전화 시스템에 대한 연결을 갖는 트랜지서 리시버에 신호를 공급하기 위하여, 상기 장치를 사용하여 상기 수신기를 통해 상기 유선 전화 시스템으로 및 상기 유선 전화 시스템으로부터 통화를 허용하는 송신기를 포함한다. 상기 장치는, 상기 컴퓨터에 대한 접근을 허용하기 전에 상기 사용자를 인증하기 위하여, 컴퓨터에 연결되어 동작되는 도킹 크래들에 연결하기 위한 커넥터를 포함하며, 또한, 상기 커넥터는 배터리 충전 인터페이스일 수 있다.

Abstract

The authentication carried electronic device like the mobile phone having the wireless frequency transmission capability, and the battery power and keypad is provided. The apparatus comprises the fingerprint reader for being adjacent to the keypad of the apparatus it authenticates the user of the apparatus, the remote area the identity of the user is determined, and the transceiver of in the apparatus the authentication signal is communicated. Moreover, in order that the apparatus supplies the signal to the LAN branch office receiver having the connection about the wireline phone system within the structure the transmitter allowing call for the wireline phone system using the apparatus through the receiver from the wireline phone system is included. In order that the apparatus authenticates the user before giving a permission of the access about the computer the apparatus includes the connector for connecting to the docking cradle which is connected to the computer and is operated and moreover, the connector can be the battery charger interface.

대표도면(Representative drawing)



청구의 범위

청구 1항:

무선 주파수 전송 능력과, 배터리 전력 및 키패드를 구비한 인증 휴대 전자 장치에 있어서, 상기 장치의 사용자를 인증하기 위하여 상기 장치의 키패드에 인접한 지문 판독 장치; 사용자의 신원을 식별하기 위하여 원격 지역과 인증 신호를 통신하기 위한 상기 장치의 수신기 및 송신기; 구조물 내의 유선 전화 시스템에 대한 연결을 갖는 트랜스미트

Scope of Claims

Claim 1:

The authentication carried electronic device which comprises the wireless frequency transmission capability, the battery power, and the connector it receives the signal as to the authentication carried electronic device equipped with the keypad in the trans sheave which has the connection about the wireline phone

에 신호를 송신/수신하기 위하여, 상기 장치를 사용하여 상기 수신기를 통해 상기 유선 전화 시스템으로 및 상기 유선 전화 시스템으로부터 통화를 허용하는 송신기/수신기; 및 컴퓨터에 대한 접근을 허용하기 전에 상기 사용자를 인증하기 위하여 상기 컴퓨터에 연결되어 동작되는 도킹 크래들에 연결하기 위한 커넥터를 포함하는 인증 휴대 전자 장치.

청구 2항:

제1항에 있어서, 상기 휴대 전자 장치는, 휴대전화기인 것을 특징으로 하는 인증 휴대 전자 장치.

청구 3항:

제2항에 있어서, 상기 전화기는, 상기 지문 판독 장치가 상기 사용자의 신원을 확인할 때 상기 원격 지역에서 RF 질의와 통신하는 것을 특징으로 하는 인증 휴대 전자 장치.

청구 4항:

제3항에 있어서, 상기 원격 지역은, 출입문, 문 및 이동식 관문으로부터 선택되는 것을 특징으로 하는 인증 휴대 전자 장치.

청구 5항:

제3항에 있어서, 상기 장치는, 상기 원격 지역과의 상기 통신을 초기화하는 것을 특징으로 하는 인증 휴대 전자 장치.

청구 6항:

제3항에 있어서, 상기 원격 지역은, 상기 지문 판독 장치를 활성화하는 상기 장치와의 상기 통신을 초기화하는 것을 특징으로 하는 인증 휴대 전자 장치.

청구 7항:

제1항에 있어서, 상기 전자 장치는, 컴퓨터에 대한 접근을 허용하기 전에 상기 사용자를 인증하기 위하여 상기 컴퓨터에 연결되어 동작되는 도킹 크래들에 연결하기 위한 커넥터를 포함하는 것을 특징으로 하는 인증 휴대 전자 장치.

청구 8항:

제7항에 있어서, 상기 커넥터는, 배터리 충전 인터페이스인 것을 특징으로 하는 인증 휴대 전자 장치.

청구 9항:

system within the receiver of the fingerprint reader: apparatus for communicating the remote area and a authentication signal in order to distinguish the identity of the user, and transmitter adjacent to the keypad of the apparatus in order to authenticate the user of the apparatus, with the transmission / ; and for connecting to the docking cradle which is connected to the computer in order to authenticate the user before giving a permission of the access for the computer and the transmission/receiver allowing call for the wireline phone system using the apparatus through the receiver from the wireline phone system, and is operated.

Claim 2:

As for claim 1, the authentication carried electronic device in which the carried electronic device is the mobile phone.

Claim 3:

As for claim 2, the authentication carried electronic device in which the phone communicates through the remote area with the RF query when the fingerprint reader confirms the identity of the user.

Claim 4:

The authentication carried electronic device of claim 3, wherein the remote area is selected from the gate door, and the door and transportable gateway.

Claim 5:

As for claim 3, the authentication carried electronic device in which the apparatus initializes the communication of the remote area.

Claim 6:

As for claim 3, the authentication carried electronic device wherein the remote area initializes the communication with the apparatus that activates the fingerprint reader.

Claim 7:

As for claim 1, the authentication carried electronic device wherein the electronic device comprises the connector for connecting to the docking cradle that is connected to the computer and is operated for authenticating the user the access about the computer is given a permission of.

Claim 8:

As for claim 7, the authentication carried electronic device in which the connector is the battery charger interface.

Claim 9:

무선 주파수 전송 능력과, 배터리 전력 및 키패드를 구비한 인증 휴대 전자 장치에 있어서, 상기 장치의 사용자를 인증하기 위하여 상기 장치의 키패드에 인접한 지문 판독 수단; 사용자의 신원을 식별하기 위하여 원격 지역과 인증 신호를 통신하기 위한 상기 장치의 수신기 수단 및 송신기 수단; 구조물 내의 유선 전화 시스템에 대한 연결을 갖는 트랜스미브에 신호를 보내기 위하여, 상기 장치를 사용하여 상기 수신기를 통해 상기 유선 전화 시스템으로 및 상기 유선 전화 시스템으로부터 통화를 허용하는 트랜시미브 수단; 및 컴퓨터에 대한 접근을 허용하기 전에 상기 사용자를 인증하기 위하여 상기 컴퓨터에 연결되어 동작되는 도킹 크래들에 연결하기 위한 커넥터 수단을 포함하는 인증 휴대 전자 장치.

The authentication carried electronic device which comprises the wireless frequency transmission capability, the battery power, and the sheave means: of all owing call for the wireline phone system using the apparatus through the receiver from the wireline phone system it sends the signal to the trans sheave which has the connection about the wireline phone system within the receiver means of the fingerprint reading means: apparatus for communicating the remote area and authentication signal it distinguishes the identity of the user and transmitter method adjacent to the keypad of the apparatus it authenticates the user of the apparatus as to the authentication carried electronic device equipped with the keypad in *** and the connector means for connecting to the docking cradle which is connected to the computer in order to authenticate the user before giving a permission of the access about the computer and is operated.

청구 10항:

제9항에 있어서, 상기 휴대 전자 장치는, 휴대전화기인 것을 특징으로 하는 인증 휴대 전자 장치.

Claim 10:

As for claim 9, the authentication carried electronic device in which the carried electronic device is the mobile phone.

청구 11항:

제10항에 있어서, 상기 전화기는, 상기 지문 판독 장치가 상기 사용자의 신원을 확인할 때 상기 원격 지역에서 RF 질의와 통신하는 것을 특징으로 하는 인증 휴대 전자 장치.

Claim 11:

As for claim 10, the authentication carried electronic device in which the phone communicates through the remote area with the RF query when the fingerprint reader confirms the identity of the user.

청구 12항:

제11항에 있어서, 상기 원격 지역은, 출입문, 문 및 이동식 관문으로부터 선택되는 것을 특징으로 하는 인증 휴대 전자 장치.

Claim 12:

The authentication carried electronic device of claim 11, wherein the remote area is selected from the gate door, and the door and transportable gateway.

청구 13항:

제11항에 있어서, 상기 장치는, 상기 원격 지역과의 상기 통신을 초기화하는 것을 특징으로 하는 인증 휴대 전자 장치.

Claim 13:

As for claim 11, the authentication carried electronic device in which the apparatus initializes the communication of the remote area.

청구 14항:

제11항에 있어서, 상기 원격 지역은, 상기 지문 판독 장치의 활성화하는 상기 장치와의 상기 통신을 초기화하는 것을 특징으로 하는 인증 휴대 전자 장치.

Claim 14:

As for claim 11, the authentication carried electronic device which the remote area initializes the communication with the apparatus for activating of the fingerprint reader.

청구 15항:

제9항에 있어서, 상기 전자 장치는, 컴퓨터에 대한 접근을 허용하기 전에 상기 사용자를 인증하기 위하여 상기 컴퓨터에 연결되어 동작되는 도킹 크래들에 연결하기 위한 커넥터를 포함하는 것을 특징으로 하는 인증 휴대 전자 장치.

Claim 15:

As for claim 9, the authentication carried electronic device wherein the electronic device comprises the connector for connecting to the docking cradle that is connected to the computer and is operated for authenticating the user the access about the computer is given a permission of.

청구 16항:

Claim 16:

제15항에 있어서, 상기 커넥터는, 배터리 충전 인터페이스인 것을 특징으로 하는 인증 휴대 전자 장치.

As for claim 15, the authentication carried electronic device in which the connector is the battery charger interface.

청구 17항:

설비에서의 인증 및 통신 시스템에 있어서, 무선 주파수 전송 능력과 상기 설비에 접근하는 직원 및 상기 설비 내의 자산에 관련된 데이터를 저장하는 데이터베이스와, 유선 전화 시스템을 갖는 설비 IT 시스템; 및 무선 주파수 전송 능력, 배터리 및 키보드를 갖는 인증 휴대 전자 장치를 포함하며, 상기 전자 장치는, 상기 장치의 사용자를 인증하기 위하여 상기 장치의 키패드에 인접한 지문 판독 장치; 사용자의 신원을 식별하기 위하여 원격 지역과 인증 신호를 통신하기 위한 상기 장치의 트랜스리시버; 구조물 내의 유선 전화 시스템에 대한 연결을 갖는 트랜스시버에 신호를 보내기 위하여, 상기 장치를 사용하여 상기 수신기를 통해 상기 유선 전화 시스템으로 및 상기 유선 전화 시스템으로부터 통화를 허용하는 트랜스시버; 및 컴퓨터에 대한 접근을 허용하기 전에 상기 사용자를 인증하기 위하여 상기 컴퓨터에 연결되어 동작되는 도킹 크래들에 연결하기 위한 커넥터를 포함하는 인증 및 통신 시스템.

Claim 17:

The authentication and communication system which comprises the database department storing data related to the assets within the staff approaching the wireless frequency transmission capability and facility as to the authentication at the facility and communication system and facility, the facility IT system having the wireline phone system, and the connector it includes the wireless frequency transmission capability, and the authentication carried electronic device for having the battery and keyboard ; it sends the signal to the transceiver which has the connection about the wireline phone system within the transceiver: of the fingerprint reader: apparatus for communicating the remote area and authentication signal in order to distinguish the identity of the user adjacent to the keypad of the apparatus so that the electronic device authenticates the user of the apparatus ; and for connecting to the docking cradle which is connected to the computer in order to authenticate the user before giving a permission of the access for the computer and the transceiver allowing call for the wireline phone system using the apparatus through the receiver from the wireline phone system and is operated.

청구 18항:

제17항에 있어서, 상기 휴대 전자 장치는, 휴대전화기인 것을 특징으로 하는 인증 및 통신 시스템.

Claim 18:

As for claim 17, the authentication and the communication system in which the carried electronic device is the mobile phone.

청구 19항:

제18항에 있어서, 상기 전화기는, 상기 지문 판독 장치와 상기 사용자의 신원을 확인할 때 상기 원격 지역에서 RF 질의와 통신하는 것을 특징으로 하는 인증 및 통신 시스템.

Claim 19:

As for claim 18, the authentication and the communication system in which the phone communicates through the remote area with the RF query when the fingerprint reader confirms the identity of the user.

청구 20항:

제19항에 있어서, 상기 원격 지역은, 출입문, 문 및 이동식 관문으로부터 선택되는 것을 특징으로 하는 인증 및 통신 시스템.

Claim 20:

The authentication and communication system of claim 19, wherein the remote area are selected from the gate door, and the door and transportable gateway.

청구 21항:

제19항에 있어서, 상기 장치는, 상기 원격 지역과의 상기 통신을 초기화하는 것을 특징으로 하는 인증 및 통신 시스템.

Claim 21:

As for claim 19, the authentication and the communication system in which the apparatus initializes the communication of the remote area.

청구 22항:

제19항에 있어서, 상기 원격 지역은, 상기 지문 판독 장치의 활성화하는 상기 장치와의 상기 통신을 초기화하는 것을 특징으로 하는 인증 및 통신 시스템,

Claim 22:

As for claim 19, the authentication and the communication system which the remote area initializes the communication with the apparatus for activating of the fingerprint reader.

청구 23항:

제17항에 있어서, 상기 전자 장치는, 컴퓨터에 대한 접근을 허용하기 전에 상기 사용자를 인증하기 위하여 상기 컴퓨터에 연결되어 동작되는 도킹 크래들에 연결하기 위한 커넥터를 포함하는 것을 특징으로 하는 인증 및 통신 시스템.

청구 24항:

제23항에 있어서, 상기 커넥터는, 배터리 충전 인터페이스인 것을 특징으로 하는 인증 휴대 전자 장치.

기술분야

본 발명은 일반적으로 무선 전화 보안에 관한 것으로, 더욱 상세하게는, 무선 전화의 다양한 사용을 인증하는 시스템에 관한 것이다.

배경기술

휴대 전화기 또는 무선 전화기는 지난 몇 년 동안 광범위하게 발전하여 휴대 전화가 전통적인 유선 전화기를 대체하도록 위협하고 있다. 이러한 전화기는, 인터넷 연결, 비디오 전송, 게임, 벨소리, 지문 인증, 달력과 계산기, 문자 메시지, 수신자 번호 식별 등과 같은 많은 기능들을 가진다. 또한, 무선 전화기도 일하는 날의 작업을 위하여 사무 또는 기술 직원에 의하여 사용되고 있다.

동시에, 상업, 정부 또는 군사 기관들의 보안에 대한 열려가 증가하고 있으며, 컴퓨터, 신원 판독 장치(badge reader) 및 기타 신원 관리/접근 제어 시스템에 사용자를 인증하기 위한 모종의 수단을 필요로 한다. 현재 사용자는 인증을 위하여 여러 가지 장치와 기술을 가지고 있다. 고용주는 다중시스템을 유지하여야 한다. 이것은 비용이 많이 들고, 불편하며, 오류가 빈번할 수 있다.

상업, 정부 및 군사 조직은 다른 기능들과 함께 복수의 인증 방법을 필요로 하며, 2 이상의 데이터베이스 시스템이 필요하나, 복수의 데이터 시스템은 고가이며, 중복적이며, 완전성을 위한 일치가 항상 되는 것은 아니다. 다중 시스템이 하나로 결합될 수 있다면, 이러한 속성의 작업에 있어서 다른 이점이 증가한다.

모두가 아니더라도, 대부분의 휴대전화 및 PDA가 소비자
 품목으로 설계되며, 조직의 인프라 구조에는 잘 통합되지

Claim 23:

As for claim 17, the authentication and communication system wherein the electronic device comprises the connector for connecting to the docking cradle that is connected to the computer and is operated for authenticating the user the access about the computer is given a permission of.

Claim 24:

As for claim 23, the authentication carried electronic device in which the connector is the battery charger interface.

Technical Field

The present invention relates to generally, the cordless phone security, more particularly, to the system authenticating the various use of the cordless phone.

Background Art

In order to the mobile phone or the wireless mobile phone extensively develop for the past several years and the wired telephone in which the mobile telephone is traditional is replaced it intimidates. Such phone has the internet connection, the video transmission, the game, the ring tone, the fingerprint authentication, the calendar and the calculator, the text message, and many functions like the called party number identification light. Moreover, it is used for the operation of the day in which the wireless mobile phone works by the deskwork or the engineer staff.

Simultaneously, commerce, and the concern about the security of positive and negative or the military agencies increase and the means of the seed for authenticating the user in the computer, and the identity reading wand (badge reader) and the other identity administration / system of access controlling is required. The current user has many device for the authentication and technology. The employer has to maintain the multiple system. It as to the this, very much requires cost and the this, is inconvenient and the error can be frequent.

Commerce, and positive and negative and military organization require multiple authentication methods with dissimilar functions and the database system more than 2 is needed. But multiple data systems are the high price and it is duplicate and it does not become always the coincidence for integrity. If the multiple system can be combined to one, the dissimilarity advantage increases as to the operation of such a attribute.

It is not everyone. And yet the most of mobile telephones and PDA are designed to the consumer item a

r interface like USB connection about the computer or the dissimilar electronic device.

도면에 대한 간단한 설명

본 발명의 더 완전한 이해를 위해서, 다음의 도면을 참조한다.

도 1은 본 발명의 장치 및 시스템에 대한 구조를 도시한 블록도이다.

Brief explanation of the drawing

The following drawing is referred to for the complete understanding of the invention.

Figure 1 is a block diagram showing the structure about the apparatus and the system of the present invention.

실시예

도면을 참조하면, 일반적으로, 시스템(10)은 고용주 설비(13)와 같은 지역과 상호 작용하는 휴대 전화기(11)와 같은 인증 휴대 전자 장치(authenticating portable electronic device)를 포함한다. 바람직한 휴대 전자 장치는 휴대 전화기(11)이지만, 무선통신기, PDA 및 이와 유사한 것과 같은 신호를 송수신할 수 있는 휴대용 장치일 수 있다. 도면에 도시된 인증 전화기(11)는 일반적인 무선 주파수 휴대 전화기이며, 표시화면(display), 키패드, 배터리 및 상기 배터리를 충전하기 위한 연결부를 구비한다. 전화기(11)는 일반적으로 사용되는 휴대 전화 주파수에서 동작하며, 스마트 카드를 에뮬레이트(emulate)하기 위한 13.56Mhz 인터페이스를 포함한다.

고용주 설비(13)는 종업원의 출입과 재산정보, PC와 랩톱 및 이와 유사한 것과 같은 자산 관리에 관해서 보안의 필요성이 있는 전형적인 회사 건물로 도시된다. 설비(13)는 제한이 없으며, 창고, 정부 건물, 군사 시설 또는 기지, 공항, 학교, 은행 또는 기타 금융 기관, 또는 특정 직원에게 접근이 제한되는 설비가 될 수 있다.

일반적으로, 본 발명의 제1 실시는 한 사람이 상기 설비에 접근을 시도할 때 있을 수 있다. 사용자가 블록(17)으로 개념적으로 도시된 출입문(gate)에 접근하면, 상기 게이트와 상기 전화기(11)는 RF 신호를 통해 서로를 검출한다. 사용자가 손가락을 지문 판독장치에 대고 생체 정보 인증을 제공한다. 전화기는 상기 전화기(11)가 인식할 수 있도록 프로그램된 정확한 사용자를 수락하거나 검증한다. 상기 전화기(11)는 무선 링크를 통해 암호화되고 서명된 인증서를 출입문(11)과 교환한다. 전화기는 상기 서명된 인증서를 송신하거나 수신할 수 있으며, 이와 반대로 상기 출입문(17)이 상기 신호를 송신하거나 수신할 수 있다는 것에 유의해야만 한다. 이 지점에서, 출입문은 자동차 또는 사용자가 접근함에 따라 열린다.

Example(s)

Referring to the figure, generally, the system (10) includes the authentication carried electronic device (authenticating portable electronic device) like the mobile phone (11) interacting with the region, such as the employer facility (13). The carried electronic device done with desirable is the mobile phone (11). However it can be the handheld device sending and can receive the signal like being similar to the radio pager, and PDA to this. The authentication phone (11) shown in drawing comprises the display screen it is the general radio frequency mobile phone, the keypad, and the battery, and the connection part for charging the battery with electricity. It operates in the mobile telephone frequency in which the phone (11) is generally used and 13.56Mhz interface which is for the smart card with the emulate (emulate) the following is included.

Is illustrated to the typical company building in which it has the necessity of security about the asset management in which the employer facility (13) is similar to the access and information on assets of the employee, and PC and laptop to this. There the limit is no facility (13) and it can become the facility in which the access is controlled to the warehouse, the governmental building, and the military equipment or the base, airport, school, bank or the other financial facilities or the specific staff.

Generally, the access can have the first operation of the invention when one human tries to the access in the facility. If the user approaches the gate door (gate) conceptually illustrated to the block (17) gate and phone (11) detect through the radio frequency signal. The user touches finger to the fingerprint reader and the bio-information authentication is provided. The phone agrees to the exact user who is programmed so that the phone (11) recognizes or it verifies. The phone (11) exchanges the certificate which is encrypted through the radio link and is signed with the gate door (11). The phone transmits the above-mentioned signed certificate or the phone can receive and it has to take care about about. That it transmits the signal or on the contrary, the gate door (17) can receive. In this spot, the gate door is opened as the vehicle or the user approaches.

일반적인 시나리오에서, 사용자는 자동차를 주차한 후, 설비의 정문에 접근한다. 인증 전화기(11)와 블록(19)의 신원 판독 장치는 서로 감지한다. 다시, 사용자는 필요한 생체 정보를 공급하고, 상기 신원 판독 장치(19)는 문을 연다. 또한, 상기 신원 판독 장치(19)는 중앙원 데이터베이스에 시간 및 출근 정보를 보낼 수 있다.

In the general scenario, after the user resides the car the car approaches the fontanel of the facility. The identity reading wand of the block (19) and authentication phone (11) senses. Again, the bio-information in which the user is necessary is supplied and the identity reading wand (19) opens. Moreover, the identity reading wand (19) can send time and attendance information to the employee database.

일반적으로, 사용자는 홀(hall)로 걸어 가며, 이동 중에 통화를 걸 수 있다. 이 통화는 블럭(19)에 함께 있는 로컬 휴대 전화가 피코 트랜스시버(cell phone pico transceiver)와, PBX(21)를 통해 블럭(23)에 도시된 유선 전화 시스템에 연결된다.

Generally, the user walks to the hole (hall) and call can be set up among the movement. It is connected to the wireline phone system shown in the block (2 3) through the local mobile phone pico transceiver (cell phone pico transceiver), in which this call is together in the block (19) and PBX (21).

상기 통화는 PBX(21)에 의해 처리되기 때문에, 설비 정책에 따라, 상기 사용자는 상기 통화에 대해서는 과금되지 않을 수 있다. 사용자는 책상에 유선 전화를 더 이상 가지지 않을 수 있다.

Call is processed by the PBX (21). Therefore the user is not charged according to the facility policy about call. The user any more does not have the wire telephone on desk.

사용자가 작업이다 다른 활동이 일어나는 책상에 도착하여, 블럭(27)에 도시된 데스크 탑 또는 랩탑 컴퓨터에 연결되는, USB 도킹 크래들과 같은 크래들(25)에 전화기(11)를 삽입한다. 컴퓨터는 일반적인 워크 스테이션의 예로서 블럭(27)에 도시되지만, 전자 부품을 갖는 전자 장치 또는 기타 장치가 사용될 수 있다. 예로써, 블럭(27)은 기계 색층 분석기, x선 기기 또는 군사 또는 정부 장비, 또는 기타 다른 장치와 같은 기기를 포함한다. 전화기(11)가 크래들(25)에 삽입되면, 사용자는 생체 정보 또는 지문을 제공하며, 상기 휴대 전화기(11)는 상기 사용자에 대한 자동 로그인을 수행한다. 이것은 활성 디렉토리와 같은 종업원 데이터베이스(29)를 포함하거나, 상기 컴퓨터(27)와 전화기(11) 사이에만 지역적으로 수행될 수 있다. 전화기는 장치(PC, 사원 판독 장치, 등)에 사용자 지문 데이터를 선택적으로 통과시켜, 상기 장치가 상기 지문에 대한 검증을 수행하게 할 수 있다. 또한, 상기 크래들(25)은 사용자의 말력에 PDA 기능을 직접 동기시킬 수 있다. 또한, 전화기(11)의 배터리를 충전할 수 있다.

It arrives the desk in which the activity the user is the operation dissimilar occurs and the phone (11) is inserted into the cradle (25) connected to the laptop computer such as the desktop shown in the block (27) and USB docking cradle. The computer is for example illustrated of the general work station in the block (27). However the electronic device or the etc apparatus for having the electronic component can be used. The block (27) with the example includes the instrument, such as the apparatus which the gas chromatography, and the X-ray instrument or the military affairs or positive and negative equipment or the other is different. If the phone (11) is inserted into the cradle (25), the user serves the bio-information or the fingerprint and the mobile phone (11) performs the auto login about the user. This includes the employee database (29) like the activity directory or this can be performed between the computer (27) and phone (11). The phone selectively passes user fingerprint data through in the apparatus (PC, the identity reading wand, etc) and the verification about the fingerprint can be allowed the apparatus to perform. Moreover, the directly the cradle (25) can synchronize the PDA function in the calendar of the user. Moreover, the battery of the phone (11) can be charged with electricity.

사용자는 설비(13)를 떠날 수 있으며, 전화 통화를 거는 것이 필요할 수 있다. 인증 휴대 전화기(11)는 블럭(31)에 도시된 외부 휴대 전화기 네트워크에 연결되며, 상기 통화는 일반적인 휴대 전화기 통화와 같이 일어날 수 있다. 상기 통화는 종업원 또는 사용자가 등록한 휴대 전화 공급자를 통해 과금/청구된다.

The user can leave the facility (13) and it can be necessary to speak the telephone call. It is connected to the outside mobile phone network in which the authentication mobile phone (11) is illustrated in the block (31) and call can occur like the general mobile phone call. Call is claimed through the mobile telephone supplier whom the employee or the user registers with the charging /.

어떤 조직들은, 보안, 접근 제어 및 건물 제어를 포함하는 허니웰 엔터프라이즈 건물 통합 인증자로 알려진 것과 같은 건물 통합 시스템으로 알려진 것을 가진다. 그러한 시스템과 더불어 본 발명을 실시하는 것은, 예를 들어, 전술한 전자 스위치 판독 장치로 경비실에 있는 경비원을 대체하

Any kind of organizations has the thing known as the building integrated system like being considered as the honeywell enterprise building integrated authorization person including security, the access control, and the building control. It is according to replace

는 것에 의하여 많은 비용의 절감을 제공한다. 본 발명은 IT 시스템 관리로 물리적인 건물 제어의 통합을 가능하게 하며, 본 발명은 건물의 PBX를 무선 전화 시스템과 통합한다. 이것은 EBI 데이터 베이스와 IT 데이터 베이스를 필요로 하는 것과 같은 중복된 노력을 방지하고, 오류나 혼란 또는 새로운 데이터의 관점에서 한 데이터베이스를 다른 데이터베이스에 업데이트할 필요성을 제거한다.

the guard who is in the guardroom with for example, the above-described electronic identity reading wand and many cost reduction is provided to perform the invention with that system. It makes the integration of the building control which is physical to the IT system management the invention possible and the invention integrates PBX of the building with the wireless phone system. The effort of being overlapped which need this is the EBI database and IT database are prevented and the necessity to update one database in the viewpoint of the error or the disruption or new data in the dissimilar database is removed.

본 발명의 특정 실시예가 도시되고 설명되었지만, 단순한 예시에 불과하며, 본 발명의 기술분야에서 통상의 지식을 가진 자는 본 발명의 사상과 범위를 벗어나지 않고서 본 명세서에 설명된 실시예에 대하여 변형 및 수정을 가할 수 있다. 그러한 모든 균등한 변형과 수정은 본 발명의 범위 내에 포함되도록 의도되었으며, 첨부된 청구범위에 정의된 것과 같이 본 발명을 한정하도록 의도된 것을 아니다.

The certain embodiment of the invention was illustrated and it was explained. However it is nothing but the simple example and after a person skilled in the art does not deviate from thought and range of the present invention from the technical field of the invention deformation and correction can be added toward the embodiment explained in this specification. It was intended so that deformation and the correction which was equal with that all were included within the scope of the present invention and it is not being intended in order to limit the invention as been defined in the attached claims.

Disclaimer

본 문서는 특허 및 과학기술문헌 전용의 첨단 자동번역 시스템을 이용해 생성되었습니다. 따라서 부분적으로 오역의 가능성이 있으며, 본 문서를 자격을 갖춘 전문 번역가에 의한 번역물을 대신하는 것으로 이용되어서는 안 됩니다. 시스템 및 네트워크의 특성때문에 발생한 오역과 부분 누락, 데이터의 불일치등에 대하여 본원은 법적인 책임을 지지 않습니다. 본 문서는 당사의 사전 동의 없이 권한이 없는 일반 대중을 위해 DB 및 시스템에 저장되어 재생, 복사, 배포될 수 없음을 알려드립니다.

(The document produced by using the high-tech machine translation system for the patent and science & technology literature. Therefore, the document can include the mistranslation, and it should not be used as a translation by a professional translator. We hold no legal liability for inconsistency of mistranslation, partial omission, and data generated by feature of system and network. We would like to inform you that the document cannot be regenerated, copied, and distributed by being stored in DB and system for unauthorized general public without our consent.)



Unexamined Patent Publication(A)

Bibliographic Data

Int.Cl.	G06F 17/00 G06F 21/20
Application No.	1020000031371
Application Date	RT-Trans Word-Search Copy-to-clip Error-report
Unexamined Publication No.	1020010111403
Unexamined Publication Date	20011219
Requested Date of Examination	20000608
Agent.	LEE, Byong Ho
Inventor	OH, SangGyoon
Applicant	BURUSO INTERNATIONAL CO., LTD.

발명의 명칭

인증서를 이용하여 이용자의 인터넷 서비스 액세스 및 인터넷 서비스 이용 범위를 제어하는 방법

Title of Invention

The method for controlling internet service access and the range of use of internet service of user by utilizing certificates

요약

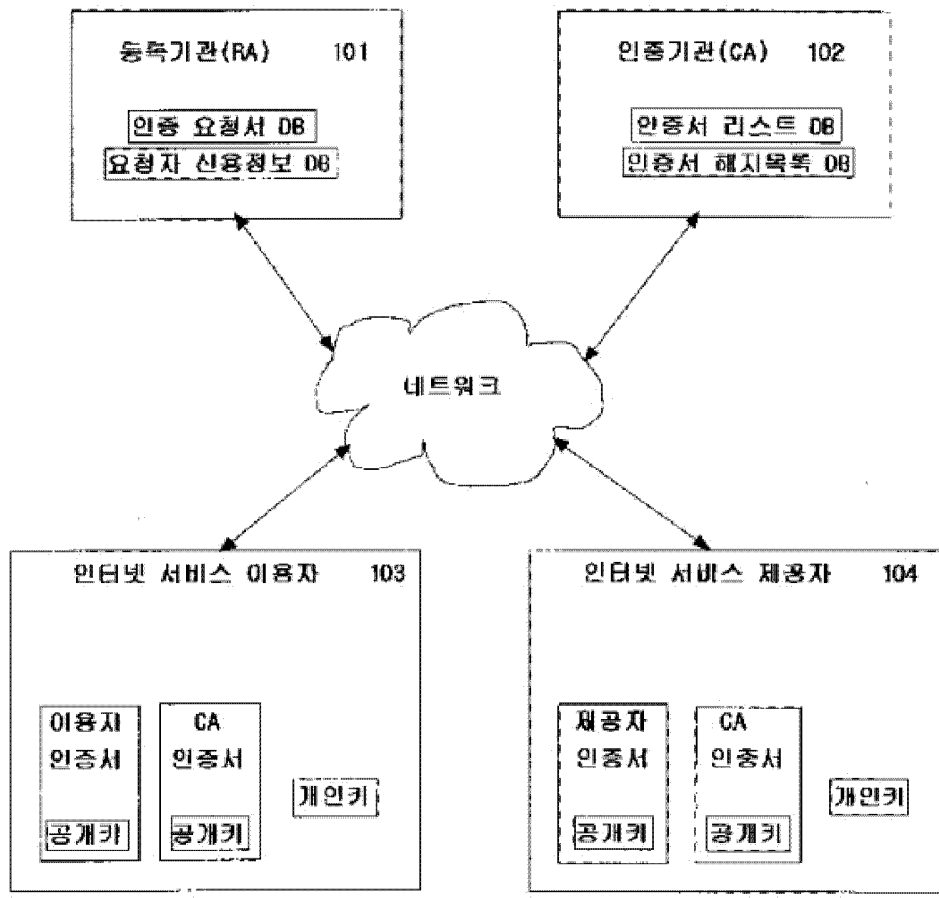
본 발명은 인증서를 이용하여 인터넷 서비스 액세스 로그인 및 인터넷 서비스 이용자의 서비스 이용 범위를 제어할 수 있도록 하는 방법에 관한 것이다. 인증서 제출을 의미하는 클릭 절차에 의해 인터넷 서비스 이용자로부터 인증이 요청되면, 인터넷 서비스 제공자가 이용자로부터 제출된 인증서를 판독하여 인터넷 서비스 로그인을 통제할 수 있고, 또한 인증서에 포함된 서비스 이용범위를 나타내는 정보를 판독하여 인터넷 서비스 이용자의 등급별 서비스 액세스 로그인을 통제할 수 있도록, 인증기관은 인터넷 서비스 이용자가 이용하기를 희망하는 인터넷 서비스 제공자에 관한 정보 및 인터넷 서비스 이용 범위에 관한 정보를 포함하는 인증서를 인터넷 서비스 이용자에게 제공한다. 인터넷 서비스 제공자는 인증서를 이용하여 정당한 사용자의 확인을 용이하고 완전하게 함과 동시에, 정당하지 않는 제 3자의 침입에 의한 부당한 손실을 방지할 수 있다. 또한 인터넷 서비스 이용자는 인증서 제출이라는 간단한 절차로 인터넷 서비스 로그인 및 등급별 서비스 이용 권한을 획득할 수 있으며, 이용자 개인의 정보가 유출되는 것을 막을 수 있다. 등록기관, 인증기관, 인증서, 전자서명, 개인키, 공개키, 인터넷 서비스 로그인, 서비스 이용권한, 암호화된 메시지

Abstract

The present invention relates to the method for controlling the service use range of the internet service client and internet service access log-on using the certificate. And if the authentication is demanded with the click procedure of meaning submission of the certificate from the internet service client, the certificate in which the Internet service provider is submitted from the user is read and the internet service log-on can be controlled and in order that the information showing the service use range included in moreover, the certificate is made out and by grade service access log-on of the internet service client is controlled the certificate in which the certifying authority includes the information about the information about the Internet service provider which desires that the internet service client uses and range of use of internet service is provided for the internet service client it is facilitated and it makes the authentication of user in which the Internet service provider is justifiable using the certificate perfect. Simultaneously the unjust loss by the invasion of the third party which is not justifiable can be prevented the internet service log-on and by grade service using authority can be obtained to the simple procedure. Moreover, the in

ternet service client is submission of the certificate I
t can prevent that the information of the user indivi
dual is taken out.
The registration authority, the certifying authority,
the certificate, the electronic signature, the private
key, the public key, the internet service log-on, the
service using authority, the encoded message .

대표도면(Representative drawing)



청구의 범위

Scope of Claims

청구 1항:

인증서를 이용하여 이용자의 인터넷 서비스 액세스 이용 범위를 제어하도록 인증서를 제공하는 방법에 있어서, 인터넷 서비스 제공자로부터 이용자가 희망하는 인터넷 서비스 이용 범위를 나타내는 정보를 수신하는 단계와, 상기 인터넷 서비스 제공자로부터 수신한 상기 인터넷 서비스 이용 범위를 나타내는 정보를 상기 인증서에 포함시키는 단계와, 상기 이용자에게 상기 인증서를 제공하는 단계를 포함하는 인증서를 이용하여 이용자의 인터넷 서비스 액세스 이용 범위를 제어하도록 인증서를 제공하는 방법.

청구 3항:

인증서를 이용하여 이용자의 인터넷 서비스 액세스를 제어하는 방법에 있어서, 상기 이용자로부터 사용자 인증서를 포함하는 암호화된 메시지를 수신하는 단계와, 상기 사용자 인증서를 포함하는 암호화된 메시지를 복호화하는 단계와, 상기 복호화 결과에 따라 상기 이용자의 인터넷 서비스 액세스를 제어하는 단계를 포함하는 인증서를 이용하여 이용자의 인터넷 서비스 액세스를 제어하는 방법.

청구 4항:

제 3 항에 있어서, 상기 이용자 인증서에는 서비스 이용범위를 나타내는 정보가 포함되고, 상기 복호화 결과에 따라 상기 이용자의 인터넷 서비스 액세스를 제어하는 단계는, 상기 복호화 결과 얻어진 이용자 인증서의 서비스 이용범위를 판독한 결과에 따라 상기 이용자의 인터넷 서비스 액세스를 제어하는, 인증서를 이용하여 이용자의 인터넷 서비스 액세스를 제어하는 방법.

청구 7항:

인증서를 이용하여 인터넷 서비스 이용자의 인터넷 서비스 로그온 액세스를 제어하는 방법에 있어서, 인터넷 서비스 제공자와 인터넷 서비스 이용자에게 각각 제공자 인증서와 이용자의 서비스 이용범위를 나타내는 정보를 포함하는 이용자 인증서를 제공하는 단계와, 상기 인터넷 서비스 제공자는 상기 인터넷 서비스 이용자로부터 상기 이용자 인증서를 포함하는 암호화된 메시지를 수신하는 단계와, 상기 인터넷 서비스 제공자는 상기 수신된 암호화된 메시지를 복호화하는 단계와, 상기 복호화 결과 상기 이용자 인증서에 포함된 서비스 이용범위에 따라 상기 인터넷 서비스 이용자의 인터넷 서비스 로그온 액세스를 제어하는 단계를 포함하는 인증서를 이용하여 인터넷 서비스 이용자의 인터넷 서비스 로그온 액세스를 제어하는 방법.

Claim 1:

The method for providing the certificate in order to control the internet service access usage range of the user using the certificate including providing the step, of receiving the information showing the range of use of internet service that the user desires the certificate as to the method for providing from the Internet service provider the step of including the information showing the range of use of internet service received from the Internet service provider in the certificate, and the certificate to the user to control the internet service access usage range of the user using the certificate.

Claim 3:

The method for controlling the internet service access of the user using the certificate, wherein the method for controlling the internet service access of the user using the certificate including the step of controlling the step, of receiving the encoded message including the user certificate from the user the step of decoding the encoded message including the user certificate, and the internet service access of the user according to the descrambling result.

Claim 4:

As for claim 3, the method wherein the step the information showing the service use range is included in the user certificate ; and of controlling the internet service access of the user according to the descrambling result controls the internet service access of the user using the certificate that controls the internet service access of the user according to the result reading the service use range of the gained user certificate.

Claim 7:

The method for controlling the internet service log-on access of the internet service client using the certificate, wherein the method for controlling the internet service log-on access of the internet service client using the certificate including the step of controlling the step, of providing the user certificate including the information showing the service use range of the user and provider certificate to the Internet service provider and internet service client the step, that the Internet service provider receives the encoded message including the user certificate from the internet service client the step that the Internet service provider decodes the above-mentioned received encoded message, and the internet service log-on access of the internet service client according to the service use range included in the descrambling result user certificate.

배경기술

Background Art

본 발명은 인터넷 서비스 로그인 및 등급별 인터넷 서비스 이용 권한 획득방법에 관한 것으로서, 좀 더 구체적으로는, 인증서를 이용하여 인터넷 서비스에 로그인하고 등급별 인터넷 서비스 이용 권한을 획득하는 방법에 관한 것이다.

지금까지 인터넷 서비스 로그인 및 등급별 서비스 이용 권한 획득 방법으로는 대부분 데이터베이스를 활용한 ID/Password 방식을 사용하여 왔다. 상기 ID/Password 방식은 인터넷 서비스 이용자가 인터넷 서비스 제공자의 초기 사이트에 접속하여 사용자 자신의 ID와 Password 등을 입력하면, 인터넷 서비스 제공자는 자신의 시스템의 데이터베이스에 인터넷 서비스 이용자의 ID, Password, 인터넷 서비스 사용의 유효기간, 사용자의 등급 등을 저장하여, 상기 데이터베이스화된 사용자의 ID와 Password에 따라 이용자의 인터넷 서비스 로그인을 제어하고, 상기 데이터베이스화된 이용자의 등급에 따라 이용자의 인터넷 서비스 이용 권한을 제어하도록 한 것이다.

실제로 흔히 볼 수 있는 상기 인터넷 서비스 이용 권한 제어의 예로는, 인터넷 서비스 제공자의 데이터베이스에 guest 라는 목록을 만들어 놓고, 상기 guest 목록에 저장된 인터넷 서비스 이용자는 인터넷 서비스 제공자가 제공하는 인터넷 서비스의 일부분만 이용할 수 있도록 하여 인터넷 서비스 이용 권한을 축소시키는 방법이 있다.

The invention relates to the internet service log-on and by grade internet service using right acquiring method, more specifically, to the method for logging on using the certificate in the internet service and obtaining by grade internet service using right.

So far, it came to the internet service log-on and by grade service using authority acquiring method using the mode of the ID / Password which mostly utilized the database. The ID / Password mode controls ID of the user oneself the internet service client connects to the initial site of the Internet service provider and the internet service using right of the user according to the class of the above-mentioned user stored in a database the internet service log-on of the user is controlled according to ID and Password of the above-mentioned user stored in a database the input image, and the Internet service provider store ID of the internet service client, the Password, the term of validity of the internet service use, the class of the user etc. the Password etc. in the database of its own system.

In fact, as an example of the internet service using right control which it generally can look, there are the method the list called the guest is comprised of the database of the Internet service provider and for the internet service client stored in the guest list on one part of the internet service which the Internet service provider provides using and reducing the internet service using right.

발명의 내용

발명의 효과

본 발명은 인터넷 서비스 사용자에게 서비스 로그인 권한과 등급별 서비스 이용 권한을 부여하는 데에 인증서를 이용함으로써, 인터넷 서비스 제공자는 자신의 서버로의 불법적인 침입을 막고, 정당한 사용자만을 시스템에 접근시킬 수 있으므로, 인터넷 서비스 제공자의 운영 시스템의 안정성을 유지할 수 있다.

또한, 암호화 기법을 이용한 인증서의 사용에 의해, 사용자의 PC에 저장된 개인키는 단 한명의 개인만이 보유하고 있고, 따라서 개인 정보 및 개인의 권한에 관한 정보는 인증 기관은 물론이고 인터넷 서비스 제공자조차도 볼 수 없으므로, 개인 정보 유출을 막을 수 있고 개인 정보를 확실하게 보호할 수 있다.

또한, 인증서를 이용한 인터넷 서비스 로그인 및 이용 권한 통제 시스템은 한번의 클릭으로 인터넷 서비스 사용자의 신분을 증명해 줄 수 있으므로, 사용자가 키보드를 이용하여 ID/Password를 입력하는 방식보다 편리하게 서비스를 이용할 수 있다.

Summary of Invention

Effects of the Invention

The invention uses the certificate to the internet service user for the service log-on authority and granting by grade service using authority. In that way the Internet service provider prevents the illegal invasion to its own server and it can get near the system only the just user. Therefore the stability of the operating system of the Internet service provider can be maintained.

Moreover, using the use of the certificate using the cryptography, however the private key stored in PC of the user holds only one individual and therefore the information about the personal information and individual authority cannot look even the Internet service provider as well as the certifying authority. Therefore the personal information outflow can be prevented and the personal information can be authentically protected.

Moreover, the internet service log-on and the using right control system using the certificate can prove the identity of the internet service user to one click. Therefore the service can be conveniently used than the mode in which the user inputs the ID / Password using the keyboard.

또한, 인증서에 이용자가 사용을 희망하는 서비스 등급 등을 설정할 수 있으므로, 인터넷 서비스 제공자와 이용자간의 커뮤니케이션을 활성화시킬 수 있다.

Moreover, the grade of service etc. can be set up. Therefore the user desires the use in the certificate the communication between the user and the Internet service provider can be activated.

기술적 과제

상기 설명한 종래의 기술은 이용자의 인터넷 서비스 로그인 및 등급별 서비스 이용 권한이 ID/Password에만 의존되어 있다는 점 때문에 다음과 같은 문제가 있다.

ID/Password 방식은 사용자의 ID/Password가 인터넷 서비스 제공자의 시스템에 데이터베이스화되어 있으므로, 데이터베이스에 문제가 발생하게 되면, 즉, 예를 들어 인터넷 서비스 제공자의 실수로 데이터베이스가 삭제되거나, 크래커의 침입으로 ID/Password가 변경되거나 삭제된 경우, 인터넷 서비스 사용자는 물론이고 인터넷 서비스 제공자조차도 손을 쓸 수가 없어, 서비스 제공자나 서비스 사용자 양방에 막대한 피해를 입힐 수밖에 없다.

또한, 대부분의 사용자는 다수의 인터넷 서비스를 이용하고 있고 이를 이용하기 위해 ID/Password를 만들어 사용하고 있으나, 자주 사용하지 않는 ID/Password의 경우 분실 가능성이 높으며, 잃어버린 ID/Password를 되찾는 과정도 쉽지 않다. ID/Password의 분실에 대한 대책으로 이메일 등을 통하여 개인의 정보를 보내면 ID/Password를 알아낼 수 있는 정책을 세우기는 했지만, 사용자는 ID/Password를 잃어버릴 때마다 되찾는 절차가 번거로운 수밖에 없고, 이를 검색해서 다시 사용자에게 통지해 주어야 하는 인터넷 서비스 제공자의 입장에서조차 역시 비생산적일 수밖에 없다. 그 뿐만 아니라, 사용자가 분실한 ID/Password를 되찾지 않고 새로 발급 받거나, 발급 받고도 사용하지 않는 ID/Password도 또한 데이터베이스의 한 구역을 차지하고 있어 데이터베이스를 방대하게 하므로 운영자에게 골칫거리가 아닐 수 없다.

인터넷을 이용하는 계층은 이미 소수의 특정 집단을 벗어나 대중에게로 확산되었고, 인터넷 시장은 이미 포화 상태인 현실 속 시장과는 달리 개척의 여지가 있고, 확장의 가능성이 보유한 장이다. 그러나, 인터넷 발전 초기에는 전혀 고려되지 않았던 보안상의 문제와 윈도우 환경에 익숙하여 마우스 조작에만 능숙한 이용자에게 키보드 이용을 강요하는 환경은 인터넷 사용을 위축시킬 수 있는 요인으로 꼽히고 있어, 인터넷 시장의 확장가능성을 살리지 못하고 있는 형편이다.

Technical Task

The problem as follows has as to the above-mentioned conventional technology illustrated, because the internet service log-on and by grade service using a authority of the user are depended on the ID / Password.

The ID / Password of the user the ID / Password mode is databased in the system of the Internet service provider. Therefore if the problem occurs in the database the database is mistakenly expunged of in other words, for example, the Internet service provider or in case the ID / Password is changed to the invasion of the cracker or it is deleted the user cannot take a step and the enormous damage cannot help being played the service provider or the service user both with.

Moreover, in order to most of users use multiple internet services and use the same, the ID / Password is made and it uses. But the lost possibility is high in case of the ID / Password which it frequently does not use and process of regaining the ID / Password lost are not easy. The policy which could find the ID / Password if it sent the individual information to the measures toward the loss of the ID / Password through the e-mail etc. was established. However the procedure of regaining whenever the user loses the ID / Password cannot help being troublesome and it cannot help being also nonproductive in the position of the Internet service provider which searches this and notified user. Besides, the ID / Password which the user loses is not regained and it newly gets issuance or since the ID / Password which it does not use even though it receives issuance occupies moreover, one corner of the database and it makes the database massive it cannot be not to the administrator the headache.

The decimal specific class was already deviated from and the layer using the internet was diffused to the mass of people and the layer has the filter paper of the pathfinding to the reality inside market where the internet market is already the saturation condition and it is the place where the possibility of the expansion is held. But in the internet development initial, it is reckoned as the factor in which the environment which is familiar with the problem and window environment of in security which was not considered and forces the user who is tactful for the mouse management to do the keyboard usage can dwindle the internet using and it is the consequence which does not save the expandability of the internet market.

따라서, 본 발명은 상기와 같이 ID/Password 방식의 문제점 즉, 크래커의 침입, ID/Password 분실, 관리의 어려움, ID/Password 사용상의 불편함, 확장가능성이 무한한 인터넷의 사용범위 위축 등을 인식하여 이루어진 것으로, 인증서를 이용하여 인터넷 서비스 로그인 및 등급별 서비스 이용 권한을 획득하게 함으로써 인터넷상의 서비스 제공자와 서비스 사용자 모두의 편의성을 추구하고, 인터넷 사용의 보안성을 높이는 것을 목적으로 한다.

Therefore, the problem of the ID / Password mode, in other words, the invasion of the cracker, the ID / Password loss, the difficulty of the administration, the inconvenience of the ID / Password use of, the usage flexibility shrinkage of the internet in which the expandability is unlimited etc. are recognized and as described above, the invention is made. The convenience of the service provider on the internet and service user everyone are sought after by obtaining the internet service log-on and by grade service using a authority using the certificate and it is done by the purpose heightening the security of the internet using.

발명의 구성 및 작용

본 발명은 인증기관과 암호화기법을 이용한 인증서를 활용하여 인터넷 서비스 이용자가 인증기관에 등록된 인터넷 서비스 제공자의 인터넷 서비스에 로그인 및 등급별 서비스 이용권한 획득을 가능하게 하는 방법에 관한 것이다.

본 발명의 하나의 특징은 인증서를 이용하여 이용자의 인터넷 서비스 액세스 이용 범위를 제어하도록 인증서를 제공하는 방법에 관한 것으로, 인터넷 서비스 제공자로부터 이용자가 희망하는 인터넷 서비스 이용 범위를 나타내는 정보를 수신하는 단계와, 상기 인터넷 서비스 제공자로부터 수신한 상기 인터넷 서비스 이용 범위를 나타내는 정보를 상기 인증서에 포함시키는 단계와, 상기 이용자에게 상기 인증서를 제공하는 단계를 포함한다.

본 발명의 다른 특징은, 상기 인증서를 이용하여 이용자의 인터넷 서비스 액세스 이용 범위를 제어하도록 인증서를 제공하는 방법에서, 상기 이용자가 희망하는 인터넷 서비스 이용 범위를 나타내는 정보가, 인터넷 서비스의 이용에 따른 이용대금의 유무, 유료 인터넷 서비스의 경우 지불 금액, 이용자의 참여도에 따라 구분되는 범위를 나타내는 것이다.

본 발명의 또 다른 특징은 인증서를 이용하여 이용자의 인터넷 서비스 액세스를 제어하는 방법에 관한 것으로, 상기 이용자로부터 이용자 인증서를 포함하는 암호화된 메시지를 수신하는 단계와, 상기 이용자 인증서를 포함하는 암호화된 메시지를 복호화하는 단계, 그리고 상기 복호화 결과에 따라 상기 이용자의 인터넷 서비스 액세스를 제어하는 단계를 포함한다.

본 발명의 또 다른 특징은 상기 인증서를 이용하여 이용자의 인터넷 서비스 액세스를 제어하는 방법에서, 상기 사용자 인증서에는 서비스 이용범위를 나타내는 정보가 포함되고, 상기 복호화 결과에 따라 상기 이용자의 인터넷 서비스 액세스를 제어하는 단계는, 상기 복호화 결과 얻어진

Structure & Operation of the Invention

The present invention relates to the method for utilizing the certificate using the certifying authority and cryptography and making the log-on and by grade service using authority acquisition possible in the internet service of the Internet service provider in which the internet service client is registered in the certifying authority.

The characteristic of one of the invention comprises the step of providing the step, of receiving the information which shows the range of use of internet service that the user desires the certificate as the method for providing from the Internet service provider it controls the internet service access usage range of the user using the certificate the step of including the information showing the range of use of internet service received from the Internet service provider in the certificate, and the certificate to the user.

As to the dissimilar characteristic of the invention, the information showing the range of use of internet service that the user hopes shows the range classified according to the payment amount, and the participation score of the user in the method for providing the certificate in order to control the internet service access usage range of the user using the certificate, in case of the occurrence of the usable funds according to the usage of the internet service, and the charged internet service.

Another characteristic of the present invention comprises the step of receiving the encoded message including the user certificate as the method for controlling the internet service access of the user using the certificate from the user, the step of decoding the encoded message including the user certificate and the step of controlling the internet service access of the user according to the descrambling result.

In the method in which another characteristic of the present invention controls the internet service access of the user using the certificate, the information showing the service use range is included in the user certificate and the internet service access of the use

이용자 인증서의 서비스 이용범위를 판독한 결과에 따라
상기 이용자의 인터넷 서비스 액세스를 제어하는 것이다.

r is controlled according to the result reading the service use range of the user certificate in which the step of controlling the internet service access of the user according to the descrambling result is obtained.

본 발명의 또 다른 특징은 상기 인증서를 이용하여 이용자의 인터넷 서비스 액세스를 제어하는 방법에서, 상기 이용자로부터 인터넷 서비스 액세스 요청을 수신하면 메시지 원본, 인터넷 서비스 제공자의 제공자 인증서를 상기 이용자에게 전송하는 단계를 더 포함하고, 상기 이용자로부터 수신한 이용자 인증서를 포함하는 암호화된 메시지는, 상기 메시지 원본, 상기 이용자 인증서, 상기 제공자 인증서를 이용자 개인키, 제공자 공개키, 비밀키로 암호화한 메시지와, 상기 이용자 인증서를 포함하는 암호화된 메시지를 복호화하는 단계는, 상기 이용자 인증서를 포함하는 암호화된 메시지를 제공자 개인키, 이용자 공개키, 비밀키를 이용하여 복호화하는 것이다.

In the method in which another characteristic of the present invention controls the internet service access of the user using the certificate, message original copy, and the step of transmitting the provider certificate of the Internet service provider to the user further are included if the internet service access request is received from the user and the encoded message including the user certificate received from the user is the message original copy, the user certificate, and the message encoding the provider certificate to the user private key, the provider public key, and the secret key and the encoded message in which the step of decoding the encoded message including the user certificate includes the user certificate is decoded using the provider private key, the user public key, and the secret key.

본 발명의 또 다른 특징은 상기 인증서를 이용하여 이용자의 인터넷 서비스 액세스를 제어하는 방법에서, 이용자로부터 인터넷 서비스 액세스 요청을 수신하면 메시지 원본, 제공자 인증서를 이용자에게 전송하는 단계를 더 포함하고, 상기 이용자로부터 수신한 이용자 인증서를 포함하는 암호화된 메시지는, 상기 메시지 원본, 상기 메시지 원본의 전자 서명, 상기 이용자 인증서를 비밀키로 암호화한 제 1 암호화된 메시지와, 상기 제공자 인증서와 상기 비밀키를 제공자 공개키로 암호화한 제 2 암호화된 메시지를 포함하고, 상기 이용자 인증서를 포함하는 암호화된 메시지를 복호화하는 단계는, 상기 제 2 암호화된 메시지를 제공자 개인키를 이용하여 제공자 인증서와 비밀키로 복호화하는 단계와, 상기 제 1 암호화된 메시지를 상기 비밀키를 이용하여 메시지 원본, 전자서명, 이용자 인증서로 복호화하는 단계를 포함하는 것이다.

Another characteric of the present invention includes the encoded message, is the message original copy, the electronic signature of the message original copy, and the first encoded message, encoding the user certificate to the secret key and the second encoded message encoding the provider certificate and secret key to the provider public key including the user certificate which it further includes the message original copy, and the step of transmitting the provider certificate to the user if it receives the internet service access request by the method for controlling the internet service access of the user using the certificate from the user and the user receives from the user and the step of decoding the encoded message including the user certificate includes the provider certificate using the provider private key the second encoded message and the step of decoding to the secret key, the message original copy using the secret key the first encoded message, the electronic signature, and the step of the user authentication *** decoding.

본 발명의 또다른 특징은 인증서를 이용하여 인터넷 서비스 이용자의 인터넷 서비스 로그온 액세스를 제어하는 방법에 관한 것으로, 인터넷 서비스 제공자와 인터넷 서비스 이용자에게 각각 제공자 인증서와 이용자의 서스 이용범위를 나타내는 정보를 포함하는 이용자 인증서를 제공하는 단계와, 상기 인터넷 서비스 제공자는 상기 인터넷 서비스 이용자로부터 상기 이용자 인증서를 포함하는 암호화된 메시지를 수신하는 단계와, 상기 인터넷 서비스 제공자는 상기 수신된 암호화된 메시지를 복호화하는 단계와, 상기 복호화 결과 상기 이용자 인증서에 포함된 서비스 이용범위에 따라 상기 인터넷 서비스 이용자의 인터넷 서비스 로그온 액세스를 제어하는 단계를 포함한다.

Another characteristic of the invention comprises the step of controlling the step, of providing the user certificate including the information showing the usage range of the user and provider certificate as the method for controlling the internet service log-on access of the internet service client using the certificate to the Internet service provider and internet service client the step, that the Internet service provider receives the encoded message including the user certificate from the internet service client the step that the Internet service provider decodes the above-mentioned received encoded message, and the internet service log-on access of the internet service client according to the service use range included in the descrambling result user certificate.

인증기관(102)은 수신한 인증요청서에 서명을 하여 인증서를 발급하고 발급된 인증서 리스트를 데이터베이스화하고 인증서 해지목록 또한 데이터베이스화하며, 발급된 인증서를 네트워크를 통하여 인증서 발급 요청자에게 발송한다.

이용자(103)는 통신 네트워크를 통해 등록기관(101)으로 인증서 발급 요청을 전송하고, 인증기관(102)으로부터 발급된 인증서를 수신하며, 이용자(103)의 컴퓨터에서 내부적으로 생성된 개인키와 공개키 중 개인키와 상기 인증서를 이용하여 네트워크를 통해 인터넷 서비스 제공자(104)의 인터넷 서비스에 로그인 액세스한다.

인터넷 서비스 제공자(103) 역시 본 인증 시스템을 이용하기 위해서 상기 이용자와 마찬가지로 절차를 거쳐 인증기관(102)으로부터 인증서를 발급받으며, 서비스 제공자 컴퓨터에서 내부적으로 생성된 개인키와 공개키 및 인증서를 이용하여 인터넷 서비스 제공자의 인터넷 서비스에 액세스하기를 희망하는 이용자의 로그인 허용 또는 통제를 한다.

도 2는 인터넷 서비스 이용자가 인증기관으로부터 인증서를 발급받는 과정을 보여주는 흐름도이다.

인터넷 서비스 액세스시 인증서를 이용하기를 희망하는 이용자(103)는 서비스 이용을 희망하는 인터넷 서비스 제공자에게 희망하는 서비스 등급등을 표시하여 회원신청을 한다(단계 201). 상기 인터넷 서비스 제공자가 제공하는 인터넷 서비스는 유료 또는 무료일 수 있으며, 상기 서비스 등급은 서비스 비용에 따라 분류된 등급일 수도 있고 이용자의 사용범위에 따라 분류된 등급일 수도 있다. 상기 회원신청을 수신한 인터넷 서비스 제공자는 회원등록을 하고(단계 202), 상기 이용자의 정보 예컨대, 이용자가 희망하는 서비스 등급 등의 정보를 등록기관에 전송한다. 그 후 인증기관(102)으로부터 인증서를 발급받기를 희망하는 이용자(103)는 인증서를 발급받기 위한 요청을 등록기관(101)에 전송한다(단계 203). 이용자로부터 상기 요청을 수신한 등록기관은 인증서 발급을 위해 기재되어야 하는 인증요청서를 이용자에게 발송한다(단계 204). 이때 인터넷 서비스 제공자로부터 수신한 이용자의 서비스 등급 정보를 참조하여, 상기 이용자의 서비스 등급이 디폴트로 설정되어 있는 인증요청서를 발송한다. 이용자는 상기 등록기관으로부터 발송된 인증요청서를 수신하고(단계 205), 상기 요청서에 이용자 개인의 정보를 기록한다(단계 206). 또한, 등록기관으로부터 상기 인증요청서의 수신은 이용자 컴퓨터에서 이용자가 사용하고 있는 웹브라우저, 예컨대 인터넷 익스플로러 또는 넷스케이프 네비게이터 등의 내에 내재되어 있는 키 생성 모듈을 자극시켜 구동시키고, 상기 구동에 의해 이용자 컴퓨터의 내부에서 한쌍의

ment and credit information of the requester etc. are transmitted through the network in the certifying authority.

It attaches signature to the authentication request document which the certifying authority (102) receives and the certificate is issued and the issued certificate list is made into a database and the moreover makes into a database in the certificate termination list and the issued certificate is forwarded to the issuing of certificate requester through the network.

The user (103) transmits the certificate issue request to the registration authority (101) through the communication network and the certificate issued from the certifying authority (102) is received and the log-on accesses in the internet service of the Internet service provider (104) among the private key and the public key interior generated in the computer of the user (103) using the private key and certificate through the network.

In order to use the authentication system which also it looks with the Internet service provider (103), the certificate is issued after the user and identity process from the certifying authority (102) and it controls as the log-on acknowledgment of the user which desires to access using the private key, interior generated in the service provider computer the public key and certificate in the internet service of the Internet service provider.

Figure 2 is a flowchart showing the process where the certificate is issued to the internet service client from the certifying authority.

The grade of service etc. are indicated and it desires to the Internet service provider in which the user (103) which desires to use the certificate in the internet service access desires *** it applies for membership (201 step). The internet service which the Internet service provider provides can be the charge or no charge and it can be the class in which the grade of service is classified according to the service cost and it be the class classified according to the usage flexibility of the user. The Internet service provider receiving the member application registers as a member and the information including the grade of service etc. is transmitted in the registration authority. The information of the user, for example, the user hopes. Thereafter, the request in which the certificate is issued to the user (103) which desires to the certificate be issued from the certifying authority (102) is transmitted in the registration authority (101) (203 step). The registration authority receiving the request from the user forwards the authentication request document which has to be written to the user for the issuing of certificate (204 step). Then, the authentication request document in which the grade of service of the user is set as default is forwarded with reference to the service grade information of the user receiving from the Internet service provider. The user receives the authentication request document (20

대칭키인 개인키와 공개키가 생성된다(단계 207). 인증요청서에 개인정보를 모두 기록한 이용자는 상기 요청서를 등록기관에 발송(단계 208)하는데, 이때 이용자의 컴퓨터에서 생성된 이용자의 공개키도 함께 발송된다. 한편, 생성된 이용자의 개인키는 이용자의 컴퓨터에만 저장되며, 공개되지 않으므로, 인터넷 서비스 제공자는 물론이고 인증기관조차 접근할 수 없다. 상기 인증요청서를 수신한 등록기관은 이용자의 신용정보등을 조회, 심사하여 요청자를 확인하고(단계 209), 상기 인증요청서를 인증기관으로 발송한다(단계 210). 등록기관으로부터 인증요청서를 수신한 인증기관은 상기 인증요청서를 검토는데(단계 211), 다만, 이용자에 대한 실질적인 심사는 등록기관에 의해 이루어질 수 있다. 그후 인증기관은 이용자의 공개키가 담겨진 인증서에 상기 인증기관의 서명을 첨부하고, 상기 서명된 인증서를 이용자에게 발송한다(단계 212). 실제로는, 인증서에 인증기관의 서명을 첨부한다는 것은, 이용자의 공개키가 담겨진 인증서를 인증기관의 개인키로 암호화한다는 의미이며, 인증기관의 개인키로 암호화된 인증서는 인증기관의 공개키에 의해 복호화되어야 하고, 이러한 이유로, 인증기관은 이용자 인증서를 이용자에게 발송함과 아울러 인증기관의 공개키가 담겨진 인증기관 인증서도 함께 발송한다. 그러면, 이용자는 인증기관으로부터 발송된 인증서를 수신하고(단계 213), 상기 인증서를 이용자 컴퓨터에 설치하고 저장한다(단계 214).

인터넷 서비스 제공자가 인증서를 발급받는 과정은 상기 과정중 단계(201)와 단계(202)만 제외하면 이용자가 인증서를 발급받는 과정과 동일하다.

상기 인증서에 포함되는 정보를 보여주기 위해 상기 인증서의 한 예를 도 3을 참조하여 설명한다. 인증서 버전은 해당 인증서의 등급을 표시하는 것으로서, 예컨대 버전이 3인 경우는 확장영역을 표시하고, 버전이 1, 2인 경우는 확장영역을 표시하지 않는다는 것을 의미한다. 인증서 유효기간은 해당 인증서를 유효하게 사용할 수 있는 기간을

5 step) forwarded from the registration authority and the information of the user individual is recorded in the request document (206 step). Moreover, in the reception of the authentication request document from the registration authority is the user computer, the key generation module input in the web browser, which the user uses for example, in including the Internet Explorer or the Netscape navigator etc. is simulated and it drives and the private key and the public key which is a pair of symmetric keys within the user computer are generated with the driving (207 step). The user who altogether records the personal information in the authentication request document the request document in the registration authority the sending (208 step). The public key of the user then generated in the computer of the user is together forwarded. In the meantime, the generated private key of the user is stored in the computer of the user and it is not open. Therefore the computer can not approach. The registration authority receiving the authentication request document inquires the credit information of the user etc. and it examines and the requester is confirmed (209 step) and the authentication request document is forwarded to the certifying authority (210 step). The certifying authority receiving the authentication request document from the registration authority is the authentication request document increased with review (211 step). The substantial examination about the user can be made with the registration authority. Thereafter, the certifying authority attaches the signature of the certifying authority to the certificate in which the public key of the user is involved and the above-mentioned signed certificate is forwarded to the user (212 step). In fact, it is the meaning of encoding the certificate in which the public key of the user is involved to the private key of the certifying authority to attach the signature of the certifying authority to the certificate and the certificate encrypted by the private key of the certifying authority has to be decoded with the public key of the certifying authority and for this reason, the certifying authority forwards the user certificate to the user and the CA certificate in which the public key of the certifying authority is involved together forwards. And then, the user receives the certificate (213 step) forwarded from the certifying authority and it sets up and the certificate is stored in the user computer (214 step).

If it excludes, the user as to the process, where the certificate is issued to the Internet service provider the step (201) and step (202) are identical with the process of the certificate being issued among the process.

In order to show the information included in the certificate, referring to Figure 3, one example of the certificate is illustrated. The certificate version indicates the class of the correspondence certificate. The case in which it is for example, the version 3 indicates the extended area and it means that the case in which it is the version 1, 2 does not indicate the extended

나타낸다. 확장영역은, 인증서의 사용범위를 나타내는 것으로, 인증서를 인터넷 서비스 로그인에 사용할 것인지, 이메일 전송에 사용할 것인지, 인증서를 이용하여 서비스의 등급을 분류할 것인지에 관한 정보가 포함된다. 서명 알고리즘에는 해쉬(hash) 함수 정보, 비대칭(asymmetric) 함수 정보등이 기재되며, 발행자 정보에는 인증서를 발급해준 인증기관의 정보가 기재된다.

area. The period when the certification available period tellingly can use the correspondence certificate is indicated. The extended area shows the usage flexibility of the certificate. And the certificate is used in the internet service log-on whether it uses in the transmitting email whether the information which relates about classifying the class of service using the certificate is included. The hash function information, the asymmetry (asymmetric) function information etc is described in the signature algorithm and the information of the certifying authority issuing the certificate are in the issuer information.

신청자 정보에는 인증서 발급 요청을 한 신청자의 개인 정보와 함께 인터넷 서비스 이용자가 이용을 희망하는 인터넷 서비스 제공자 및 인터넷 서비스 제공자가 제공하는 인터넷 서비스의 이용 범위를 나타내는 정보가 포함된다. 인터넷 서비스의 이용 범위를 나타내는 정보에는, 유료/무료 서비스 여부, 유료 인터넷 서비스의 경우 지불 금액에 따른 인터넷 서비스 등급, 인터넷 서비스에 대한 이용자의 참여도에 따른 서비스 등급 등이 포함된다. 상기 이용 범위를 나타내는 정보에는 예를 들어, mp3 파일의 경우 다운로드가 가능한 곡의 수, 또는 다운로드가 가능한 곡의 범위(다운로드 횟수에 상관없이), 웹서적의 경우 다운로드 가능한 책의 권수, 또는 다운로드가 가능한 책의 범위(다운로드 횟수에 상관없이), 인터넷 가상 강의의 경우 수강할 수 있는 또는 청강할 수 있는 강의의 범위, 사설 인터넷 교육의 수강 범위, 네트워크 게임의 경우 자신이 소유하고 있는 사이버 머니의 양, 전자 상거래 이용 허용 여부, 전자 상거래 신뢰도 측정 여부, 인터넷 방송의 시청 범위, 의학 정보 취득의 범위, 각종 포럼, 논문 등의 정보 취득 범위, 전자 투표의 참여 범위(이중으로 투표하는 것을 방지할 수 있어, 투표의 신뢰성을 기할 수 있다), 나아가서는 전자 투표의 신원 확인의 역할등이 있다.

The applicant information includes the Internet service provider in which the internet service client desires the usage with the personal information of the applicant requesting with issuing of certificate and the information showing the usage range of the internet service which the Internet service provider provides. The information showing the usage range of the internet service includes charge / free service acceptance and rejection, the internet service class according to the payment amount in case of the charged internet service, the grade of service according to the participation score of the user about the internet service etc. In case of the range (regardless of the number of download) of the number of tune in which the download is possible in the information showing the usage range in case of for example, the mp3 file or the tune in which the download is possible, and the web book, it further more has the role of the identification of the electronic voting etc. in case of the range (regardless of the number of download) of the book in which the number of turns or the download of the downloadable book is possible, and the internet imaginary lecture in case of the range of the lecture, which can take and which or it can listen the attending range of the private internet education, and the network game with the information acquisition range, participation range (it can prevent dually from voting and the reliability of the vote can be pledged) of the electronic voting including the view range of the amount, electronic commerce permission of use acceptance and rejection, electronic commerce trust measurement acceptance and rejection, the intercast of the cyber money, the range of the medical information captured, all kinds of the forum, paper etc. oneself possesses.

이용자 공개키에는 이용자 컴퓨터에서 생성된 공개키가 표시되며, 인증기관의 서명은, 인증서에 포함된 위의 항목을 모두 해수 알고리즘을 이용하여 인증기관의 개인키로 암호화한 부분이다. 상기 설명한 인증서는 예시적인 것이므로, 인증서에는 정책에 따라 다른 다양한 정보를 포함시킬 수 있으며, 인터넷 서비스 제공자는 상기 인증서에 포함된 정보를 판독하여 서비스 로그인, 등급별 서비스 이용권한 부여 등을 판단할 수 있다.

In the user public key, the public key generated in the user computer is indicated and the signature of the certifying authority is the part which altogether encodes the item included in the certificate using the hash algorithm to the private key of the certifying authority. The above-mentioned certificate illustrated is illustrative. Therefore the dissimilar and various information can be included in the certificate according to the policy and the information in which the Internet service provider is included in the certificate is made out and the service log-on, by grade service using authority granting etc. can be determined.

is produced. As to the hash function, the message compression function is added to the property of the one-way function. It cannot decode since the inverse function is nonexistent.

이렇게 생성된 전자 서명과 메시지 원본, 그리고 이용자의 인증서 이 세가지를 한데 묶어 비밀키로 암호화하여 제 1 암호화된 메시지(Encrypted Message)를 생성한다.

In this way, the generated electronic signature, the message original copy and certificate this man of influence paper of the user are together bound and it encodes to the secret key and the message (Encrypted Message) encrypted with the first is produced.

여기서 비밀키라는 것은 암호화와 복호화를 하나의 키로 해내는 암호방식을 의미하는 것으로, 암호화속도가 빨라서 많은 양의 메시지의 암호화에 유리하지만, 암호화와 복호화가 하나의 키로 이루어지므로, 키 관리를 철저히 해서 인터넷 서비스 제공자에게 보내야만 인터넷 서비스 제공자는 이 비밀키를 이용해서 제 1 암호화된 메시지를 복호화시킬 수 있다. 이와 같은 이유로, 상기 비밀키와 인터넷 서비스 제공자의 인증서를 한데 묶어 인터넷 서비스 제공자의 인증서에 담겨진 공개키로 암호화시켜, 제 2 암호화된 메시지(전자 봉투, digital envelope)를 생성한다. 물론, 이때 인터넷 서비스 제공자의 인증서는 인증기관의 개인키로 암호화되어 있고, 이용자는 인증기관으로부터 수신한 인증기관의 인증서에 포함된 인증기관의 공개키를 이용하여 인터넷 서비스 제공자의 인증서를 복호화하여 인터넷 서비스 제공자 인증서에 담겨진 인터넷 서비스 제공자의 공개키를 얻을 수 있다.

Here, the cryptography system in which called the secret key performs the encoding and decoding to one key is meant. The coding speed is fast and it is advantageous for the encoding of many message of the amount. However the encoding and decoding are made of one key. Therefore only when the key management being downright and sending to the Internet service provider the Internet service provider use this secret key and the first encoded message can be decoded. The certificate of the Internet service provider and secret key is together bound with this kind of reason and it encrypts into the public key held in the certificate of the Internet service provider and second encoded message (the digital envelope, and the digital envelope) are produced. Of course, the then the certificate of the Internet service provider is encrypted by the private key of the certifying authority and the certificate of the Internet service provider is decoded using the public key of the certifying authority included in the certificate of the certifying authority which the user receives from the certifying authority and the public key of the Internet service provider held in the Internet service provider certificate can be obtained.

이와 같은 방법에 의해 인터넷 서비스 이용자에서 생성된 상기 제 1 암호화된 메시지와 제 2 암호화된 메시지는 네트워크를 통하여 인터넷 서비스 제공자에게 전송된다.

The first encoded message and the second encoded message generated with this kind of method in the Internet service client are transmitted through the network to the Internet service provider.

인터넷 서비스 제공자는 상기 제 1 암호화된 메시지와 제 2 암호화된 메시지를 수신하고, 상기 제 2 암호화된 메시지를 인터넷 서비스 제공자의 개인키를 이용하여 복호화시켜 인터넷 서비스 제공자의 인증서와 비밀키를 획득한다. 그다음, 상기 비밀키를 이용하여 상기 제 1 암호화된 메시지를 복호화하여 메시지 원본과 전자서명, 그리고 인터넷 서비스 이용자의 인증서를 획득한다. 그리고 나서, 이용자가 전송한 이용자의 인증서에 담겨진 이용자의 공개키를 이용해서 전자서명을 복호화시켜 제 1 메시지 다이제스트를 획득한다. 물론, 이때 이용자의 인증서는 인증기관의 개인키로 암호화되어 있고, 인터넷 서비스 제공자는 인증기관으로부터 수신한 인증기관의 공개키를 이용하여 상기 이용자의 인증서를 복호화함으로써 이용자의 공개키를 얻을 수 있다. 한편, 상기 제 1 암호화된 메시지를 비밀키로 복호화하여 얻어진 메시지 원문을 다시 해쉬함수를 이용하여 암호화시키므로써 제 2 메시지 다이제스트를 획득한다. 그리고 나서 인터넷 서비스 제공자는 상기 제 1 암호화된 메시지와 제 2 암호화된 메시지를 비교하는데, 해쉬함수는 다른 메시지를 암호화했을 때 같은 결론이 거의 나오지 않는다는 특징이 있기 때문에, 만약, 상기

The Internet service provider receives the first encoded message and the second encoded message and the second encoded message is decoded using the private key of the Internet service provider and the certificate and secret key of the Internet service provider are obtained. Next, the first encoded message is decoded using the secret key and the message original copy, the electronic signature and certificate of the Internet service client are obtained. And held in the certificate of the user which the user transmits the first message digest is obtained. Of course, the then the certificate of the user is encrypted by the private key of the certifying authority and the public key of the user can be obtained by decoding the certificate of the user using the public key of the certifying authority which the Internet service provider receives from the certifying authority. In the meantime, by the again encrypting the message text decoding the first encoded message to the secret key and is obtained using the hash function the second message digest is obtained. And the Internet service provid

비교된 제 1 메시지 다이제스트와 제 2 메시지 다이제스트가 다르다면, 메시지는 위조된 것이고, 정당한 이용자가 아닌 제 3자가 접근한 것을 의미하며, 제 1 메시지 다이제스트와 제 2 메시지 다이제스트가 동일하다면, 메시지는 위조되지 않은 것이고, 정당한 이용자에 의한 액세스임을 확인할 수 있다.

도 6은 인증서를 이용하여 이용자가 등급별 인터넷 서비스에 로그인하는 과정을 설명한다. 인터넷 서비스에 로그인한 이용자가 등급별 서비스에 액세스하면(단계 601), 제공자는 이전 단계에서 암호화된 메시지 복호화결과 획득된 이용자의 인증서를 판독하고(단계 602), 상기 인증서에 기재된 서비스 등급 정보에 기초하여 해당 이용자에게 상기 등급별 서비스 이용권한이 있는지를 판단하고(단계 603), 판단결과 이용권한이 있는 경우에는 등급별 서비스 로그인을 허용하고(단계 604), 이용권한이 없는 경우에는 등급별 서비스 로그인을 통제한다(단계 605). 다만, 인터넷 서비스 로그인시 이용자가 액세스하려는 해당 서비스가 등급별로 분류된 것이라면, 도 4에서 정당한 사용자인지를 판단(단계 408)하고 나서, 정당한 사용자인 경우에 이용자의 인증서를 판독(단계 602)하여 등급별 서비스 로그인 허용 또는 통제를 행하게 될 것이다.

도 7은 인증기관으로부터 인증서를 발급받은 이용자 또는 제공자가 인증서를 폐기하는 과정을 보여주는 흐름도이다. 이용자는 인증기관이 제공하는 인증서서비스 사이트에 접속하여(단계 701), 인증서 폐기 신청서를 인증기관으로 발송한다(단계 703). 인증기관은 인증서 폐기 신청서를 수신하고(단계 703), 상기 인증서 폐기 신청서를 발급한 이용자의 인증서를 해지목록에 포함시키고(단계 704), 상기 해지목록에 포함된 폐기 요청 인증서에 관한 정보를 인터넷 서비스 제공자에게 통보한다(단계 705). 상기 통보를 수신한 인터넷 서비스 제공자는 인증서 폐기 신청을 요청한 이용자를 이용자 목록에서 삭제한다(단계 706). 이와 같은 과정에 의해, 인증기관으로부터 발급받은 인증서는 폐기될 수 있다.

이용자가 인증기관으로부터 발급받은 인증서를 상기와 같이 폐기했거나 분실한 경우에, 다시 인증서를 발급받기를 희망하는 이용자는 인증서를 재발급받아야 하고 재발급받는 과정은 도 2에 도시한 바와 같이 인증서를 처음 발급받는 절차와 동일한 절차에 의해 이루어진다. 인증서의 유효기간이 도과한 경우에 이용자는 인증서를 갱신해야 하는데, 이때에도 인증서를 재발급받아야 하지만 이 경우에는

er compares the first encoded message and the second encoded message. It has the characteristic in which the outcome which the same when encoding the message in which the hash function was different nearly does not come out. Therefore the above-mentioned compared first message digest and the second message digest are different. The message is counterfeited and it means that the third party which is not just user approaches and the first message digest and the second message digest are identical with that. It is and the message is not counterfeited the just user can confirm being the access by the user.

Fig. 6 illustrates process where the user logs on using the certificate in by grade internet service. If the user logging on in the internet service accesses in by grade service (601 step), the certificate of the user in which the provider is obtained in the former step with the encoded message descrambling result is read (602 step) and it determine (603 step)s whether it has by grade service using authority based on the service grade information written in the certificate to the target user and by grade service log-on is allowed (604 step) in case it has *** using right and by grade service log-on is controlled in the case without the using right (605 step). But the target service which the user accesses in the internet service log-on is classified as by grade. If it is the case the just use authentication is played in fig. 4 with the determination (408 step). And yet in case of being the just user the certificate of the user is done with the read (602 step) and by grade service log-on acknowledgment or the control is performed.

Figure 7 is a flowchart showing the user which the certificate is issued from the certifying authority or the process where the provider discards the certificate. The user connects to the authentication service site (701 step) which the certifying authority provides and the certificate discard application is forwarded to the certifying authority (703 step). The certifying authority receives the certificate discard application (703 step) and the certificate of the user forwarding the certificate discard application is included in the termination list (704 step) and information about the discard request certificate included in the termination list is notified to the Internet service provider (705 step). The user in which the Internet service provider receiving the notice requests request for the certificate discard is deleted from the user catalogue (706 step). According to this procedure, the certificate issued from the certifying authority can fall into disuse.

It is made with the same procedure as the procedure as described above, of as shown in the process which in case discarded or it loses the user who desires to the certificate be again issued has to be issued again with the certificate and is issued again, the certificate issued to the user from the certifying authority being the certificate issued for the first time. The user has to renew the certificate in case the term of

인증서의 폐기, 분실의 경우와 달리 개인 정보를 다시 제공할 필요는 없다.

이상의 방법 중 각 과정들은 이 방법을 수행하기 위하여 그 순서가 바뀔 수 있다. 또한, 본 발명은 본 발명이 속하는 분야에서 다양한 변경, 수정이 당업자에 의해 행해질 수 있고, 본 발명은 상기 예시적으로 설명한 예들에 의해 한정되는 것이 아니며, 특허청구범위에 기재된 범위에 의해 한정된다.

validity of the certificate exceeds. It the even in this case has to be issued again with the certificate but there is no need to again provide the personal information to the discard of the certificate, and the case of the loss.

The order can be reversed in order to each process perform this method among the method described in the above. Moreover, the various change, and the correction can be performed in the field in which as to the invention, the invention belongs by the person skilled in the art and the invention is not restricted with examples which it illustratively illustrates but the field is restricted by the range written in the patent claim.

도면에 대한 간단한 설명

도 1은 본 발명이 이용되는 네트워크 시스템의 개략도.

도 2는 인터넷 서비스 이용자 및 인터넷 서비스 제공자에게 인증서를 발급하는 과정을 보여주는 흐름도.

도 3은 인증서에 기재되는 정보를 보여주기 위한 개략도.

도 4는 인증서를 이용하여 인터넷 서비스에 로그인하는 과정을 보여주는 흐름도.

도 5는 본 발명의 인증서, 개인키, 공개키를 이용하여, 암호화하고 복호화하는 방법을 보여주는 도면.

도 6은 인증서를 이용하여 등급별 인터넷 서비스에 로그인하는 과정을 보여주는 흐름도.

도 7은 인증서를 폐기하는 과정을 보여주는 흐름도.

Brief explanation of the drawing

The schematic diagram of the network system in which fig. 1 the invention is used.

Figure 2 is a flowchart showing the process of issuing the certificate to the internet service client and Internet service provider.

The schematic diagram in which fig. 3 shows the information written in the certificate.

Figure 4 is a flowchart showing the process of logging on using the certificate in the internet service.

Figure 5 is drawing showing the method for encoding using the certificate, the private key and the public key of present invention and decoding.

Figure 6 is a flowchart showing the process of logging on using the certificate in by grade internet service.

Figure 7 is a flowchart showing the process of discarding the certificate.

Disclaimer

본 문서는 특허 및 과학기술문헌 전용의 첨단 자동번역 시스템을 이용해 생성되었습니다. 따라서 부분적으로 오역의 가능성이 있으며, 본 문서를 자격을 갖춘 전문 번역가에 의한 번역물을 대신하는 것으로 이용되어서는 안 됩니다. 시스템 및 네트워크의 특성때문에 발생한 오역과 부분 누락, 데이터의 불일치등에 대하여 본원은 법적인 책임을 지지 않습니다. 본 문서는 당사의 사전 동의 없이 권한이 없는 일반 대중을 위해 DB 및 시스템에 저장되어 재생, 복사, 배포될 수 없음을 알려드립니다.

(The document produced by using the high-tech machine translation system for the patent and science & technology literature. Therefore, the document can include the mistranslation, and it should not be used as a translation by a professional translator. We hold no legal liability for inconsistency of mistranslation, partial omission, and data generated by feature of system and network. We would like to inform you that the document cannot be regenerated, copied, and distributed by being stored in DB and system for unauthorized general public without our consent.)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
26 June 2008 (26.06.2008)

PCT

(10) International Publication Number
WO 2008/076074 A1

- (51) International Patent Classification:
G07C 11/00 (2006.01) **G07C 9/00** (2006.01)
- (21) International Application Number:
PCT/SE2007/051042
- (22) International Filing Date:
19 December 2007 (19.12.2007)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
0602754-4 20 December 2006 (20.12.2006) SE
- (71) Applicant (for all designated States except US):
PHONIRO AB [SE/SE]; Rörekullsvägen 4, S-302 41 Halmstad (SE).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **KNUTSSON, Lars** [SE/SE]; Gagegatan 45 A, S-302 37 Halmstad (SE).
RUNESSON, Jonas [SE/SE]; Skolgatan 14, S-302 32

Halmstad (SE). **BLIDING, Olle** [SE/SE]; Fjärdingsstigen 13, S-302 51 Halmstad (SE). **KARLSSON, Johan** [SE/SE]; Prästgården Pl 1024, S-310 31 Eldsberga (SE).

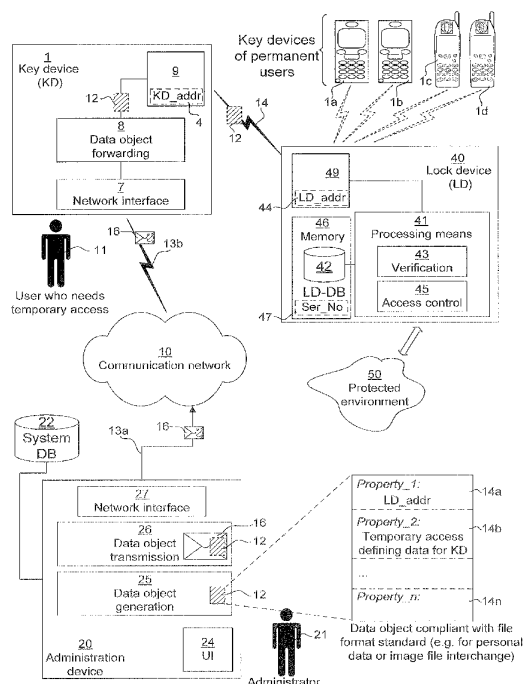
(74) Agent: **ANDERSSON, Björn**; Ström & Gulliksson AB, Box 4188, S-203 13 Malmö (SE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

[Continued on next page]

(54) Title: ACCESS CONTROL SYSTEM, LOCK DEVICE, ADMINISTRATION DEVICE, AND ASSOCIATED METHODS AND COMPUTER PROGRAM PRODUCTS



(57) Abstract: An access control system uses an existing file format standard, e.g. for personal data interchange (PDI) or image file interchange, for novel access control purposes to provide temporary access for a wireless key device to a lock device and its protected environment by creating appropriate temporary access defining data in a data object compliant with the file format standard and communicating the data object to the lock device via the wireless key device.



FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL,
PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

**ACCESS CONTROL SYSTEM, LOCK DEVICE, ADMINISTRATION DEVICE,
AND ASSOCIATED METHODS AND COMPUTER PROGRAM PRODUCTS**

5 Field of the Invention

The present invention relates to access control systems, and more particularly to an access control system in which a wireless key device can be provided temporary access to an environment protected by a lock device. The invention also relates to an associated lock device, an associated administration device for providing temporary
10 access to the lock device for a user of a wireless key device, as well as associated methods and computer program products.

Background of the Invention

WO 2006/098690 discloses an access control system in which users of wireless
15 key devices can get access to an environment protected by a lock device by means of short-range wireless data communication technology such as Bluetooth®. A lock device performs authentication of a wireless key device by checking, among other things, the Bluetooth® address of the key device.

The key devices of WO 2006/098690 are high-end mobile phones which are
20 provided with customized access control software for handling their appropriate authentication via short-range wireless data communication (Bluetooth communication) with the lock device. Using such mobile phones with customized software provides user-friendliness as well as a high degree of security thanks to a two-stage authentication procedure proposed in WO 2006/098690. It also allows for convenient updating of the
25 database of a particular lock device by using the customized access control software in the mobile phone as a relay station for forwarding lock device updating data in a secure manner from a remote administration device via a mobile telecommunications network.

Thus, in the solution of WO 2006/098690, if a new person is to be added as an allowed user for a certain lock device, one of two possible ways must be employed:

30 The first way is to provide the lock device in advance with database updating data which indicates the new user (or rather his mobile phone) as allowed. This may be done by bringing a special administration device close to the lock device for direct wireless data transmission of the updating data to the lock device, or it may be done by sending the updating data to another key device which will bring it to the lock device
35 when seeking access to it at some earlier point in time.

The second way involves using the particular new user's own mobile phone for bringing about the database updating data. In order for this to work, the user's mobile phone must at least have been upgraded in advance to include the required customized access control software, since this software is needed in order to perform a second-stage authentication during which upgrading of the lock device's database must take place.

Since both these ways require certain actions to be taken in advance, the system of WO 2006/098690 is less convenient when a new user only needs temporary access to a certain lock device. There may be many situations where a new user may need temporary access. One example is when a craftsman or repair man needs to access an apartment in order to repair or replace something in the apartment (e.g. a plumber repairing a pipe, or a glazier replacing a window pane). One difficulty for an administrator of an access control system of the kind used WO 2006/098690 when wanting to give temporary access for a new user, which only has a standard mobile terminal to use as key device, would be that the new user must inform the administrator about the Bluetooth® address of his mobile terminal. However, it is difficult for an ordinary user to find out the Bluetooth® address of the Bluetooth® transceiver in a mobile terminal.

Summary of the Invention

In view of the above, an objective of the invention is to solve or at least reduce the problems discussed above. More particularly, a purpose of the invention is to enable temporary access via a lock device to a protected environment in an access control system also for a user which does not possess a wireless key device which has been configured in advance for such purposes (for instance, having been provided with customized software for handling appropriate authentication via short-range wireless data communication with the lock device). Thus, the invention seeks to provide such temporary access by using standard wireless key devices such as mobile terminals that only contain standard mobile phone software but not any customized one for access control.

Generally, the above objectives and purposes are achieved by an access control system, a lock device and an administration device, as well as associated methods and computer program products, according to the attached independent patent claims.

A first aspect of the invention is an access control system including:
a lock device for a protected environment, said lock device comprising short-range wireless data communication means capable of short-range wireless data communication based on a communication identifier of said lock device;
5 a wireless key device having short-range wireless data communication means and data interchange means for communication of data objects compliant with a file format standard; and
an administration device comprising:
generator means for generating a data object in accordance with said
10 file format standard, a first property of said generated data object being assigned the communication identifier of said lock device, and at least a second property of said generated data object being assigned temporary access defining data for said key device to said environment protected by said lock device, and
15 transmitter means for transmitting said generated data object to said key device;
wherein said lock device further comprises:
processing means, associated with said short-range wireless data communication means, for processing said data object as received and
20 forwarded by said key device,
verification means for verifying that said first property of the received data object matches the communication identifier of the lock device, and
access control means, responsive to successful verification by said
25 verification means, for providing temporary access for said key device in accordance with said second property of the received data object.
The short-range wireless data communication means of the lock device may comprise a radio transceiver, preferably a Bluetooth® transceiver or another commercially available radio transceiver for one or more unlicensed RF communication
30 frequencies or frequency bands. In such embodiments, the communication identifier of the lock device may advantageously be the unique Bluetooth communication address which is assigned to every Bluetooth transceiver chip in conjunction with the manufacture thereof or later. As an alternative for such or other embodiments, the communication identifier of the lock device may be comprised by unique identifying
35 data which is included in the payload of the communication traffic to the lock device

and which is compared at the reception thereof with prestored reference data in order to determine that the communication traffic is intended for the particular lock device in question.

5 In one advantageous embodiment, the data interchange means of the wireless key device is in the form of personal data interchange means for communication of data objects compliant with a file format standard for personal data interchange. In this embodiment, accordingly, the generator means of the administration device is adapted for generating a data object in accordance with said file format standard for personal data interchange.

10 For such an embodiment, the file format standard for personal data interchange is advantageously selected from the group consisting of vCard, vCalendar, hCard, iCalendar, and any standard compatible therewith. This embodiment of the invention therefore uses an existing file format standard for personal data interchange (PDI) for a novel access control purpose to provide temporary access for a wireless key device to a lock device and its protected environment by creating appropriate temporary access
15 defining data in a data object compliant with the PDI file format standard and communicating the data object to the lock device via the wireless key device. Since the conveyed data object complies with an existing PDI file format standard, the only requirements put on the wireless key device are that it shall contain software (or other
20 functionality) compatible with the PDI file format standard and be capable of receiving and forwarding a data object in this PDI file format standard by means of a short-range wireless data communication means. There is no need for the wireless key device to have customized access control software installed.

In another advantageous embodiment of the invention, the file format standard
25 used for said data object by the data interchange means of the wireless key device and by the generator means of the administration device is a file format standard for media data interchange, preferably an image file interchange format standard such as JFIF ("JPEG File Interchange Format", Exif ("Exchangeable image file format") or TIFF ("Tagged Image File Format"), or any standard compatible therewith, or an audio or
30 video file interchange format standard, or any other predefined and commercially spread file format standard for data objects.

Since numerous kinds of portable communication devices like mobile terminals are compliant with PDI file format standards like vCard (Versitcard), hCard, iCalendar or vCalendar, and/or file format standards for media data interchange as mentioned
35 above, and furthermore have short-range wireless data communication means such as a

Bluetooth[®] radio transceiver, the wireless key device is advantageously a mobile terminal, such as a mobile phone or a personal digital assistant (PDA), suitable for telecommunication with a mobile telecommunications network compliant with for instance GSM, UMTS, D-AMPS, CDMA2000, FOMA or TD-SCDMA.

5 In one or more embodiments, the transmitter means of the administration device comprises a network interface to a communications network, for instance in the form of or including a mobile telecommunications network. The transmitter means also has means for including the generated data object in a digital message, such as an SMS ("Short Message Service", MMS ("Multimedia Messaging Service") or email message,
10 and for transmitting said digital message addressed to said wireless key device via said network interface over said communications network. Thus, the administration device may advantageously be a server computer or a mobile terminal.

Embedding the generated data object in a digital message represents a convenient transport channel for the generated data object from the administration
15 device to the wireless key device. This is particularly convenient when a mobile terminal is used as the wireless key device, since mobile terminals are very often provided with standard utility software which includes a messaging application and a contacts application. Therefore, such standard utility software in the mobile terminal will conveniently implement the required data interchange means of the wireless key
20 device, as referred to above, by allowing the mobile terminal user to receive the digital message from the administration device, temporarily save the embedded data object in the mobile terminal and then have it forwarded to the lock device by way of Bluetooth[®] communication.

A second aspect of the invention is an administration device for an access
25 control system which further includes a wireless key device and a lock device of a type having a short-range wireless data communication means capable of short-range wireless data communication based on a communication identifier of said lock device. The administration device comprises:

generator means for generating a data object in accordance with a file format
30 standard, a first property of said generated data object being assigned the communication identifier of said lock device, and at least a second property of said generated data object being assigned temporary access defining data for a wireless key device to an environment protected by said lock device, and

transmitter means for transmitting said generated data object to said key device.

The temporary access defining data, which is assigned by said generator means to said second property of said generated data object, may include temporal data which defines one or more time frames during which access is permitted for said key device to said protected environment. In one or more embodiments, such temporal data is
5 specified in a calendar data format, for instance in the form of one or more dates and/or times which define start and end points for permitted temporary access.

The temporary access defining data may include usage limitation data which defines how many times said key device is permitted to access said protected environment.

10 The generator means may be adapted to encrypt at least one of said first and second properties of said data object using an encryption key which includes said communication identifier of said lock device. This encryption key may also include a unique serial number of said lock device. Thus, in one embodiment, enhanced security is obtained by configuring the administration device to encrypt the contents of the
15 generated data object, using as encryption key the communication address (Bluetooth[®] address) of the lock device's radio transceiver as well as a serial No of the lock device, provided by its manufacturer and prestored in local memory of the lock device. This will eliminate any need for a separate communication of the decryption key from the administration device to the lock device.

20 It is to be noticed that the terms "first property" and "second property" as used above for the generated data object are to be interpreted openly without any specific limitations as regards the order of their actual appearance in the data structure of the generated data object. Thus, the "first property" can actually appear after the "second property" in the data structure, and the generated data object can have other properties
25 as well, which may appear before, after or between the "first property" and "second property". Moreover, the "first and second properties" need to be two properties only on a logical level; the data they are assigned may be physically stored in one common data field in the generated data object, or be distributed among a plurality of physical data fields.

30 It is also to be noticed that the "access control means [being] responsive to successful verification by said verification means", as specified for the lock device, shall not be construed in any more limiting way than to mean that a match between the first property of the received data object and the communication identifier of the lock device is a requisite for the lock device to be able to grant temporary access. Whether or
35 not such temporary access will be granted will in addition depend on the temporary

access defining data for the key device, as conveyed by the second property of the received data object.

- A third aspect of the present invention is a lock device for a protected environment in an access control system which further includes an administration device and a wireless key device, the lock device comprising:
- 5 short-range wireless data communication means capable of short-range wireless data communication with said key device based on a communication identifier of said lock device and capable of receiving from said key device a data object which originates from said administration device and complies with a file format standard;
 - 10 processing means, associated with said short-range wireless data communication means, for processing the received data object to derive a first property and a second property of the data object;
 - verification means for verifying that said first property matches the communication identifier of the lock device; and
 - 15 access control means, responsive to successful verification by said verification means, for providing temporary access for said key device in accordance with said second property.

- The processing means, verification means and access control means may be implemented in various different ways. In one embodiment, they are all implemented by
- 20 a processor which is programmed to provide the above-mentioned processing, verification and access control functionality. In other embodiments, these means may instead be implemented in hardware (e.g. as one or more application-specific integrated circuits (ASICs), or as one or more field programmable gate arrays (FPGA), or as basically any other available form of electronic logic circuitry configurable to perform
 - 25 the specified processing, verification and access control functionality.

In one or more embodiments, the processing means is configured to detect a communication identifier of the key device (such as its Bluetooth[®] address), wherein the access control means is configured to:

- create a database record for the key device,
 - 30 enter the detected communication identifier into the database record,
 - enter temporary access defining data, represented by the derived second property of the data object, for the key device into the database record, and
 - store the database record in a local access control database in the lock device.
- Creating a database record for the key device in a local access control database
- 35 in the lock device allows for multiple temporary accesses for the key device based on

just one transmission of a single data object in e.g. a digital message from the administration device via the key device to the lock device. The first time the key device connects to the lock device, the data object will be transmitted to the lock device, and the database record will be created. Provided that the temporary access defining data so permits, the key device will then be granted temporary access a first time to the lock device. Then, when the key device seeks access a second time to the lock device, there is no need to transmit a data object at this time, since a database record already exists for the key device in the lock device's local access control database. Therefore, on condition that the temporary access defining data of this database record so permits, the key device may be granted a second temporary access to the lock device by simply detecting the communication identifier (e.g. Bluetooth[®] address) of the key device.

To this end, to facilitate multiple temporary accesses in this way, the temporary access defining data (represented by the second property of the data object) may include usage limitation data which defines how many times the key device is permitted to access the protected environment.

The temporary access defining data may also include temporal data which defines one or more time frames during which access is permitted for the key device to the protected environment.

The processing means may be configured to decrypt at least one of said first and second properties of said data object using a decryption key which includes said communication identifier of said lock device. The decryption key used by said processing means may also include a unique serial number of said lock device.

In one or more embodiments, the processing means is further adapted to derive a third property of the data object in the form of a unique data object identifier set by the administration device, wherein the verification means is further adapted to verify that said third property matches one of a number of allowed unique data object identifiers which have been prestored in local memory in the lock device.

In addition, the verification means may be further adapted to delete or mark as consumed a matching one of the prestored unique data object identifiers so as to prohibit future use by a key device of a data object having the same data object identifier as said matching one in an attempt to obtain temporary access through said lock device to said protected environment.

Using prestored unique data object identifiers in this way to allow one-time use only of a certain data object will increase the security and counteract malicious repeated use of the same data object. This may be an important advantage particularly in

embodiments where the data object is conveyed in a digital message from administration device to key device (digital messages being easy to copy, relay or forward to other key devices than the receiver intended by the administration device).

Additional aspects of the invention relate to associated methods and computer
5 program products.

The additional aspects of the invention may have the same or corresponding features as any of the embodiments referred to above for the first, second or third aspect of the invention. Likewise, the access control system according to the first aspect may include any of the features of the administration device according to the second aspect
10 and/or the lock device according to the third aspect.

Other objectives, features and advantages of the present invention will appear from the following detailed disclosure, from the attached dependent claims as well as from the drawings.

Generally, all terms used in the claims are to be interpreted according to their
15 ordinary meaning in the technical field, unless explicitly defined otherwise herein. All references to "a/an/the [element, device, component, means, step, etc]" are to be interpreted openly as referring to at least one instance of said element, device, component, means, step, etc., unless explicitly stated otherwise. The steps of any method disclosed herein do not have to be performed in the exact order disclosed,
20 unless explicitly stated.

Brief Description of the Drawings

The above, as well as additional objectives, features and advantages of the present invention, will be better understood through the following illustrative and non-
25 limiting detailed description of embodiments of the present invention, reference being made to the appended drawings in which:

Fig 1 is a schematic illustration of an access control system, including an administration device, a wireless key device and a lock device,

Fig 2 is a schematic front view illustrating a wireless key device according to
30 one embodiment,

Fig 3 is a schematic block diagram illustrating internal components and modules of a lock device according to one embodiment,

Fig 4a illustrates a data structure for a data object which is compliant with a file format standard for personal data interchange and which may be used for providing
35 temporary access for the key device to an environment protected by the lock device,

Fig 4b gives an example of a data object generated in accordance with the data structure of Fig 4a,

Fig 5a is a flowchart diagram of a method performed by the administration device to assist in providing temporary access for the key device,

5 Fig 5b is a flowchart diagram of a method performed by the key device to assist in providing temporary access for the same,

Fig 5c is a flowchart diagram of a method performed by the lock device to assist in providing temporary access for the key device, and

10 Fig 6 is a flowchart diagram which illustrates an access control method performed by the lock device according to one embodiment.

Detailed Description of Embodiments

Generally, in the exemplifying access control system of Fig 1, a user 11 needs temporary access to an environment 50 protected by a lock device 40. An administrator
15 21 can make this temporary access possible by creating, with the aid of an administration device 20, appropriate temporary access defining data for the user 11 and have it communicated to a wireless key device 1 which the user 11 is in possession of. The user 11 will then use his wireless key device 1 to forward the received temporary access defining data wirelessly to the lock device 40, which upon processing of the
20 temporary access defining data may take the necessary actions to grant the intended temporary access for the user 11 to the protected environment 50.

The protected environment 50 may for instance be a room, apartment, commercial or public premises, garage, cabinet, locker, etc, with a controllable physical access interface in the form of a lockable door, garage port, hatch, etc. To this end, the
25 lock device 40 will be integrated with or coupled to a lock mechanism in the lockable door or garage port and in particular have a controllable lock actuator configured to unlock the lock mechanism upon detection and successful authorization of the key device 1, based on the temporary access defining data, or another key device which already has been defined in the lock device 40 as authorized to access the protected
30 environment 50 (see "key devices 1a-1d of permanent users" in Fig 1). One possible lock actuator is shown in the afore-mentioned WO 2006/098690 and involves an electromechanical arrangement with an electric step motor, but various other arrangements are of course also possible within the context of the present invention.

The structure and functionality of the administration device 20, key device 1 and
35 lock device 40 will now be described in more detail in the following.

In the disclosed embodiment, the administration device 20 is a computer, such as a personal computer, workstation or server computer, having a user interface 24 in the form of input devices such as keyboard and mouse, an output device such as a display (e.g. liquid crystal display monitor or cathode ray tube monitor), and an operating
5 system with a graphical user interface (GUI). In other embodiments, the administration device 20 may for instance be a mobile terminal.

The administration device 20 has access control administration software by means of which the administrator 21 may control which users (or more specifically which key devices held by such users) that shall have access to the protected
10 environment of the lock device 40, as well as of other lock devices if included in the access control system. Thus, the access control administration software may contain various functionality for controlling the access control rules for permanent users 1a-1d by communicating database upgrading data to the lock device 40 for storage in a local access control database 42 of the lock device 40. The afore-mentioned WO 2006/-
15 098690 discloses particulars of such database upgrading.

In addition, in line with the objectives of the present invention, the access control administration software in the administration device 20 includes a system database 22 as well as functionality for creating, packaging and transmitting the temporary access defining data for the key device 1 and its user 11 who is to get
20 temporary access to the lock device 40. In the disclosed embodiment, this functionality includes a data object generation module 25 which is configured to invite the administrator 21 to specify the temporary access defining data through interaction with the user interface 24.

The data object generation module 25 is configured to create a data object 12
25 which complies with an existing file format standard for communication of data objects. The disclosed embodiment uses the personal data interchange (PDI) standard vCard. Also see step 502 of Fig 5a. For more information on vCard, or on alternative PDI standards such as vCalendar, hCard and iCalendar, reference is made to the Internet Mail Consortium (<http://www.imc.org/pdi/>). A later section of this specification will
30 refer to an alternative embodiment which instead uses a file format standard for image file interchange.

The created data object 12 is then assigned the data which is necessary for the lock device 40 to be able to grant temporary access for the key device 1. Also see step 504 of Fig 5a. This necessary data includes a communication identifier ("LD_addr" in
35 Fig 1) of the lock device 40, and the temporary access defining data as specified by the

administrator 21 for the key device 1. The communication identifier ("LD_addr"), too, is conveniently specified or otherwise selected through interaction with the user interface 24. In the disclosed embodiment, the lock device 40 has short-range wireless data communication means 49 in the form of a Bluetooth® transceiver, and therefore the communication identifier specified in the created data object 12 in the administration device 20 is conveniently the Bluetooth® address 44 of the lock device's 40 Bluetooth® transceiver 49.

In the disclosed embodiment, this necessary data is included in the generated vCard 12 by assigning a first property 14a the communication identifier "LD_addr", and assigning a second property 14b the specified temporary access defining data. As seen more clearly in Figs 4a and 4b, the generated vCard 12 may contain additional properties, such as a Formatted Name 14c, a Unique Identifier 14d of the generated vCard, a Name 14e of the user 11, and a Checksum 14f of the data contained in the other properties.

In some embodiments, the data of some or all of the vCard properties 14a-14f may be encrypted by the data object generation module 25, preferably using as encryption key the communication identifier (Bluetooth® address) of the lock device's radio transceiver 49 and, optionally, also a serial No 47 of the lock device 40, the latter having been prestored in local memory 46 of the lock device by for instance the manufacturer.

In the disclosed embodiment of Figs 4a and 4b, the temporary access defining data assigned to the second vCard property 14b includes temporal data which defines one or more time frames during which access is permitted for the key device 1 to the protected environment 50. Such temporal data may be specified in a calendar data format, for instance in the form of one or more dates and/or times which define start point ("Valid_from") and end point ("Valid_to") for the temporary access permitted.

Additionally, in the disclosed embodiment, the temporary access defining data includes usage limitation data which defines how many times the key device 1 is permitted to access the protected environment 50. Such usage limitation data may for instance be in the form of a maximum counter value ("Max_usage"). When such a maximum counter value is used and is greater than 1, the lock device 40 will keep a counter value associated with the stored temporary access defining data for the key device 1 in the local access control database 42. Each time the key device 1 seeks access through the lock device 40, the lock device will check that the current counter value

permits temporary access in view of the maximum counter value, and increment the counter value each time temporary access is granted for the key device 1.

The administration device 20 also has a data object transmission module 26, associated with a network interface 27. The data object transmission module includes the generated data object 12 in a digital entity suitable for communication to the key device 1 over a communication network 10. Also see steps 506 and 508 of Fig 5a. In the disclosed embodiment, the data object transmission module 26 creates a digital message 16, such as an SMS, attaches the data object 12 (vCard) to this digital message and addresses it to the key device 1. The network interface 27 transmits the digital message 16 onto the communication network 10, as seen at 13a in Fig 1 and step 508 in fig 5a. The system database 22 is updated accordingly in step 510 of Fig 5a.

In the disclosed embodiment, the key device 1 is a mobile terminal (Fig 2), and at least part of the communication network 10 is a mobile telecommunications network compliant with for instance GSM, UMTS, D-AMPS, CDMA2000, FOMA or TD-SCDMA. The communication network 10 may in addition comprise a wide-area data communication network, for instance being a part of the Internet. Appropriate interface equipment is provided in the communication network 10 to allow forwarding of the digital message 16, as received from the network interface 27 of the administration device 20, to the key device 1, as seen at 13b in Fig 1.

As seen in Fig 2, in a familiar manner, the mobile terminal comprises an apparatus housing 201, a loudspeaker 202, a display 203, an input device 204a-c, and a microphone 205. In the disclosed embodiment, the input device 204a-c includes a set of keys 204a arranged in a keypad of common ITU-T type (alpha-numerical keypad), a pair of soft keys or function keys 204b, and a biometrical data reader 204c in the form of a fingerprint sensor. Hence, a graphical user interface 206 is provided, which may be used by a user of the mobile terminal to control the terminal's functionality and get access to any of the telecommunications services referred to above, or to any other software application executing in the mobile terminal.

Being a mobile terminal in the disclosed embodiment, the key device 1 also has a network interface 7 (Fig 1) in the form of cellular radio circuitry compliant with the mobile telecommunications network of the communication network 10. The key device also has data object forwarding functionality 8 capable of receiving the digital message 16 and forwarding the attached vCard data object 12 through short-range wireless data communication means 9 to the lock device 40, as seen at 14 in Fig 1 and in Fig 5b. In

the disclosed embodiment, the short-range wireless data communication means 9 is a Bluetooth® transceiver 9 having a Bluetooth® address 4 ("KD_addr").

Thus, the interface 7 and functionality 8 together constitute data interchange means capable of receiving the data object 12 with its included temporary access
5 defining data from the administration device 20 and forwarding the data object to the lock device 40 with the aid of the short-range wireless data communication means 9. In the disclosed mobile terminal embodiment of the key device 1, the mobile terminal comprises standard messaging and contacts handling software, in the form of a messaging application and a contacts application (or in the form of a combined
10 application for messaging and contacts). Thus, the steps to be performed in the key device 1 when receiving the digital message 16 are as shown in Fig 5b:

In step 512, the messaging application receives the SMS 16 from the administration device and detects the attached vCard 12. A new message alert is shown in step 514 to the user 11 on the display 203, advantageously showing the contents of
15 the Formatted Name property 14c (which may contain an explanatory text for the user 11 as seen in Fig 4b) and inviting the user 11 to save the attached vCard as a record in the Contacts application (step 516).

When the appropriate time comes to enter the protected environment 50, the user 11 will bring his wireless key device 1 to the correct lock device 40 and retrieve the
20 previously stored record in the Contacts application. By selecting an option like "Send by Bluetooth®", in step 520, the user 11 will cause the key device 1 to attempt to establish short-range data communication 14 with the lock device 40 in step 522 by making a Bluetooth® enquiry. First, however, there may be an optional wake-up stage 518, for the purposes which are described below.

25 In the disclosed embodiment, the lock device 40 is operable in a sleep mode and an operational mode. The purpose of the sleep mode is to keep as much as possible of the electronics in the lock device in a shut-off or disabled condition so as to minimize the power consumption during periods of inactivity. Therefore, as is also seen at 610 in Fig 6 as well as in Fig 3, the lock device of the disclosed embodiment has a wake-up
30 arrangement 320 capable of performing an initial wake-up step 532 in Fig 5c (see also steps 612-616 in Fig 6). During this wake-up step 532, the lock device 40 may be awoken and brought from its sleep mode into operational mode. The wake-up arrangement has a proximity sensor 324 positioned and configured to detect the presence of a user or key device near the lock device.

Whereas various different proximity sensors 324 are possible (including IR sensors, optical sensors, RF sensors, pressure sensors, and electrical switches), the disclosed embodiment of the lock device 40 uses an acoustic or vibration sensor 324 which is adapted to detect door knocks on a door to which the lock device 40 is mounted. Such a sensor may be provided in the form of a microphone which is attached via a spacer to the door leaf. The spacer will transfer vibrations caused by door knocks to the microphone. The wake-up arrangement 320 has circuitry 322 which is programmed or designed to apply predetermined wake-up criteria when deciding whether or not to generate a wake-up control signal 326 which will trigger the transition from sleep mode to operational mode. Such wake-up criteria may for instance be the detection of more than one door knock within a certain time frame. This may prevent an accidental wake-up because of a spurious detection of a non-related sound from the environment. Even more advanced wake-up criteria may be used, such as a given sequence of short and long door knocks, much like a code of Morse signals.

To this end, the disclosed embodiment of the lock device 40 is configured to react on a special door-knocking sequence which is to be used when a user like user 11 seeks temporary access by means of a key device, like key device 1, which is not known on beforehand to the lock device 40. This special door-knocking sequence is thus different from a normal door-knocking sequence which is to be used by permanent users of key devices 1a-1d.

Referring back to step 518 of Fig 5b, the user 11 is assumed to generate this special door-knocking sequence on the door of the lock device 40 sufficiently early, so that the lock device 40 will have time to wake up in step 532 of Fig 5c and enter its operational mode. Then, in step 534, the lock device responds to the Bluetooth® enquiry from the key device 1.

If more than one lock device respond to the Bluetooth® enquiry, the user 11 will be prompted to select the desired one in step 522.

Optionally, a pairing procedure may be performed between the key device 1 (step 524) and lock device 40 (step 536). Such a pairing procedure may increase the security and may therefore require the user 11 to enter a PIN or other verification on the key device 1. The lock device will verify in the optional step 536 that the PIN is correct before it allows any further communication with the key device 1. Such a PIN may have been communicated in advance from the administrator 21 to the user 11 over a separate channel, for instance during a voice call.

When a Bluetooth[®] link 14 has been duly established between the key device 1 and lock device 40, the data object (vCard) 12 will be transmitted by the key device 1 in step 526 and be received by the lock device 40 in step 538.

5 In a step 540, the lock device 40 detects the communication identifier (Bluetooth[®] address, "KD_addr") 4 of the key device 1.

The lock device 40 has processing means 41 for processing the received data object 12 in steps 542-552 of Fig 5c to derive its first property 14a and second property 14b, plus additional properties 14c-14f if applicable. If the data object was encrypted at the administration device 20, the processing means 41 performs decryption as has
10 already been described above.

Verification means 43 are provided for verifying that the first property 14a of the received data object 12 matches the communication identifier (Bluetooth[®] address, "LD_addr") 44 of the lock device in a step 544. If a Checksum property is used, the verification also includes verifying that the Checksum as derived from the property 14f
15 of the received data object 12 corresponds to a checksum calculated for the other properties in the received data object 12.

In case of verification failure, the execution ends in step 546, and otherwise it continues to step 548 where access control means 45 acts to provide the desired temporary access for the key device 1 by reading the temporary access defining data
20 represented by the second property 14b of the received data object 12. Then, in a step 550, a database record is created for the key device 1 in the lock device's local access control database 42. Data fields of this database record are filled with the key device's Bluetooth[®] address ("KD_addr") as detected in step 540, with the temporary access defining data, and with other appropriate data from the received data object 12, such as
25 the Name and Unique Identifier properties 14d and 14e. The database record is stored in step 552.

Now, in the disclosed embodiment, to actually let the user 11 into the protected environment 50, the execution proceeds by entering the normal access control authorization routine, which is normally used for permanent users, at step 612 in Fig 6 (if no
30 wake-up stage is used, the entry point may instead be at step 628, as indicated in Figs 5c and 6).

The access control authorization routine of Fig 6 will soon be described in detail. First, however, components of the lock device 40 according to the disclosed embodiment will be briefly described with reference to Fig 3.

The lock device 40 has a lock actuator 308 in the form of for instance an electric motor or a relay. The lock actuator 308 is coupled to a lock mechanism in a lockable door, garage port, etc, which forms a controllable entry to the protected environment 50. An actuator controller 307 is coupled to the lock actuator 308 and is adapted to provide
5 a control signal 307b for engaging or disengaging the lock actuator 308 to cause unlocking when appropriate.

In turn, the actuator controller 307 is controlled by a control signal 307a from a CPU 313 in the lock device 40.

The CPU 313 is programmed to read and execute program instructions stored in
10 a memory 311 so as to perform a method for wireless automatic unlocking in response to the appearance and proper authentication of a key device. The CPU may be identical to the aforementioned processing means 41, and the memory 311 may be identical to the aforementioned local memory 46.

The lock device 40 of this embodiment is a stand-alone, autonomously operating
15 device which requires no wire-based installations, neither for communication nor for power supply. Instead, the lock device 40 is powered solely by a local battery power unit 303 and interacts with the key device, as already mentioned, by Bluetooth®-based activities. To this end, the lock device 40 has a Bluetooth® radio module 309 with an antenna 310. The Bluetooth® radio module 309 may be identical to the aforementioned
20 communication means 49.

The lock device 40 of the disclosed embodiment further includes a real-time clock 304 capable of providing the CPU 313 with an accurate value of the current time.

The lock device 40 may have a simple user interface involving input device(s) 305 and output device(s) 312. In some embodiments, an authorized administrator may
25 configure the lock device 40 manually through this user interface.

Since the lock device 40 is a stand-alone, battery-powered installation which is intended to be operative for long time periods without maintenance, it is desired to keep power consumption at a minimum. Therefore, the disclosed embodiment is provided with the wake-up arrangement 320 which has already been referred to above.

Reference is now again made to the access control authorization routine of Fig 6.
30 On a general level, the method consists of two main authentication stages 620 and 640, and, in the present embodiment but optionally, the initial wake-up stage 610. The first authentication stage 620 is designed to be fast and therefore does not involve any establishment of a two-way Bluetooth® communication link between lock device and
35 key device.

In the first authentication stage, authorization is based solely on the key device's Bluetooth® address and the current time, both of which are detected automatically by the lock device 40 and require no interaction from the user (other than bringing the key device near the lock device 40). Certain users are entrusted to enter the protected environment simply through this first authentication stage 620, whereas other users must be authorized during the following, second and more extensive authentication stage 640 which requires establishment of a two-way Bluetooth® communication link and involves additional verification data from the key device 100 – for instance in the form of a PIN code or biometric data. Temporary users, such as user 11 of the key device 1, will also get access through the first authentication stage 620.

The lock device 40 bases its operation upon the authentication data (access control data) stored in LD-DB 42. In the present embodiment, the record structure of the LD-DB 42 includes the following data fields for authentication data:

Field	Contents example #1	Contents example #2
LD ID	121	121
User name	Lars	Jonas
Key device BT ID	0x00223af3	0x002e5af4
Stage-1 time slot (1)	2005-03-24: 19-22	
Stage-1 time slot (2)	Mon-Fri: 07-15	
...		
Stage-1 time slot (n)		
Stage-2 time slot – single		
Stage-2 time slot – scheduled	00-24	Sat-Sun: 10-18
PIN code	****	****
Administrator	No	No

In the example given above, it is thus configured that permanent user Lars is authorized for access through the lock device 40 having ID 121, by using his key device having Bluetooth® ID 0x00223af3 by fast stage-1 authentication during working days between 07:00 and 15:00. He was also granted a single stage-1 authority on 24 March 2005 between 19:00 and 22:00. If he arrives at the door outside of these stage-1 time slots, he may still access the door at any time (00-24), but in such a case he must go through a more complex stage-2 authentication which involves additional authorization, namely by providing a PIN code from the key device and having it communicated to the

lock device 40 over a two-way Bluetooth® communication link. Thus, stage-2 authentication requires a special software in the key device, since data exchange is involved. Therefore, if mobile terminals are used as key devices for permanent users, they are preferably of an advanced model provided with a suitable operating system, such as Symbian, at least for users that require stage-2 authentication.

As regards the PIN code, it may either be prestored in memory in the key device and fetched by the software therein upon communication to the lock device, or the software may invite the user to enter his PIN code manually on e.g. the keypad 204a upon establishment of the two-way Bluetooth® communication link. In other embodiments, if biometric data instead of PIN code is used as verification data, they are treated in the corresponding way, i.e. either prestored in memory or read by e.g. the fingerprint sensor 204c. It is to be observed that all communication between key device and lock device may be encrypted in accordance with an encryption algorithm, such as Blowfish. Therefore, data integrity is ascertained.

As for permanent user Jonas, only stage 2-authentication is available to him, and only on weekends between 10:00 and 18:00.

In addition to the exemplifying database records above and continuing with the use case example described above with reference to the preceding figures, the LD-DB 42 will also of course contain the database record created for temporary user Olle (see Fig 4b). This database record will, as previously explained, contain the temporary access defining data in the form of the time frame(s) for the permitted temporary access, as well as the maximum usage counter value if applicable.

With reference to Fig 6, assuming that the lock device 40 is in sleep mode, the initial wake-up stage 610 is performed in steps 612, 614 and 616 by using the proximity sensor 324 to detect the presence of the user of key device 1 near the lock device 40 and in response generate the wake-up control signal 326 to the CPU 313.

This causes the CPU 313 to enter the first authentication stage 620. A step 622 searches for Bluetooth®-enabled devices by paging, i.e. sending inquiry requests at regular intervals. Each Bluetooth®-enabled device within operating range (i.e. within a radius of some meters from the lock device 40, depending on e.g. the output power of the Bluetooth® radio module 309 and the performance of the Bluetooth® transceivers in the devices paged for) will transmit an inquiry response to the lock device. It is checked in step 624 whether at least one inquiry response is received within a time limit; if not a time out 626 occurs and the lock device 40 returns to sleep mode.

If an inquiry response was received, step 628 proceeds to determine the Bluetooth® address from the inquiry response. Moreover, a current time is determined by reading a value from the real-time clock 304.

Then, the CPU 313 proceeds in step 630 to check whether the determined Bluetooth® address of the responding device matches one of afore-described authentication data records in the LD-DB 42. In case of a match, it is also checked whether the current time falls within any stage-1 time slot defined for that Bluetooth® address. If the outcome of these checks is fully positive, as checked in step 632, the CPU 313 proceeds to step 634 and generates the control signal 307a to the actuator controller 307. As described above, this will cause unlocking of the lock, etc, and allow opening of the door, etc, to the protected environment.

If the check in step 632 reveals that the determined Bluetooth® address is not present in the LD-DB 42, or that the Bluetooth® address is present but the current time matches neither a stage-1 time slot nor a stage-2 time slot for that address, then no unlocking will take place, and the execution will return to step 622. In some embodiments it is possible to list certain undesired Bluetooth® addresses as explicitly forbidden in LD-DB 42. If the determined Bluetooth® address matches such a forbidden Bluetooth® address, appropriate action may be taken in a step 636, such as generating an alarm signal or registering the access attempt in memory 311 for later reporting.

If the check in step 632 reveals that the determined Bluetooth® address is present in the LD-DB 42, but that the current time does not fall within any stage-1 time slot defined for that Bluetooth® address but only within a stage-2 time slot, the execution proceeds to step 640.

In step 640, the CPU controls the Bluetooth® radio module 309 to establish a two-way Bluetooth® communication link with the key device detected in step 628. In step 642, data transmitted by the software in the key device is received in the lock device 40. Step 644 extracts verification data, such as a PIN code for key device, which as previously explained is included in the received data. Then, in step 646 it is checked whether the extracted verification data matches the corresponding authentication data stored for the key device's Bluetooth® address in LD-DB 42. In case of a match, step 648, the CPU 313 proceeds to step 650 and generates the control signal 307a to the actuator controller 307. Again, this will cause unlocking and allow the door, etc, to be opened.

Instead of a personal data interchange (PDI) standard like vCard, an alternative embodiment of the invention is based on a file format standard for image file inter-

change. In this embodiment, the data object generation module 25 of the administration device 20 is thus configured to create a data object 12 which complies with an existing image file interchange format standard such as JFIF ("JPEG File Interchange Format"), Exif ("Exchangeable image file format") or TIFF ("Tagged Image File Format").

- 5 Metadata tags available in accordance with the chosen image file interchange format standard may conveniently be used to implement the first property 14a of the image file object (for storing the communication identifier of the lock device 40), and the second property 14b (for storing the specified temporary access defining data). As non-limiting examples, the MakerNote tag may be used if the data object 12 is an Exif object,
- 10 whereas the thumbnail data field may be used if the data object 12 is a JFIF object, etc. As an alternative, new metadata tags may be defined and used, provided that the chosen image file interchange format standard so permits.

- Alternatively, the contents of some or all of the generated data object's 12 properties 14a-14n may be stored with the payload data of the data object (for instance embedded in the JPEG image data, when the data object 12 is a JFIF image object).
- 15 This may be useful if the chosen file format standard does not support metadata tags. It may also be used as a measure to improve security - if the data object's 12 properties 14a-14n are hidden as distributed data among JPEG image data representing a dummy image, it will be difficult for a third party to localize the positions in the image data
- 20 where the properties 14a-14n are stored and, thus, make manipulation attempts harder.

- An advantage of using a file format standard for image file interchange instead of personal data interchange is that less manual steps may be required by the user 11 in order to receive and forward the data object 12 in the message 16. In some mobile terminals, a received image can be forwarded directly from the inbox of the messaging
- 25 application, without having to store it temporarily in for instance a Contacts application.

- In one alternative embodiment, the access control system uses one-time tickets to enhance the security when it comes to providing temporary access. To this end, each lock device 40 is initially provided with a prestored set of one-time tickets, for instance 100 tickets. The system database 22 of the administration device 20 will keep track of
- 30 the one-time tickets as they have been used for each lock device 40. When a data object 12 is to be generated (step 504 of Fig 5a), the data object generation module 25 will determine the next available one-time ticket to use for the lock device 40 in question, and also include this particular one-time ticket in any of the properties 14a-14n of the data object 12. The one-time ticket may be represented as a sequence of hexadecimal
- 35 data (for instance the unique data object identifier 14d as described above for Figs 4a

and 4b), or it may be generated in a more sophisticated way as a function of one or more unique parameters of the lock device 40 in question, such as its communication identifier (e.g. Bluetooth[®] address 44) and the temporal data included in the temporary access defining data. Upon receipt of the data object 12, the lock device will derive the one-time ticket included therein and verify that it matches a valid (not already used) ticket in the prestored set of one-time tickets (steps 542-544 of Fig 5c). The lock device 40 will then scrap (e.g. delete or marked as used) the particular one-time ticket from the prestored set, so that it cannot be used again for a future temporary access to this particular lock device 40. Security may be enhanced further by requiring that the one-time tickets be used in sequential order (i.e., only one ticket (the one “first in line” among the non-used ones) will be valid at a time).

The invention has mainly been described above with reference to a few embodiments. However, as is readily appreciated by a person skilled in the art, other embodiments than the ones disclosed above are equally possible within the scope of the invention, as defined by the appended patent claims. Further, even if the disclosed embodiments use Bluetooth[®] for the short-range wireless data communication, another communication standard is also feasible, including but not limited to IrDA or a wireless local area network (WLAN) standard such as IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, HiperLAN2, WiMAX (IEEE 802.16), or HomeRF.

20

CLAIMS

1. An access control system including:
a lock device (40) for a protected environment (50), said lock device comprising
5 short-range wireless data communication means (49) capable of short-range wireless
data communication based on a communication identifier (44) of said lock device;
a wireless key device (1) having short-range wireless data communication means
(9) and data interchange means (7, 8) for communication of data objects compliant with
a file format standard; and
10 an administration device (20) comprising:
generator means (25) for generating a data object (12) in accordance
with said file format standard, a first property (14a) of said generated data
object being assigned the communication identifier (44) of said lock device
(40), and at least a second property (14b) of said generated data object being
15 assigned temporary access defining data for said key device (1) to said
environment (50) protected by said lock device, and
transmitter means for transmitting said generated data object to said
key device;
wherein said lock device (40) further comprises:
20 processing means (41), associated with said short-range wireless data
communication means (49), for processing said data object (12) as received
and forwarded by said key device (1),
verification means (43) for verifying that said first property (14a) of
the received data object (12) matches the communication identifier (44) of
25 the lock device, and
access control means (45), responsive to successful verification by
said verification means, for providing temporary access for said key device
(1) in accordance with said second property (14b) of the received data
object (12).
30
2. An access control system as defined in claim 1, wherein the short-range
wireless data communication means (49) of said lock device (40) comprises a radio
transceiver and wherein the communication identifier (44) of said lock device is a
unique communication address assigned to said radio transceiver.
35

3. An access control system as defined in claim 1 or 2, wherein said file format standard is a standard for personal data interchange selected from the group consisting of vCard, vCalendar, hCard, iCalendar, and any standard compatible therewith.

5 4. An access control system as defined in claim 1 or 2, wherein said file format standard is an image file interchange format standard selected from the group consisting of JFIF, Exif, TIFF, and any standard compatible therewith.

10 5. An access control system as defined in any preceding claim, wherein the transmitter means of said administration device (20) comprises
a network interface (27) to a communications network (10), and
means (26) for including said generated data object (12) in a digital message and for transmitting said digital message addressed to said wireless key device (1) via said network interface over said communications network.

15 6. An administration device (20) for an access control system which further includes a wireless key device and a lock device of a type having a short-range wireless data communication means (49) capable of short-range wireless data communication based on a communication identifier (44) of said lock device, the administration device comprising:

20 generator means (25) for generating a data object (12) in accordance with a file format standard, a first property (14a) of said generated data object being assigned the communication identifier (44) of said lock device (40), and at least a second property (14b) of said generated data object being assigned temporary access defining data for a
25 wireless key device (1) to an environment (50) protected by said lock device, and
transmitter means for transmitting said generated data object to said key device.

30 7. An administration device as defined in claim 6, wherein said file format standard is a standard for personal data interchange selected from the group consisting of vCard, vCalendar, hCard, iCalendar, and any standard compatible therewith.

35 8. An administration device as defined in claim 6, wherein said file format standard is an image file interchange format standard selected from the group consisting of JFIF, Exif, TIFF, and any standard compatible therewith.

9. An administration device as defined in any of claims 6-8, the transmitter means comprising
a network interface (27) to a communications network (10), and
means (26) for including said generated data object (12) in a digital message and
5 for transmitting said digital message addressed to said wireless key device (1) via said network interface over said communications network.

10. An administration device as defined in any of claims 6-9, wherein the temporary access defining data, which is assigned by said generator means (25) to said
10 second property (14b) of said generated data object (12), includes temporal data which defines one or more time frames during which access is permitted for said key device (1) to said protected environment (50).

11. An administration device as defined in any of claims 6-10, wherein the
15 temporary access defining data, which is assigned by said generator means (25) to said second property (14b) of said generated data object (12), includes usage limitation data which defines how many times said key device (1) is permitted to access said protected environment (50).

20 12. An administration device as defined in any of claims 6-11, wherein said generator means (25) is adapted to encrypt at least one of said first and second properties of said data object (12) using an encryption key which includes said communication identifier (44) of said lock device (40).

25 13. An administration device as defined in claim 12, wherein the encryption key used by said generator means (25) also includes a unique serial number of said lock device (40).

30 14. A lock device (40) for a protected environment (50) in an access control system which further includes an administration device (20) and a wireless key device (1), the lock device comprising:
short-range wireless data communication means (49) capable of short-range wireless data communication with said key device based on a communication identifier (44) of said lock device and capable of receiving from said key device a data object (12)

which originates from said administration device (20) and complies with a file format standard;

processing means (41), associated with said short-range wireless data communication means (49), for processing the received data object (12) to derive a first property (14a) and a second property (14b) of the data object (12);

verification means (43) for verifying that said first property (14a) matches the communication identifier (44) of the lock device; and

access control means (45), responsive to successful verification by said verification means, for providing temporary access for said key device (1) in accordance with said second property (14b).

15. A lock device as defined in claim 14,
wherein the processing means (41) is configured to detect a communication identifier of the key device (1), and
15 wherein the access control means (45) is configured to
create a database record for the key device (1),
enter the detected communication identifier into the database record,
enter temporary access defining data, represented by the derived second property (14b) of the data object (12), for the key device (1) into the database
20 record, and
store the database record in a local access control database (42) in the lock device (40).

16. A lock device as defined in claim 14 or 15,
25 wherein the derived second property (14b) of the data object (12) represents temporary access defining data for the key device (1) to the lock device, said temporary access defining data including usage limitation data which defines how many times said key device (1) is permitted to access said protected environment (50).

30 17. A lock device as defined in any of claims 14-16,
wherein the derived second property (14b) of the data object (12) represents temporary access defining data for the key device (1) to the lock device, said temporary access defining data including temporal data which defines one or more time frames during which access is permitted for said key device (1) to said protected environment (50).

35

18. A lock device as defined in any of claims 14-17, wherein said processing means (41) is configured to decrypt at least one of said first and second properties of said data object (12) using a decryption key which includes said communication identifier (44) of said lock device (40).

5

19. A lock device as defined in claim 18, wherein the decryption key used by said processing means (41) also includes a unique serial number of said lock device (40).

10

20. A lock device as defined in any of claims 14-19, wherein the processing means (41) is further adapted to derive a third property (14d) of the data object (12) in the form of a unique data object identifier set by the administration device (20), and

15

wherein the verification means (43) is further adapted to verify that said third property (14d) matches one of a number of allowed unique data object identifiers which have been prestored in local memory in the lock device.

20

21. A lock device as defined in claim 20, wherein the verification means (43) is further adapted to delete or mark as consumed a matching one of the prestored unique data object identifiers so as to prohibit future use by a key device of a data object having the same data object identifier as said matching one in an attempt to obtain temporary access through said lock device to said protected environment.

25

22. A method of providing temporary access for a wireless key device (1) to an environment (50) protected by a lock device (40), the method involving:

generating, in an administration device (20), a data object (12) in accordance with a file format standard;

30

assigning a communication identifier (44) of said lock device (40) to a first property (14a) of said generated data object;

assigning temporary access defining data for said key device (1) to at least a second property (14b) of said generated data object;

transmitting said generated data object from said administration device (20) to said key device;

35

receiving said data object (12) in said key device (1);

transmitting said data object (12) from said key device (1) to said lock device (40);

receiving said data object (12) in said lock device (40);

5 verifying that the first property (14a) of the received data object (12) matches the communication identifier (44) of the lock device; and

in response to successful verification by said verification means, providing temporary access for said key device (1) in accordance with the second property (14b) of the received data object (12).

10 23. A method in an administration device (20) for providing temporary access for a wireless key device (1) to an environment (50) protected by a lock device (40), the method comprising:

generating a data object (12) in accordance with a file format standard;

15 assigning a communication identifier (44) of said lock device (40) to a first property (14a) of said generated data object;

assigning temporary access defining data for said key device (1) to at least a second property (14b) of said generated data object; and

transmitting said generated data object to said key device.

20 24. A computer program product comprising program code which is loadable into a processor and executable to perform the method according to claim 23.

25 25. A method in a lock device for providing temporary access for a wireless key device (1) to an environment (50) protected by the lock device (40), the method comprising:

receiving from said key device a data object (12) which originates from an administration device (20) and complies with a file format standard;

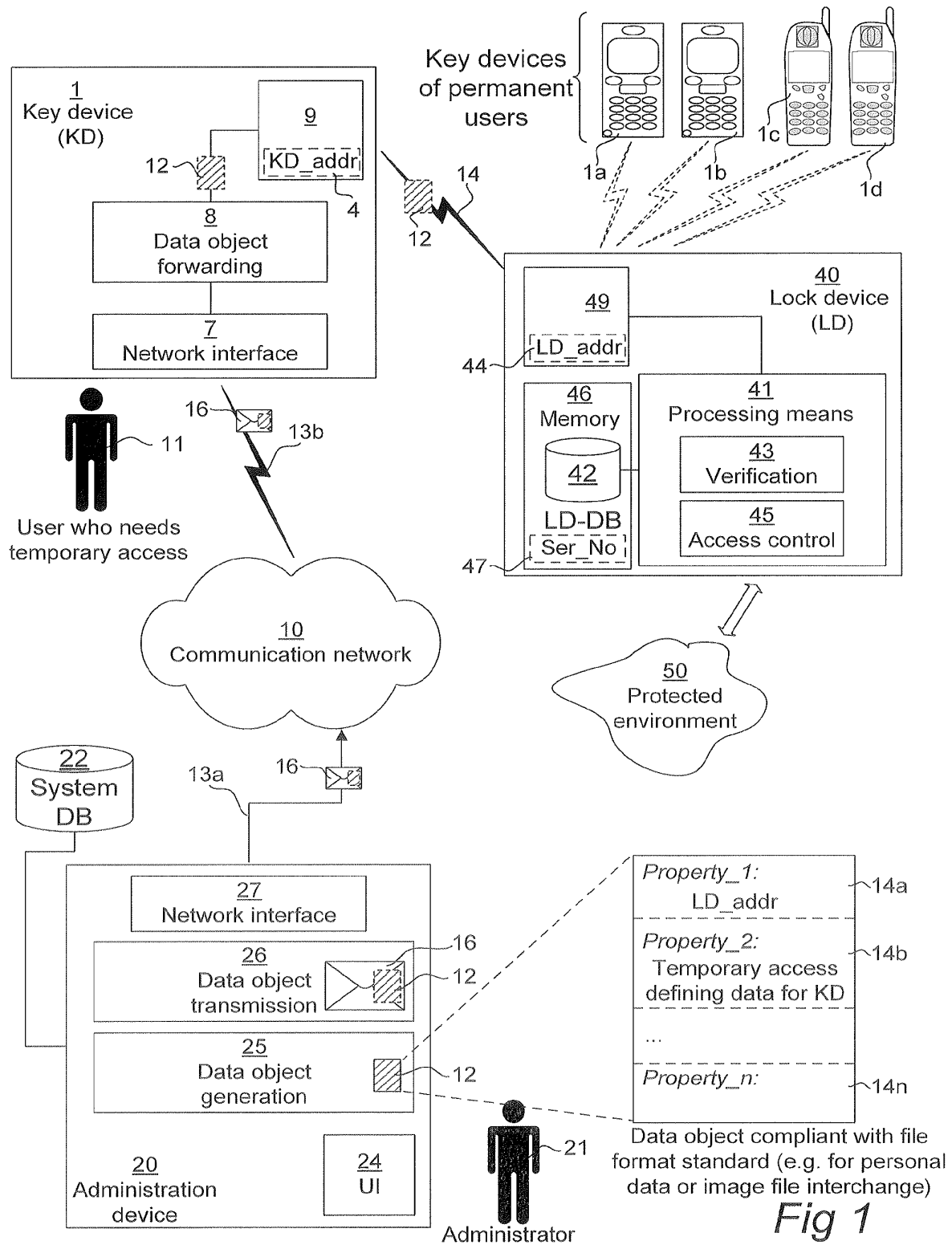
processing the received data object (12) to derive a first property (14a) and a second property (14b) thereof;

30 verifying that said first property (14a) matches a communication identifier (44) of the lock device; and

in response to successful verification, providing temporary access for said key device (1) in accordance with said second property (14b).

26. A computer program product comprising program code which is loadable into a processor and executable to perform the method according to claim 25.

1/6



2/6

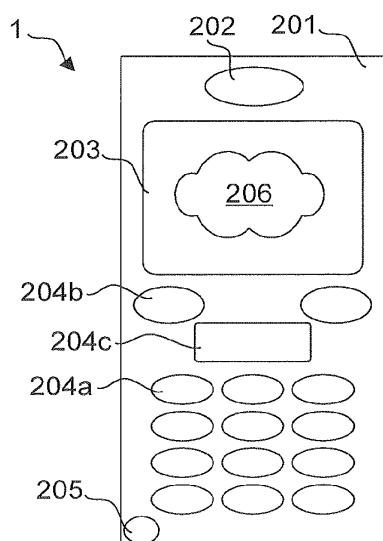


Fig 2

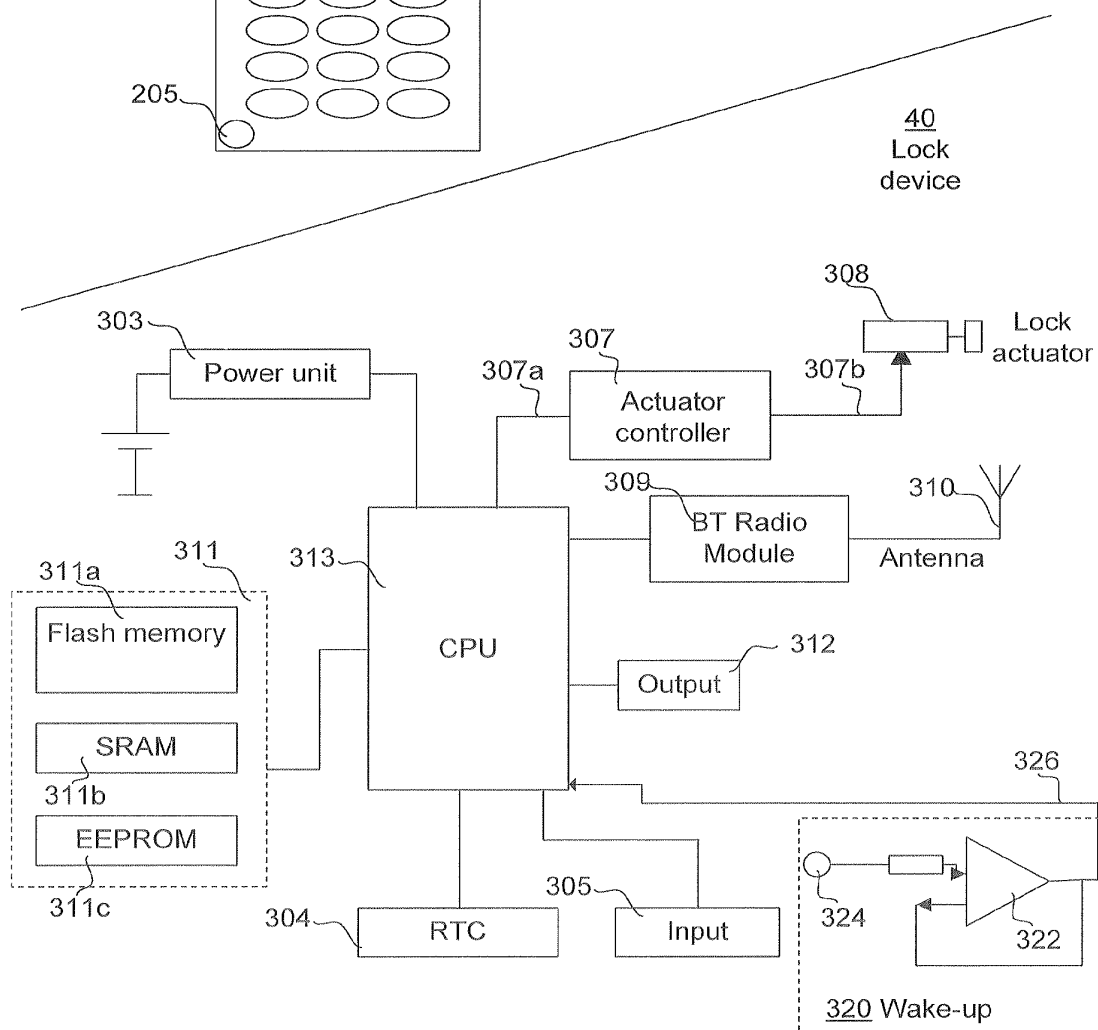


Fig 3

3/6

Structure of generated data object 12:

```

begin:vcard
14c~fn:Temp access for <user 11> to <LD 40>.
14d~uid:<Unique identifier for the generated vCard>
14a~x-phoniro;LD_addr:<Bluetooth address of lock device 40>
14e~x-phoniro;Name:<Name of user 11>
14b~{ x-phoniro;Valid_from:<Start date, Start_time>
      x-phoniro;Valid_until:<End date, End time>
      x-phoniro;Max_usage:<Integer value for maximum No of
      accesses available for user 11>
14f~X-phoniro;Checksum:<Checksum to prevent manipulation>
end:vcard

```

*Fig 4a*Example of generated data object 12:

```

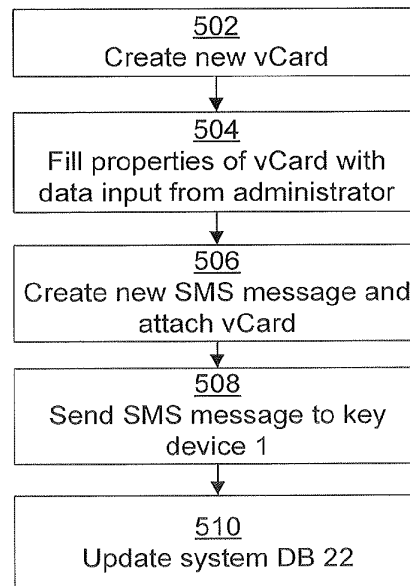
begin:vcard
14c~fn:Temp access for Olle to Elm Street 12.
14d~uid:20061127-099045-99990F192713-0052
14a~x-phoniro;LD_addr:0x00281ec3
14e~x-phoniro;Name:Olle
14b~{ x-phoniro;Valid_from:20061128,090000
      x-phoniro;Valid_until:20061128,150000
      x-phoniro;Max_usage:3
14f~X-phoniro;Checksum:1EA450FFC76D8233
end:vcard

```

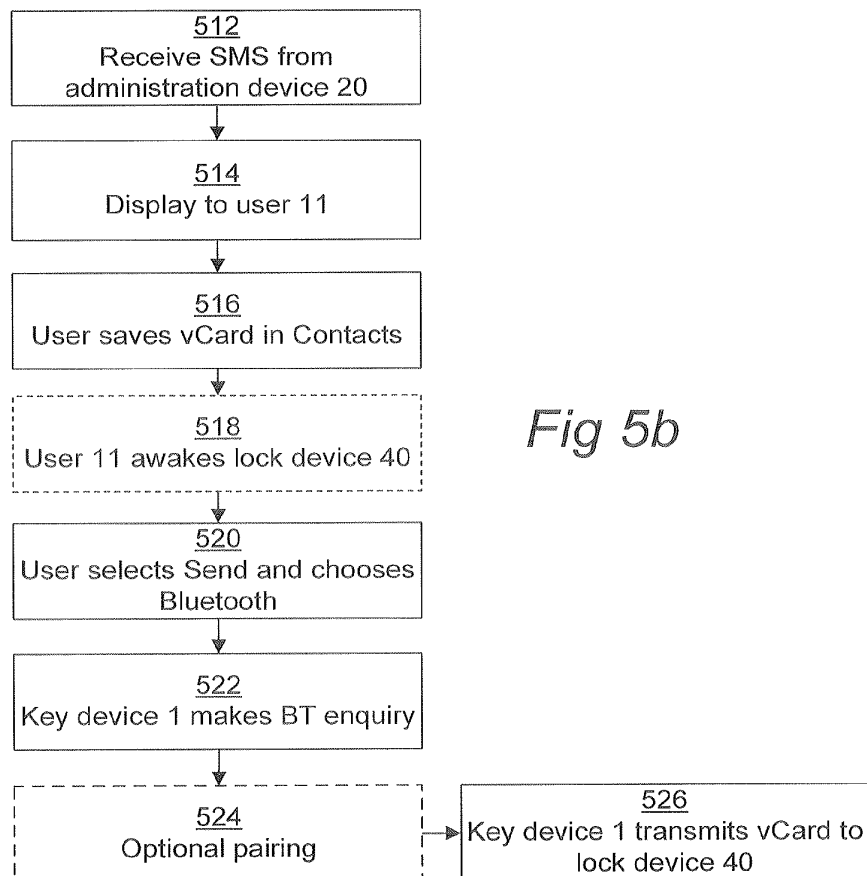
Fig 4b

4/6

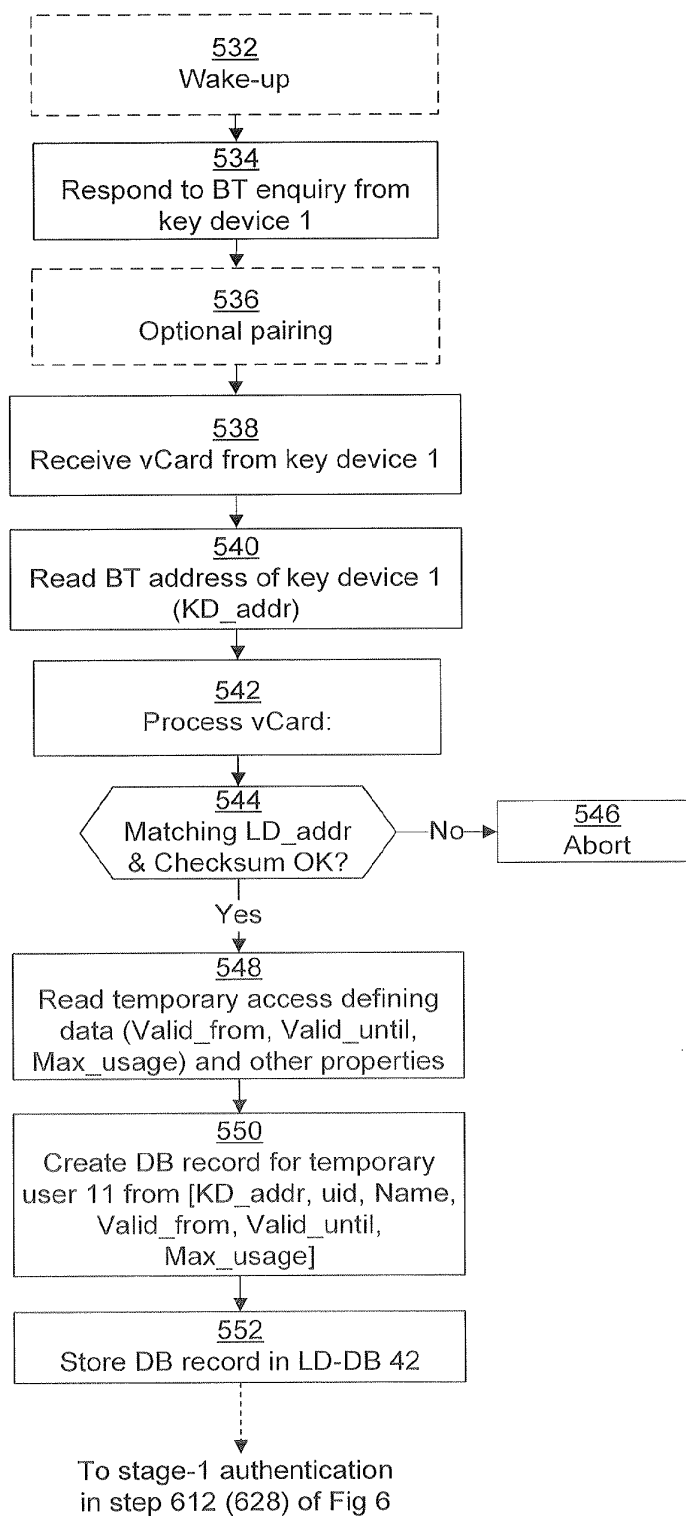
In administration device 20:

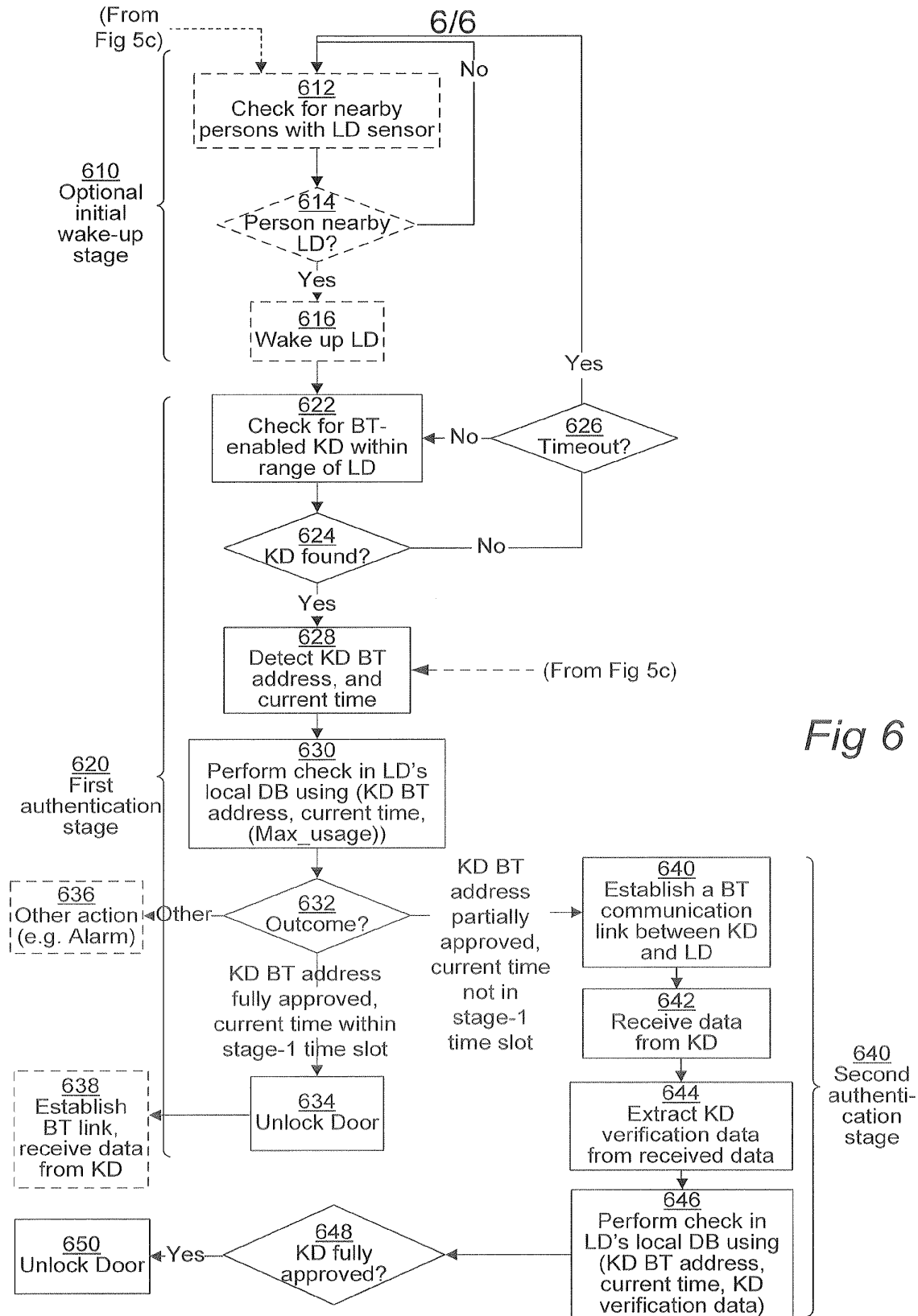
Fig 5a

In key device 1:

Fig 5b

5/6

In lock device 40:*Fig 5c*



INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE2007/051042

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet

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)

IPC: G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2364202 A (NOKIA MOBILE PHONES LTD.), 27 June 2000 (27.06.2000), page 2, line 4 - line 8; page 9, line 18 - line 20; page 12, line 23 - line 28 --	1-26
X	WO 0163425 A1 (TELEFONAKTIEBOLAGET LM ERICSSON(PUBL)), 30 August 2001 (30.08.2001), page 3, line 18 - page 4, line 37, abstract --	1-26
X	WO 2005080720 A1 (MIKAELWILLGERT), 1 Sept 2005 (01.09.2005), figure 1, abstract --	1-26

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 8 April 2008	Date of mailing of the international search report 10-04-2008
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Karin Jansdotter / itw Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE2007/051042

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 0231778 A1 (NOKIA CORPORATION), 18 April 2002 (18.04.2002), abstract --	1-26
X	WO 02095689 A1 (ERICSSON INC.), 28 November 2002 (28.11.2002), abstract --	1-26
A	WO 2006098690 A1 (PHONIRO AB), 21 Sept 2006 (21.09.2006), figure 1, abstract -- -----	1-26

Form PCT/ISA/210 (continuation of second sheet) (April 2007)

International patent classification (IPC)**G07C11/00** (2006.01)**G07C 9/00** (2006.01)**Download your patent documents at www.prv.se**

The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

Use the application number as username.

The password is **QHQFNAMIHT**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

INTERNATIONAL SEARCH REPORT
Information on patent family members

26/01/2008

International application No.
PCT/SE2007/051042

GB	2364202	A	27/06/2000	GB	0015716	D	00/00/0000
				US	20020031228	A	14/03/2002
WO	0163425	A1	30/08/2001	AT	330283	T	15/07/2006
				AU	3257301	A	03/09/2001
				DE	60120644	D,T	24/05/2007
				EP	1257922	A,B	20/11/2002
				JP	2003524256	T	12/08/2003
				NO	314530	B	31/03/2003
				NO	20000941	A	27/08/2001
				US	7315823	B	01/01/2008
				US	20030208386	A	06/11/2003
WO	2005080720	A1	01/09/2005	CN	1946912	A	11/04/2007
				EP	1718826	A	08/11/2006
				JP	2007523283	T	16/08/2007
				SE	525104	C	30/11/2004
				SE	0400425	A	30/11/2004
WO	0231778	A1	18/04/2002	AU	9411501	A	22/04/2002
				EP	1325476	A	09/07/2003
				FI	20002255	A	14/04/2002
				US	20060072755	A	06/04/2006
WO	02095689	A1	28/11/2002	AU	2002308549	A	03/12/2002
				EP	1423826	A	02/06/2004
				US	7114178	B	26/09/2006
				US	20020178385	A	28/11/2002
WO	2006098690	A1	21/09/2006	EP	1859415	A	28/11/2007
				SE	0500616	A	19/09/2006
				US	20070229257	A	04/10/2007

(12) UK Patent Application (19) GB (11) 2 364 202 (13) A

(43) Date of A Publication 16.01.2002

(21) Application No 0015716.4

(22) Date of Filing 27.06.2000

(71) Applicant(s)
Nokia Mobile Phones Limited
 (Incorporated in Finland)
 Keilalahdentie 4, 02150 Espoo, Finland

(72) Inventor(s)
Kalle Karkas
Matti Kantola
Jaakko Paakkonen

(74) Agent and/or Address for Service
Page White & Farrer
 54 Doughty Street, LONDON, WC1N 2LS,
 United Kingdom

(51) INT CL⁷
E05B 49/00 // H04Q 7/32

(52) UK CL (Edition T)
H4L LECY LRAX L209 L215

(56) Documents Cited
GB 2202354 A **EP 0856624 A1**
EP 0810559 A2 **EP 0416792 A2**
WO 94/01963 A1 **WO93/14571 A1**

(58) Field of Search
 UK CL (Edition R) **E2A ABC , H4L LDA LDLX LECCP**
LECCX LECY LED LESF
 INT CL⁷ **E05B 49/00 , H04Q 7/32**
 Online Databases: **WPI, EPODOC, JAPIO, TXTUS1,**
TXTUS2, TXTEP1, TXTGB1, TXTWO1

(54) Abstract Title
Mobile phone for opening locks

(57) A mobile phone receives key information via a wireless link from a server and transmits it to a device such as a lock.. If the key information is determined by the lock to be valid, the lock opens. The mobile phone may communicate with the lock using the Bluetooth (RTM) standard. The mobile phone may receive the key information via an SMS message, WAP connection or Bluetooth (RTM) connection. The server may be associated with a hotel for providing a key code for a room. The mobile phone may receive additional information such as a time limit beyond which the key is not valid. The key information and additional information sent to the mobile phone may be encrypted. Alternative embodiments include wirelessly receiving a ticket for a sporting event, theatre or cinema, a key for a rental car or travel ticket. Key codes may be stored in the mobile phone memory or smart card and may require a PIN to gain access.

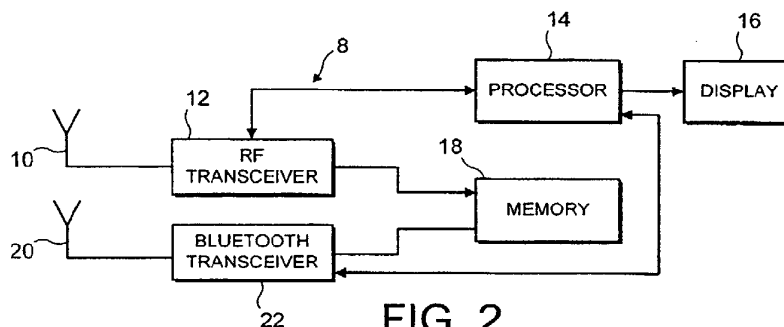


FIG. 2

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

1 / 3

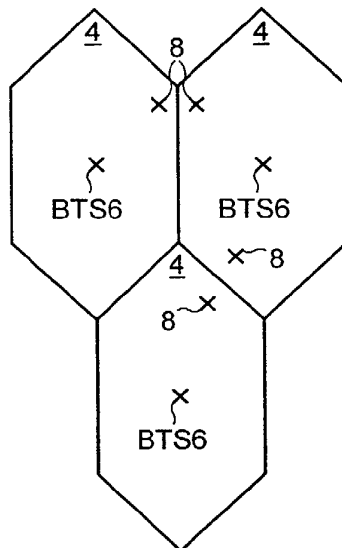


FIG. 1

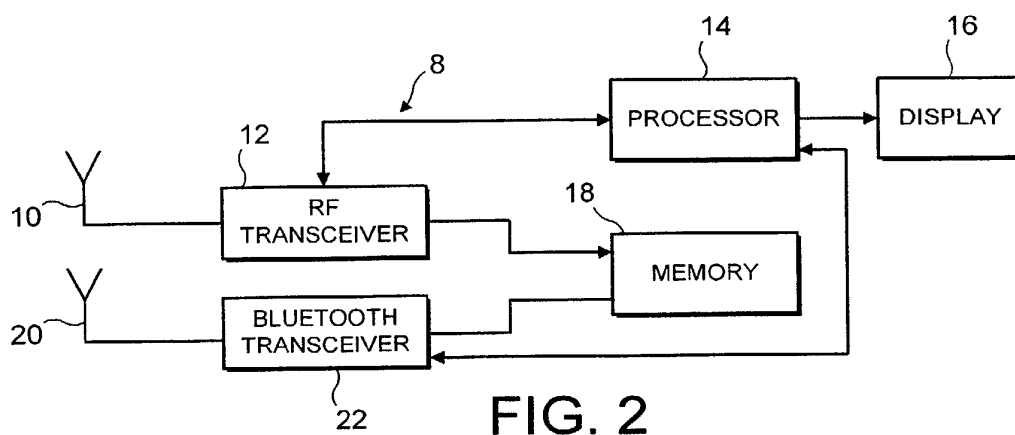


FIG. 2

2 / 3

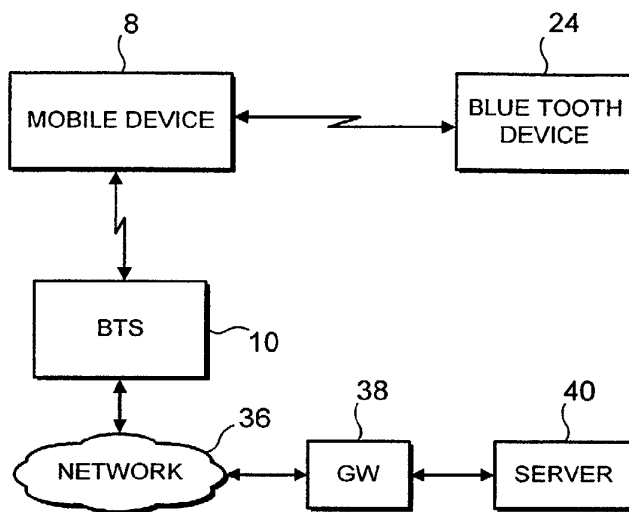


FIG. 3

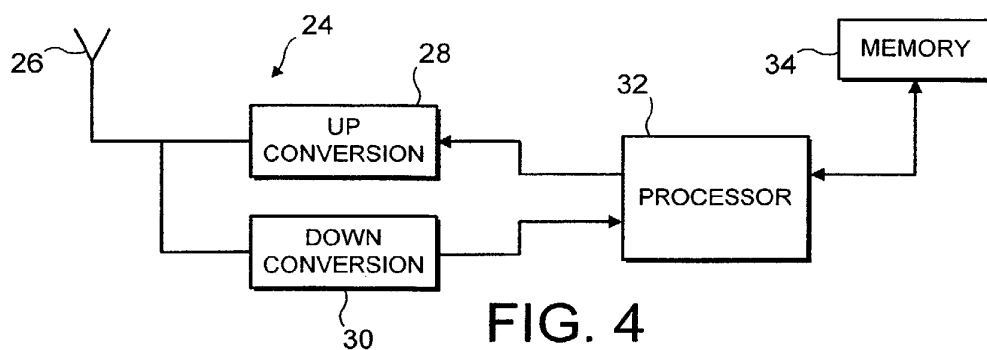


FIG. 4

3 / 3

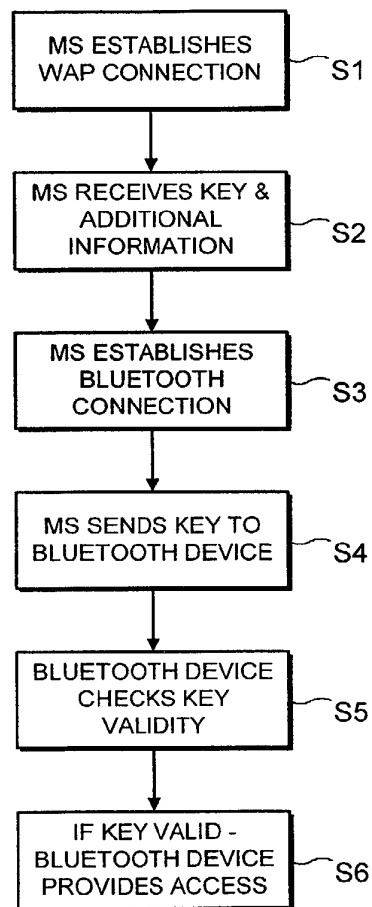


FIG. 5

2364202

1

DEVICES

The present invention relates to a device and in particular but not exclusively to a device which provides access to an entity.

5

Wireless cellular networks are known in which the area covered by the network is divided into a number of cells. Each cell is served by a base transceiver station. The base transceiver station is arranged to communicate with mobile stations in the cell associated with the base station. The mobile stations establish via the
10 base station a connection with another user, a fixed line telephone or the Internet.

Programmable keys are known. For example, plastic cards with magnetic strips are used as keys to open locks to for example doors or the like. The use of such keys is disadvantageous in that different keys are provided to access different
15 entities and therefore need to be carried by the user.

It has been proposed to allow multiple users access to the same entity. For example, a front door to an office may be accessed by a number of users or a hotel room may be accessed by different users at different times. It is necessary
20 for the accessed entity to have a database or similar to keep a record of the authorised users. It is disadvantageous if a database or similar needs to be associated with the accessed entity. For example, in a hotel, to have a database associated with each lock would be costly.

25 It is an aim of embodiments of the present invention to address one or more of the problems discussed earlier.

According to a first aspect of the present invention there is provided an access device comprising means for receiving a key and validity information, wireless
30 communication means for establishing a connection with another party, said wireless communication means being arranged to provide said key and said

validity information to said another party, wherein if said key and said validity information are determined by the another party to be valid access is provided.

5 According to a second aspect of the present invention there is provided an access method comprising the steps of receiving a key and validity information, establishing a wireless connection with another party, providing said key and said time related information to said another party, and checking at said another party if said key and said time related information are valid and if so providing access.

10 For a better understanding of the present invention and as to how the same may be carried into effect, reference will now be made by way of example to the accompanying drawings in which:-

Figure 1 shows a schematic diagram of a cellular network;

15 Figure 2 shows a block diagram of a mobile station embodying the present invention;

Figure 3 shows a block diagram of the entities with which the mobile station communicates;

Figure 4 shows the Bluetooth device of Figure 3 in more detail; and

20 Figure 5 illustrates the method embodying the present invention.

Reference is made to Figure 1 which shows a cellular network 2. The area covered by the network 2 is divided into a plurality of cells 4. Three cells 4 are shown in Figure 1. However, it should be appreciated that in networks there will
25 typically be many more cells.

Each cell 4 has associated therewith a base transceiver station 6. Each base transceiver station 6 is arranged to receive signals from and send signals to mobile stations 8 in the cell associated with the base station 6. Depending on the
30 method of communication, the mobile stations may communicate with the base stations of adjacent cells. In some embodiments of the present invention, a

mobile station may be able to communicate with two or more base stations at the same time.

The mobile stations and base transceiver stations typically use radio frequency signals to communicate. The base stations and mobile stations may use a frequency division multiple access technique. This means that the available frequency spectrum is divided up into a number of bands and the mobile station will be allocated a given frequency to communicate with the base station with the base station being allocated another frequency to communicate with the mobile station. Generally, the frequencies will be different but this is not essential. The mobile stations and the base stations may use a time division multiple access technique. With this method, a frequency band is divided up into a number of time slots and a mobile station is allocated a given one of those time slots to communicate with the base station and vice versa. In the GSM (global system for mobile communication) standard, a combination of frequency division multiple access and time division multiple access is used. Spread spectrum techniques such as code division multiple access may also be used. In this technique, different spreading codes are used by different mobile stations so that the signals from the different mobile stations can be distinguished. Similarly, the different base stations will use different spreading codes. In the third generation system, a wideband CDMA system has been proposed. It should be appreciated that in embodiments of the present invention, any of these techniques may be used either on their own or together. It is of course possible that any other suitable techniques may be used.

25

Reference is now made to Figure 2 which shows a block diagram of a mobile station embodying the present invention. The mobile station 8 has a first antenna 10. The first antenna 10 is arranged to receive signals from the respective base transceiver station 6. The first antenna 10 is also arranged to transmit signals to the base station 6.

30

The signals received by the first antenna 10 are forwarded to a radio frequency transceiver 12. The radio frequency transceiver 12 will down convert the radio frequency signals to a baseband frequency. The radio frequency transceiver may perform other functions such as decoding, demodulation or the like. The received
5 information at the baseband frequency is forwarded by the radio frequency transceiver 12 to a processor 14 which extracts the necessary information from the received signal. The processor 14 may be arranged to provide an output which is connected to a speaker which may provide received voice signals. The processor 14 may receive control information from the base station which is used
10 to control the mobile station or the like. The processor 14 may also extract information which is to be displayed and display that information on a display 16. The processor may also receive an input from a user interface such as a keyboard or the like.

15 The processor 14 is also used to process signals to be transmitted by the first antenna 10 and may also receive an output from for example a microphone or the like. The signals which are to be transmitted by the first antenna are output by the processor 14 at the baseband frequency. The radio frequency transceiver 12 upconverts the baseband signals to the radio frequency and forwards them to the
20 first antenna 10 for transmission. The radio frequency transceiver may encode the information, modulate it or carry out any other processing of the signal.

The radio frequency transceiver 12 may be connected to a memory 18. The memory 18 is arranged to store some information received by the radio frequency
25 transceiver. In alternative embodiments of the present invention, the memory may be connected to the processor 14 and so may receive information via the processor.

The mobile station 8 has a second antenna 20. The second antenna is arranged
30 to receive and transmit signals in the Bluetooth range of frequencies. Bluetooth is a standard which has been proposed for short range, low power, high frequency

signals. Typically, the signals will be of the order of giga Hertz. The second antenna 20 is arranged to receive Bluetooth signals from a Bluetooth device. The signals received by the second antenna are forwarded to a Bluetooth transceiver 22. The Bluetooth transceiver 22 performs similar functions to the radio frequency transceiver 12. In particular, the Bluetooth transceiver 22 downconverts the received signals to a baseband frequency. If required, the Bluetooth transceiver may demodulate and decode the received signal. The received signals may be forwarded to the processor 14 for further processing.

The Bluetooth transceiver 22 is also arranged to receive information from the processor 14. The received information is at the baseband frequency and the Bluetooth transceiver upconverts the signals to the Bluetooth frequency so that they can be transmitted by the second antenna. If required, the Bluetooth transceiver 22 will modulate, encode and perform any other required function.

The Bluetooth transceiver 22 is arranged to have access to the memory 18 and can retrieve information stored therein. In alternative embodiments of the present invention, the information may be retrieved by the processor from the memory and forwarded to the Bluetooth transceiver 22.

Reference will now be made to Figure 3 which schematically illustrates embodiments of the present invention. The mobile station 8 is arranged to have a Bluetooth connection with a Bluetooth device 24. This means that signals are exchanged between the mobile device and the Bluetooth device in accordance with the Bluetooth standard. With the Bluetooth standard, two devices are able to communicate directly without going via for example a base station.

In embodiments of the present invention, it is proposed that the Bluetooth device be a lock or an access device. For example, the Bluetooth device may be provided on a hotel door. The Bluetooth device may be part of an access device. For example, the access device 24 may permit access to a cinema, public

transport, a ski lift or the like. Alternatively, the Bluetooth device may for example be incorporated in a rental car or the like. Embodiments of the present invention are particularly suitable for allowing access to a given user temporarily. However, embodiments of the present invention can be used in other situations.

5

The communications between the mobile device and the Bluetooth device 24 are via the second antenna 20 of the mobile station 8.

Reference is made to Figure 4 which shows the Bluetooth device 24 of Figure 3 in
10 more detail. The Bluetooth device 24 has an antenna 26. This antenna 26 is arranged to receive and transmit signals at the Bluetooth frequency. More particularly, the antenna 26 is arranged to transmit signals to the second antenna of the mobile station and to receive signals therefrom. The Bluetooth device has an upconverter 28. The upconverter 28 is arranged to upconvert signals from a
15 baseband frequency to the Bluetooth frequency for transmission by the antenna 26. The upconverter 28 may carry out other functions such as modulation, encoding or any other suitable function.

The signals which are received by the antenna 26 are processed by a
20 downconverter 30 which reduces the frequency of the received signals from the Bluetooth frequency to the baseband frequency. Again, the downconverter 30 may perform other functions such as demodulation or decoding.

The signals which are received by the antenna 26 and down converted by the
25 downconverter 30 are output to a processor 32 which is able to process the received signals further. Likewise, the processor 32 is arranged to output those signals which are to be transmitted to the upconverter 28. The Bluetooth device 24 also has a memory 34 which is used to store information. This will be described in more detail hereinafter.

30

Referring back to Figure 3, the mobile station is also able to communicate with the base transceiver station 6 using the first antenna 10. The base transceiver station provides a connection to other elements of a network 36. The network 36 is connected to a gateway element 38 which, usually is part of the network 36.

- 5 The gateway element 38 allows the network to be connected to an external entity, such as another network, the Internet or a server 40 of a service provider.

Reference will now be made to Figure 5 which shows a flow diagram of the steps of the method embodying the present invention and illustrates how embodiments of the present invention work. The mobile station 8 is arranged in step S1 to establish a connection with the network 36 via the base transceiver station 10. In the embodiment described, the mobile station is a WAP (wireless application protocol) mobile station. However, it should be appreciated that the mobile device may be in accordance with any other protocol and may for example be able to use the short message servicing SMS feature in embodiments of the invention. The network is also arranged to establish via the gateway 38 a connection with a server. This server 40 is associated with the service provider. For example, if embodiments of the present invention are to be used to allow access to hotel rooms, then the server 40 would be associated with the hotel. As an alternative the mobile station 8 could also access the server provider via a Bluetooth transceiver connected to the server. In this way the mobile station can get the key over the Bluetooth connection without the need for network connection. Cost would also be reduced. If however an order for a service(for example a hotel room) was made in advance the key could be obtained remotely via the base transceiver station 10 using WAP or SMS.

In the second step S2, the server 40 provides the mobile station with key information and additional information. For example, in the context of a hotel, the additional information could take the form of the hotel room. In this particular embodiment, the key and additional information are downloaded to the mobile station in the same call where the mobile station establishes the connection.

However, in alternative embodiments of the present invention, it is possible that the mobile station in step 1 establish a WAP connection and provides an indication to the server as to the particular service required. The server may then cause the mobile station to be called back with the required key and additional
5 information.

The key information which is sent to the mobile station is usually encrypted. The whole of the key may be encrypted or only part of the key may be encrypted. In alternative embodiments of the present invention, the key may not be encrypted.
10 If the key is encrypted, the mobile station may be able to decrypt all or part of the key information. However, in preferred embodiments of the present invention, the mobile station is not able to decrypt the key information. The additional information which is sent to the mobile station may also be encrypted but this is not necessary. Where this additional information is encrypted, the mobile station
15 will usually be able to decrypt that information. For example, if the additional information relates to a room key, the user will need to know which hotel room the user is allowed access to. This additional information may be communicated to the user. For example, the information may be displayed on the display or may take the form of a voice message. Once the additional information has been
20 received by the mobile station, the connection with the server 40 is terminated.

In the next step, step S3, the mobile station is arranged to establish a Bluetooth connection with the Bluetooth device 24. The connection with the Bluetooth device 24 can take place some time after the first two steps are being completed.
25 As indicated previously, Bluetooth is a standard which has been proposed to permit the direct communication between two devices. One feature of the Bluetooth standard is that each packet is transmitted with a different frequency.

Once the Bluetooth connection has been established, in step S4 the mobile
30 station sends the key information to the Bluetooth device. This may be in response to a request from the Bluetooth device for the key.

In step S5, the Bluetooth device will check the validity of the key. In particular, the Bluetooth device attempts to decrypt the keys and will compare it with key information which it has stored thereon.

5

In step S6, if the key is valid, then the Bluetooth device 24 will provide access for example to the room.

10 In embodiments of the present invention, it is envisaged that the mobile station could be used to store more than one key. So that the Bluetooth device 24 is able to receive the correct key, it is preferred that each key has an identification tag which identifies the service provider. The Bluetooth device would in its request sent to the mobile station for the key include this information identifying the associated service provider. The mobile station would then only send the key(s)
15 which have the tag associated with the given service provider. Where a number of different keys are associated with the given service provider, the Bluetooth device could try all of the keys to see which one matches. It is of course possible in embodiments of the present invention that each Bluetooth device has a unique identity tag so that the mobile station only sends the key which matches that
20 identity tag provided by the Bluetooth device.

In alternative embodiments of the present invention, the mobile station may provide all of the keys which it has to the Bluetooth device which will then test all of them in order to determine which key is the correct key. This may be less
25 preferable in those embodiments where security is of importance.

The key may have a time limit beyond which it is not valid. For example, a hotel room key may be only valid for the time that the user stays in the hotel. Accordingly, in some embodiments of the present invention, time information may
30 form part of the key. Alternatively, there may be separate information provided relating to time information. The Bluetooth device, when determining if the key is

valid or not, will check to see whether or not the key is still valid. The time information may take any suitable format such as a start time and/or an end time or any other suitable format. For this, the Bluetooth device will require access to a clock. That may be part of the Bluetooth device itself or the information may be
5 provided by the mobile station.

In embodiments of the present invention, asymmetric encryption or symmetric encryption may be used. With symmetric encryption, the same key is used for encrypting as for decrypting. With asymmetric encryption, different keys are used
10 for encryption and decryption. For example, public and private keys may be used. Thus, the data may be encrypted with a public key which is well known and decrypted with a private key which is only known to a given user. It should be appreciated that any suitable form of encryption and decryption could be used.

15 In order to further increase the security, a hash code can be applied to the key data.

It should be appreciated that any suitable way of transmitting key data securely between the server, the mobile station and the Bluetooth device may be used. In
20 many of these forms the BTS and GW would not be needed.

In embodiments of the present invention, the mobile device has been described as being a mobile station. It should be appreciated that any suitable device can be used. For example, items such as wrist watches could be modified so as to
25 provide the functions of the embodiments of the present invention. Indeed, dedicated devices may be provided in order to perform the functions of embodiments of the invention. It has been proposed to provide a credit card type device which has the capability of making radio connections. Embodiments of the present invention may be incorporated in such devices.

30

In embodiments of the present invention, the mobile station has been described as using the Bluetooth protocol. However, in alternative embodiments of the present invention, different radio frequencies can be used. For example, infrared, wireless LAN and HomeRF could be used instead of the Bluetooth .

5

Embodiments of the present invention may be used in a wide range of situations. For example, the mobile station 8 may receive from the server a ticket for a sporting event, theatre or cinema. The mobile station may receive from the server a key which allows a rented car to be driven. The mobile station may receive
10 tickets which allow the user to travel on public transport such as aeroplanes, buses or trains. Embodiments of the present invention may be arranged to provide access to for example ski lifts. Embodiments of the present invention are particularly applicable to the provision of temporary access for example to a hotel or access to a cinema. However, embodiments of the present invention can be
15 used to permit a user to obtain access to more permanent services. For example, embodiments of the present invention can be arranged to allow a user to access their office or home.

The additional information will be appropriate for a particular service. In the
20 context of a hotel room, the additional information will take the form of the room number. In the case of car rental, the additional information will take the form of the registration number of the car and/or a reference. In the case of tickets to an event, the information may take the form of the seat information. The additional information may also provide time information. For example, the amount of time
25 for which a hotel room is available may be included. In embodiments of the present invention, the same technique can be used to obtain more user time. For example, in the case of a rental car the user may use the same technique in order to obtain a longer rental time.

30 In embodiments of the present invention, there is no need to connect each of the Bluetooth devices together to a central control element. This is because of the

provision of information relating to the time for which the key is valid. In the case of a lock, the key used by the lock does not have to be continually changed. For example, a hotel room may be validly opened by a user one day but if the user has not requested the room for an additional day, the user will not be permitted to enter that room on the next day. Thus, the need for additional infra structure connecting the Bluetooth devices can be avoided. The validity time for the key can be in the non-encrypted part of the key so that the mobile station can remove it automatically. Also this would allow the Bluetooth device to send a request to the mobile station to remove the key. As an alternative rather than a valid time information any other validity information indicating the validity of a user or validity of use of the item being accessed can be transferred. For example a maximum speed for a hire car during use could be stipulated.

The access key is stored in the memory 18 of the mobile station. Alternatively, the access key may be stored in an integrated part of the device for example on a smart card. The key information is also stored in the memory 34 of the Bluetooth device. Again, the information may be stored in any other suitable location in the Bluetooth device.

Mobile stations or devices embodying the present invention may store any number of different keys for different purposes.

In alternative embodiments of the present invention, the mobile station may be arranged to provide the Bluetooth device with user identification information. This may be part of the key or separate therefrom. This information can be used to provide additional security. For example, in the car rental situation, the user may be required to identify himself by entering a personal identification number code to prevent misuse or crime. Additionally the key may be stored in the part of the memory which requires the user to enter their personal identity number (PIN). Without the PIN the mobile station will not send the key. Additionally each key can be provided with its own PIN. The user needs to know the PIN in order to

use the key. The mobile station sends the key together with the PIN (the PIN could be, for example, part of the key for decryption). Furthermore no PIN might be required.

- 5 It is preferred that the validity time for the key be encrypted. This means that the mobile station can automatically delete those keys which are out of date.

The keys are preferably stored in a tamper proof memory which may be an ASIC, smart card or the like.

10

In alternative embodiments of the present invention, a single antenna may be provided in the mobile station and the key information and the like may be provided to the mobile station using the same antenna which is used to send the key information to the accessed entity. That single antenna may be arranged to

- 15 use the Bluetooth standard or the usual mobile station frequencies.

CLAIMS

1. An access device comprising:

means for receiving a key and validity information ;

5 wireless communication means for establishing a connection with another party, said wireless communication means being arranged to provide said key and said validity information to said another party, wherein if said key and said validity information are determined by the another party to be valid access is provided.

10

2. A device as claimed in claim 1, wherein said receiving means is arranged to receive additional information relating to the another party.

3. A device as claimed in claim 2, wherein said additional information is
15 available to a user of said access device.

4. A device as claimed in claim 3, wherein said device comprises a display and said display is arranged to display said additional information.

20 5. A device as claimed in claim 3 wherein said device comprises a speaker and said speaker is arranged to provide said additional information audibly.

6. A device as claimed in any preceding claim, wherein said means for receiving said key and validity information comprises a wireless communication
25 means.

7. A device as claimed in claim 6, wherein said wireless communication means for receiving said key and validity information operate at different frequencies to the wireless communication means for establishing a connection.

30

8. A device as claimed in any preceding claim, wherein said wireless communication means for establishing a connection uses high frequency signals of the order of giga Hertz.

5 9. A device as claimed in any preceding claim, wherein said wireless communication means for establishing a connection uses low power signals.

10. A device as claimed in any preceding claim, wherein said wireless communication means for establishing a connection uses Bluetooth signals.

10

11. A device as claimed in any of claims 1 to 9, wherein said wireless communication means for establishing a connection uses infra red signals.

12. A device as claimed in any preceding claim, wherein said device is
15 arranged to have more than one key at the same time.

13. A device as claimed in any preceding claim, wherein each key has an identifier associated therewith, said another party being arranged to provide identification information, said device being arranged to provide the or each key
20 which has the identifier associated with the received identification information to said another party.

14. A device as claimed in claim 13, wherein said identifier identifies a service provider.

25

15. A device as claimed in any preceding claim, wherein said device provides access to one or more of the following:

hotel room; theatre; cinema; hire car; ski lift; public transport; or office.

30 16. A device as claimed in any preceding claim, wherein said device comprises a memory for storing said key.

17. A device as claimed in any preceding claim, wherein at least part of said key and/or said validity information are at least partly encrypted.

5 18. A device as claimed in claim 17, wherein at least part of said key is not decryptable by said device.

19. A device as claimed in any preceding claim, wherein said device is arranged to provide to said another party information identifying the user of said
10 device.

20. A device as claimed in claimed in any preceding claim wherein said validity information comprises time related information.

15 21. An access system comprising a device as claimed in any of the preceding claims in combination with said another party.

22. A system as claimed in claim 21, wherein said another party comprises means for determining if the key and validity information received from said
20 access device are valid.

23. An access method comprising the steps of:
receiving a key and validity information ;
establishing a wireless connection with another party;
25 providing said key and said time related information to said another party,;
and
checking at said another party if said key and said time related information are valid and if so providing access.

30 24. A method as claimed in claim 23 wherein said validity information comprises time related information.

25. A device as claimed in any preceding claim, wherein said device is a mobile station.

Amendments to the claims have been filed as follows

CLAIMS

1. An access device comprising:

means for receiving, via a wireless communication link, a key and validity information;

5 wireless communication means for establishing a connection with another party, said wireless communication means being arranged to provide said key and said validity information to said another party, wherein if said key and said validity information are determined by the another party to be valid access is provided.

10

2. A device as claimed in claim 1, wherein said receiving means is arranged to receive additional information relating to the another party.

3. A device as claimed in claim 2, wherein said additional information is

15 available to a user of said access device.

4. A device as claimed in claim 3, wherein said device comprises a display and said display is arranged to display said additional information.

20 5. A device as claimed in claim 3 wherein said device comprises a speaker and said speaker is arranged to provide said additional information audibly.

6. A device as claimed in any preceding claim, wherein said means for receiving said key and validity information comprises a wireless communication
25 means.

7. A device as claimed in claim 6, wherein said wireless communication means for receiving said key and validity information operate at different frequencies to the wireless communication means for establishing a connection.

30

8. A device as claimed in any preceding claim, wherein said wireless communication means for establishing a connection uses high frequency signals of the order of giga Hertz.
- 5 9. A device as claimed in any preceding claim, wherein said wireless communication means for establishing a connection uses low power signals.
10. A device as claimed in any preceding claim, wherein said wireless communication means for establishing a connection uses Bluetooth signals.
- 10 11. A device as claimed in any of claims 1 to 9, wherein said wireless communication means for establishing a connection uses infra red signals.
12. A device as claimed in any preceding claim, wherein said device is
15 arranged to have more than one key at the same time.
13. A device as claimed in any preceding claim, wherein each key has an identifier associated therewith, said another party being arranged to provide identification information, said device being arranged to provide the or each key
20 which has the identifier associated with the received identification information to said another party.
14. A device as claimed in claim 13, wherein said identifier identifies a service provider.
- 25 15. A device as claimed in any preceding claim, wherein said device provides access to one or more of the following:
hotel room; theatre; cinema; hire car; ski lift; public transport; or office.
- 30 16. A device as claimed in any preceding claim, wherein said device comprises a memory for storing said key.

17. A device as claimed in any preceding claim, wherein at least part of said key and/or said validity information are at least partly encrypted.

5 18. A device as claimed in claim 17, wherein at least part of said key is not decryptable by said device.

19. A device as claimed in any preceding claim, wherein said device is arranged to provide to said another party information identifying the user of said
10 device.

20. A device as claimed in claimed in any preceding claim wherein said validity information comprises time related information.

15 21. An access system comprising a device as claimed in any of the preceding claims in combination with said another party.

22. A system as claimed in claim 21, wherein said another party comprises means for determining if the key and validity information received from said
20 access device are valid.

23. An access method comprising the steps of:
receiving, via a wireless communication link, a key and validity information;
establishing a wireless connection with another party;
25 providing said key and said time related information to said another party,;
and
checking at said another party if said key and said time related information are valid and if so providing access.

30 24. A method as claimed in claim 23 wherein said validity information comprises time related information.

25. A device as claimed in any preceding claim, wherein said device is a mobile station.



INVESTOR IN PEOPLE

Application No: GB 0015716.4
Claims searched: All

22

Examiner: Gareth Griffiths
Date of search: 15 December 2000

Patents Act 1977 Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:
UK Cl (Ed.R): E2A (ABC), H4L (LDA, LDLX, LECCP, LECCX, LECY, LED, LESF)
Int Cl (Ed.7): E05B 49/00, H04Q 7/32
Other: Online Databases: WPI, EPODOC, JAPIO, TXTUS1, TXTUS2, TXTEP1, TXTGB1, TXTWO1

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
X	GB2202354 A (SECURITY SERVICES) whole document	1-4,6,7,9,12,13,15-17,19-24
X	EP0810559 A2 (AT&T) whole document	1,6-9,15-17,19-23,25
X	EP0856624 A1 (VALEO) see WPI/EPODOC abstracts	1,6,9,15,16,21-23
X	EP0416792 A2 (TAYLOR) whole document	1-7,9,15,16,19,23
X	WO94/01963 A1 (ROZGONYI) p.4 line 24 - p.5 line 4	1,6,8,9,15,16,19,21-23,25
X	WO93/14571 A1 (SUPRA PRODUCTS) p.10 line 23 - p.14 line 25	1,6-9,11,12,15,16,20-24

X Document indicating lack of novelty or inventive step	A Document indicating technological background and/or state of the art.
Y Document indicating lack of inventive step if combined with one or more other documents of same category.	P Document published on or after the declared priority date but before the filing date of this invention.
& Member of the same patent family	E Patent document published on or after, but with priority date earlier than, the filing date of this application.



INVESTOR IN PEOPLE

Application No: GB 0015716.4
Claims searched: All

23

Examiner: Gareth Griffiths
Date of search: 18 July 2001

Patents Act 1977
Further Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:
 UK Cl (Ed.S): E2A (ABC), H4L (LDA, LDLX, LECCP, LECCX, LECY, LED, LESF)
 Int Cl (Ed.7): E05B 49/00, H04Q 7/32
 Other: Online Databases: WPI, EPODOC, JAPIO, TXTUS1, TXTUS2, TXTEP1, TXTGB1, TXTWO1

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
X	GB2202354 A (SECURITY SERVICES) whole document	1-4,6,7,9,12,13,15-17,19-24
X	EP0810559 A2 (AT&T) whole document	1,6-9,15-17,19-23,25
X	EP0856624 A1 (VALEO) see WPI/EPODOC abstracts	1,6,9,15,16,21-23
X	EP0416792 A2 (TAYLOR) whole document	1-7,9,15,16,19,23
X	WO94/01963 A1 (ROZGONYI) whole document	1,6,8,9,15,16,19,21-23,25
X	WO93/14571 A1 (SUPRA PRODUCTS) p.10 line 23 - p.14 line 25	1,6-9,11,12,15,16,20-24

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.



(11) **EP 1 783 694 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention
of the grant of the patent:
16.02.2011 Bulletin 2011/07

(51) Int Cl.:
G07C 9/00 (2006.01) H03K 17/955 (2006.01)

(21) Application number: **04742069.0**

(86) International application number:
PCT/ES2004/000341

(22) Date of filing: **21.07.2004**

(87) International publication number:
WO 2006/021592 (02.03.2006 Gazette 2006/09)

(54) **ELECTRONIC LOCK COMPRISING AN AUTOMATIC ACTUATION SYSTEM WHICH USES A CAPACITIVE PROXIMITY SENSOR**

ELEKTRONISCHES SCHLOSS MIT EINEM AUTOMATISCHEN BETÄTIGUNGSSYSTEM MIT EINEM KAPAZITIVEN PROXIMITÄTSSENSOR

VERROU ELECTRONIQUE AVEC SYSTEME D'ACTIVATION AUTOMATIQUE PAR CAPTEUR DE PROXIMITE CAPACITIF

(84) Designated Contracting States:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IT LI LU MC NL PL PT RO SE SI SK TR**

• **AGUEDA QUESADA, Aitor Maria**
E-20180 Oiartzun (Gipuzkoa) (ES)

(43) Date of publication of application:
09.05.2007 Bulletin 2007/19

(74) Representative: **Chiva, Andrew Peter et al**
Dehns
St Bride's House
10 Salisbury Square
London
EC4Y 8JD (GB)

(73) Proprietor: **Onity S.L.**
20180 Oiartzun (Gipuzkoa) (ES)

(72) Inventors:
• **PEREZ LOPEZ, José Angel**
E-20180 Oiartzun (Gipuzkoa) (ES)

(56) References cited:
US-A- 5 682 032 US-A1- 2002 125 994
US-B1- 6 362 632 US-B1- 6 535 136

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 1 783 694 B1

Description

Invention field

[0001] The new electronic proximity lock referred to by this invention is orientated to electronic lock applications in which the lock is an electronic stand-alone device, meaning that it is fed by batteries and not connected to an electrical supply, or is a device in which low energy consumption is required and the key with which this lock is operated is a non contact proximity key, that can be a card, a key fob, or in general any object that incorporates technologies for the exchange of information between electronic devices without any physical contact between them. For this the lock itself must also incorporate the necessary electronics so that this information exchange without contact can occur and a low consumption activation system of this communication electronics to reduce the elevated energy consumption that would be required to maintain the lock constantly in communication. At the same time, the solution referred to by this invention can be integrated into any other electronically controlled device that, like the electronic lock, is stand-alone electronically or that without being so searches for a minimum energy consumption and is operated by proximity of a non contact proximity key, such as safety boxes, encoders, wall card readers, etc. These devices are usually intended to equip, for example, rooms in hotels, cruises, government buildings, military buildings, universities and in general any premises used by a wide variety of users with timely access rights.

Prior art

[0002] Within the electronic locks field, the concept of electronic proximity lock work has developed in various prior arts, clearly differentiated and in the majority of occasions it has been directly related with the use as cards as the key element. The first electronic proximity lock concepts, such as that described in patent US4717816, understand the term of proximity, covering exclusively the reading element, meaning, the lock is not operated by the proximity of the card but by reading the card, in this case magnetically coded, is performed without the need of physical contact between the card and the reader on the lock but always with the necessity of the card being inserted into the reader slot or, in the most general term, for the card to be positioned in a precise manner on the lock reader. In the quoted patent an electronic lock is described that has a magnetic reader with three heads able to detect a code written on a card by means of three magnetic strips.

[0003] Subsequent applications of electronic proximity lock work widen this proximity concept to its more general interpretation, meaning, that the key card or the key element that must interact with the lock must not forcibly be inserted in a lock slot or in a precise position on a reader head as in the previous case, but that can operate

by an external proximity of the key card to the lock without strict positioning requirements in respect to the lock.

[0004] This new electronic proximity lock work concept is based on the application of exchange technologies of important volumes of information without contact between one electronic component, such as a lock, a key or card that have storage or information exchange elements such as the cards with proximity chips. These technologies allow an exchange of information between these two elements by the mere proximity between said elements, for example by means of radio frequency, and therefore does not require the insertion of the card in a slot nor specially precise positioning of it on a determined reader, the only necessary and sufficient condition is the proximity and the distance to which this type of communication can be made depends, among other facts, on the transmitting power of the electronic device that interacts with the proximity cards.

[0005] To date, diverse inventions have been created that respond to the previous evolution and that integrate as one of its differentiating parts the denominated automatic activation system, whose purpose is to reduce the consumption derived from maintaining the communications system constantly transmitting a signal. An initial approach is that described in patent ES2112152(A1), in which a mechanical type of automatic activation system is described. It is a stand-alone electronic lock fed by batteries that has a reader unit for proximity chip cards by means of electromagnetic waves that is lethargic in a state of minimum consumption. In the presentation manner of the chip card the user must push on some of the surfaces of the lock which is connected to a switch, which thanks to this pressure connects to the chip card reader unit feed activating it and allowing at that moment the lecture of the card without any contact between the card and the lock.

[0006] Inventions have subsequently been developed that do not require any contact for the activation of the communication system. This is the case of the inventions described in patent EP1026617(A1) which consists in an electronic lock with automatic activation systems without contact using infrared detection systems, optical barrier or composed by transmitter-receiver of a ray that reflects on the card. These systems also achieve a low total consumption of the electronic lock making the communication system transmit only in case it is potentially necessary since the consumption of the activation system proposed is less than the communication system consumption.

[0007] Some commercial solutions, of which no remarkable written references exist, are based on substituting the presence detection for the automatic activation for an activation, programming the communication system in function of the expected frequency of use of the lock in such a manner that, for example, if a user has recently opened a door, the time between a communication system switch on and the next is more extensive than after various hours of lock inactivity in which the

arrival of a possible user is expected.

[0008] The most recent advances in this field are described in patent JP2001055852. It is an electronic proximity lock equipped with an automatic activation system that has an oscillation circuit with a determined frequency and resonant circuit that causes a resonance to a harmonic of a determined higher number of times than the oscillation frequency. When a body moves in the proximity of the detection electrode the resonance state varies due to the electrostatic capacity that is generated between the body that has come near and the detection electrode, generating voltage that indicates this proximity and that activates the communication circuit. This way, the overall consumption of the lock is very low, the lock operation does not require contacts not even for automatic switch-on. This invention specifically exploits a physical phenomenon by which the environmental capacitance varies with the presence of a body, that at the same time produces a variation in the variation of the resonance, but the differentiating element is the mentioned change of electrostatic capacity.

[0009] In this sense patent US6362632 proposes a system to measure the environmental capacitance variation when there is proximity of an object. Despite it being a patent not directly related with an electronic lock, the invention consists in using a circuit with two switches whose purpose is to charge a reference condenser with a known capacitance and stable in time, by means of consecutive charges and discharges of a plaque that at the same time acts as a sensor. The first switch allows the sensor to connect to a determined voltage and the second switch connects the plaque to the reference condenser. Stemming from an initial situation in which the both the sensor as well as the condenser are discharged or with a known charge, if the first switch is short circuited, the sensor will adopt a charge in proportion to the voltage and to the capacitance at that precise moment. If after doing this the first switch opens and the second switch closes, the charge required by the sensor will be transferred to the reference condenser, generating a voltage that will be a function of its already known capacitance and the transferred charge, giving this an idea of the capacitance of the sensor from which the charge was transferred from. This type of detection systems have not been applied to date to an electronic lock combined with a communications system.

[0010] Throughout all of this description of the prior art, automatic activation system and non contact communications system for cards are always joined as two integral parts of an automatic activation and communications module. In fact, the principals of a mechanical or optical automatic activation combined with a proximity communications system has been incorporated to other stand-alone requirements similar to those of an electronic lock, as can be the case for a safety box in a hotel room operated by a proximity card. In this sense, there are commercial solutions available without noteworthy documented references, that combine automatic activation

and communication as a single module to be incorporated in any device that requires it, but as mentioned in the previous paragraph, all these modules are based on the mechanical or optical detection principals and not in principals such as the detection of environmental capacitance detection in respect to a reference condenser.

Explanation of the invention

[0011] The present invention provides an electronic lock as claimed in claim 1.

[0012] The present invention refers to a new electronic proximity lock and to the automatic activation and proximity communications module that characterizes it. It deals with a lock operated by the proximity with a key element, hereinafter a card, in which the exchange of information between the lock and the card is performed without the necessity of any contact between them and without the necessity of the card being inserted in any slot in the lock or positioned in any manner on the card reader.

[0013] The technical problem which we intend to overcome with the present invention is related with the current communication technological limitations that allow this type of communications without contact between the lock and card, such as for example the radiofrequency proximity card reader systems. These communication technologies require an important energy consumption of the reader device so that it creates around itself a field which excites the electronics incorporated in the proximity card and it can transmit the corresponding signal and that way perform the information exchange between card and device.

[0014] The majority of the current electronic locks, due to economic viability motives, are stand-alone devices from an energy point of view and are usually fed by conventional batteries. By incorporating proximity card technologies in the stand-alone electronic locks this elevated energy consumption by the proximity communications system, becomes critical for the lock viability. So that when the user nears the lock and it responds opening as the card carried by the user corresponds with the lock, the communication system must be functioning. Since it is impossible to create a precise pattern of the instant in which said user is going to come near said lock with the intention of opening it, since this is unpredictable, in an initial approach the communication system must remain permanently transmitting to detect any card that comes near the lock. From an energy point of view this would make the lock's battery life, and therefore it's autonomy, excessively reduced and would require a substitution or a recharge of the batteries in the lock excessively frequently, generating a cost and a maintenance complexity that make this solution non viable. To intend to have the batteries permanently fed by the conventional electrical current supposes and excessively high extra cost in the electrical installation for the applications in which electronic locks are usually used, such as hotels, and even

in the case that the lock is connected to the electrical current, the energy consumption of maintaining the communication system constantly transmitting a signal would be a high energy cost, not very efficient and not very profitable. Another solution is to program communication system activations, which reduces the total consumption but the features that are given to the lock user will depend on how closely fitted the activation pattern of the communication system is to the usage needs of the lock, with which if special features are required the communication system must be activated frequently, increasing the consumption of energy, and if the reduction of consumption is wanted a user must wait for the activation of the communication system to open the lock. Therefore, the only solution for this limitation is to incorporate in the lock a low consumption proximity detection system for the automatic activation of the communication system, so that the lock can detect the proximity of a body or object at all times but maintaining residual electric consumption and can activate the communications system, with an elevated energy consumption, only when it is potentially necessary. Also, these systems must allow the detection and the automatic activation on such a rapid manner that the features offered to the user are not diminished, that means that the user does not perceive any delay in the operation of the lock due to the incorporation of the automatic activation system. With this solution, the autonomy of the electronic proximity locks is adequate so that their installation is technically and economically viable in the application to which the electronic proximity lock is destined.

[0015] Just as it has been described in the prior art, to date different solutions have been given to the automatic activation of electronic proximity locks, highlighting the automatic activation by mechanical, optical or resonance means. The proximity electronic lock and the automatic activation and proximity communications module of the present invention widen this range on solutions through proximity detection, and the posterior automatic activation of the communications system, stemming from the measurement of variations in the capacitance of the environment next to the lock.

[0016] The system that uses the invention to measure the variations of capacitance of the environment, and therefore for the detection of the proximity of a body or object to the lock or the automatic activation and proximity communications module, is known as the charging pump. Figure 1 shows the theoretical circuit on which the charging pump is based. Its operation is based on the alternative conmutation between two switches (1) and (2). When switch (1) is short circuited and switch (2) is kept open, a conducting plaque (3) connects which acts as a pre-defined voltage sensor (VCC). This plaque (3) creates together with the proximity environment and grounds a fictitious capacitance (CX) condenser (4). This capacitance (CX) is variable and depends on the conditions of the environment next the plaque (3) and therefore, the proximity of an object or body to the plaque would pro-

duce a variation in (CX) in respect to the situation in which there is no proximity of a body or object to the plaque (3).

[0017] Therefore, when short circuiting the switch (1) keeping switch (2) open, the plaque (3) will charge with a charge (qx1) in direct function to the capacitance (CX) in said instant. Next, switch (1) opens and switch (2) is short circuited. At this moment charge (qx1) acquired by the fictitious condenser (4) is transferred to a reference condenser (5) connected to earth and with known capacitance and stable in time (CP). If afterwards switch (2) is open and switch (1) is short circuited, the reference condenser (5) keeps the charge (qx1), while the plaque (3) recharges with a charge (qx2) that will be in function of the capacitance (CX) of the fictitious condenser (4) at the instant of the second manoeuvre.

[0018] Continuing with this process, repeating a number (N1) of times the previous charge cycle without discharging the reference condenser (5), the reference condenser (5) will have a total charge that will be the sum of all the partial charges transferred from the plaques (3) in the (N1) charge cycles, and generates tension (V1) among its terminals that will be in function to the total charge that has been transferred from the plaque (3). When comparing the tension (V1) with a known reference tension (VREF) an environmental capacitance measure will be obtained during the execution of the cycle. According to what has been said so far, if (VREF) is predetermined as the tension that would be generated by the condenser when charged during (N1) charge cycles without the proximity of any body or object to the plaque (3), the variation of tension (V1) in respect to (VREF) will determine for example the proximity or not of a body or object during the execution of (N1) cycles.

[0019] Figure 2 shows another construction of the theoretical circuit with the same elements as in figure 1 but with a provision nearer to that required by the present invention. With the provision of switch (2) between the reference condenser (5) and ground we achieve situation said reference condenser (5) between the switches (1) and (2), facilitating the incorporation of a manoeuvre system for the switches as for example a microcontroller (6) as is shown in figure 3. The incorporation of this microcontroller (6) supplies a simple solution, of great flexibility and with great control capabilities for the execution of the charging pump cycles previously described. At the same time the microcontroller (6) allows the switch operations to be performed at a very high speed, very superior to the normal approximation time of a user with the lock card, in such a manner that the user does not perceive and delay in the operation of the lock when the complete process is processed.

[0020] The incorporation of this microcontroller (6) allows a more optimized application of the previous charging pump system, designed to measure the environmental capacitance, adapting it to its application to the detection of the proximity of a body or object to the lock in an efficient, safe and stable manner. The system improvement of the charging pump incorporated to the

present invention consists in a new method or algorithm as shown in figure 4 that executed by the microcontroller (6) offers the lock response features to the proximity of a user and to the global consumption of the proximity lock that improves the prior art of this technical field. Figure 4 shows the final construction of the low consumption automatic activation system by means of detection of the variations in environmental capacitance of the present invention. It includes two protection diodes (7) and (8) and three resistance (9), (10) and (11) for the adjustment of the currents and tensions in the circuit.

[0021] Figure 5 shows a summary of the method used by the present invention for the detection of proximity using a modified principal of the charging pump previously described. As commented, said method consists in an algorithm executed by a microcontroller (6) on the modified charging pump circuit shown in figure 4. In this process two sub processes intervene denominated as:

[0022] Charge cycle, which is the manoeuvre in which the charge is produced in the plaque (3) and its posterior discharge, transferring the charge acquired to the reference condenser (5). As mentioned before, the amount of the charge transferred in each charge cycle will depend on the environmental capacitance of the plaque (3).

[0023] Complete charge process, which is the repetition of consecutive charge cycles until the tension generated between the terminals in the reference condenser (5) equals or surpasses the tension threshold (V2). As collary to the previous process, the number of charge cycles involved in each complete charge process will depend on the environmental capacitance while performing the complete charge process. After every complete charge process the reference condenser (5) discharges to an initial known charge that can be for example null.

[0024] The method starts with the positioning of the automatic activation system in an initial position (B1) as a system restart mode and the system calibration (B2) that is produced for example in the first installation of the lock. The calibration of the system is not only produced during the restart but also in the (B7) and (B9) phases of the process, in which the complete system is recalibrated. In these calibrations value is given to the comparison variables of the measured signal and the reference tensions that the system uses, and both the fictitious condenser (4) as well as the reference condenser (5) are discharged to an initial status that could constitute for example in both condensers being completely discharged. The comparison variables and the reference tensions that give value to these calibrations are:

[0025] Tension (VCC), or the fixed tension to which the plaque charges are made (3).

[0026] Trigger threshold (N2), or the number of charge cycles necessary for the reference condenser (5) to generate in its terminals tension which is higher or equal to the tension threshold (V2), with the condition that there is no proximity to the plaque (3) by any body or object which is not a part of the lock.

[0027] Tension threshold (V2), or the tension generat-

ed in the terminals of the reference condenser (5) after performing a number of charge cycles coinciding with the trigger threshold (N2), with the condition that there is no proximity to the plaque (3) by any body or object which is not a part of the lock.

[0028] Counter value (CONT1), that in the calibration and after each complete charge process is positioned to zero, and is the variable that counts the number of charge cycles performed in each complete charge process, in such a manner that each time that a charge cycle is performed the value of the counter (CONT1) increases by one unit.

[0029] Sensitivity (S), or the value of the difference between the trigger threshold (N2) and the counter value (CONT1) after each complete charge process, which means a possible approximation of a body or object to the plaque (3).

[0030] Number of activation cycles (N3), or the number of consecutive times that the counter value (CONT1) must vary in respect to the trigger threshold (N2), and its difference must surpass the sensitivity (S), so that this unequivocally means the proximity of a body or object.

[0031] Counter value (CONT2), that in the calibration is positioned to zero, and is the variable that counts the number of consecutive complete charge processes in which the value of the counter (CONT1) has varied in respect to the trigger threshold (N2) and its difference has surpasses the sensitivity (S).

[0032] After this initial adjustment, the system executes a first measurement (B3) of the environmental capacitance by means of charge cycles. In this measure the fictitious condenser (4) initially proceeds to be discharged as well as the reference condenser (5) and to position the counter value (CONT1) to zero. After this charge it proceeds to the performance of the consecutive charge cycles. In each charge cycle, by means of a commutation of the microcontroller (6) the plaque (3) is charged connecting it to a fixed tension (VCC) while the reference condenser (5) is connected. Afterwards, the microcontroller (6) opens the plaque (3) commutation feed and closes a discharge circuit to charge the reference condenser (5) with the recently acquired charge for the plaque (3). This charge is stored in the reference condenser (5) which disconnects from the plaque (3). With this a tension increase is provoked among the terminals in the reference condenser (5) proportionate to the capacitance if the fictitious condenser (4) made up by the plaque (3) and its environment close to earth, which is dependent of the environmental conditions and the proximity or not of a body or objects. After this charge the previous counter value (CONT1) is increased by one unit and the tension between the terminals in the reference condenser (5) is measured to see if it equals or surpasses the tension threshold (V2). If the tension in the terminals of the reference condenser (5) does not surpass the tension threshold (V2) the charge cycle is repeated until the tension in the terminals of the reference condenser (5) equals or surpasses the tension threshold

(V2).

[0033] If the tension in the terminals of the reference condenser (5) equals or surpasses the tension threshold (V2), a complete charge process has been performed and we pass on to the comparison (B4) of the current counter value of the charge cycles (CONT1) and to the trigger threshold (N2). At this point the method varies lightly in function of the effect expected by the proximity of the body in the environmental capacitance of the plaque (3).

[0034] In the majority of cases, the proximity of a body to the plaque (3) creates an increase in the capacitance of the fictitious condenser (4) but the existence of determined materials has been confirmed, some of them used as support for the proximity chips that create a decrease in the environmental capacitance with their proximity to the plaque (3). The incorporation of the microcontroller (6) in the present invention allows the modification of the method applied in function of the effect expected by the proximity of the proximity support chip without more than varying the algorithm used. This difference of algorithm consists basically in that, in the comparisons of measures performed of the current counter value (CONT1) in respect to the trigger threshold (N2), the value which means possible proximity of a body or object is higher or lower than the trigger threshold (N2). Both cases are contemplated separately in the claims but to the effects of the description of the invention we only consider the case in which the proximity of a body or object generates an increase in the capacitance of the fictitious condenser (4) and therefore, the current counter value (CONT1) is less than the trigger threshold (N2) when there is proximity.

[0035] Continuing, after the last clarification, at the comparison point (B4) the current counter value (CONT1) and the trigger threshold (N2) after each complete charge process, in case that the current counter value (CONT1) is higher to the trigger threshold (N2) the capacitance of the fictitious condenser (4) is less than its capacitance without presence of a body or object, therefore there is no proximity of any body or object to the plaque (3) and the communications system (B6) must not activate. In all instances it is possible that the whether conditions, humidity, electrostatic charge have varied and this has varied the environmental capacitance, therefore the values of the comparison variables described in the restart (B1) and calibration (B2) process must be recalibrated (B7) in function to the new situation given by the last complete variation measurement of the environmental capacitance. After this calibration the moment in which the new measurement process of the environmental capacitance (B11) variation is initiated is determined and the automatic activation system (B12) is deactivated, that after the pre-programmed time period reactivates (B13). After this activation the communication circuit is checked to see if it is activated or not (B14). In case it continues to be activated, the automatic activation system considers that the last communication process has not finalized and returns to program the next activation

(B11). In case the communications circuit is not activated the process restarts from the environmental capacitance measure (B3).

[0036] In case the current counter value (CONT1) is less than the trigger threshold (N2) after the complete charge process, these means that the fictitious condenser (4) capacity has been increased and that therefore it is possible that there is proximity of a body or object to the plaque (3). In any case this first measurement is not conclusive since the increase of the capacitance of the fictitious condenser (4) can have occurred by temperature variations, humidity or electrostatic charge of the environment next to the plaque (3). Therefore in this case it proceeds to the comparison (B5) of the difference between the trigger threshold (N2) and the current counter value (CONT1) in respect to the sensitivity (S) If the difference does not surpass the sensitivity (S) an increase in capacitance has occurred not related with the proximity of a body or object to the plaque (3), and therefore the communication system (B6) must not activate, but a change has occurred in the environmental conditions and therefore the values must be recalibrated (B7) of the comparison variables describe in the restart (B1) and calibration (B2) process to the new situation given by the last complete measurement of variation of the environmental capacitance. After this calibration the moment in which the new measurement process of the environmental capacitance (B11) variation is initiated is determined and the automatic activation system (B12) is deactivated, that after the pre-programmed time period reactivates (B13). After this activation the communication circuit is checked to see if it is activated or not (B14). In case it continues to be activated, the automatic activation system considers that the last communication process has not finalized and returns to program the next activation (B11). In case the communications circuit is not activated the process restarts from the environmental capacitance measure (B3).

[0037] If the difference between the counter value (CONT1) and the trigger threshold (N2) after the complete charge process is higher to the sensitivity (S) there is a second proximity indication of a body or object to the plaque (3) but with a single measurement also does not confirm the proximity since it could be due to internal feed or electronically errors. Therefore, the counter value is increased by one unit (CONT2) and (B8) the complete charge and comparison process is repeated from (B3) to (B5) until one of the following three cases occurs:

[0038] That in one of the complete charge processes the value of the counter (CONT1) is higher than the trigger threshold (N2) when the tension threshold (V2) has been surpassed, with which the environmental capacitance has decreased and therefore there is no proximity.

[0039] That in one of the complete charge processes the difference between the trigger threshold (N2) and the current value of the counter (CONT1) is lower to the sensitivity (S) when the value of the counter (CONT1) is lower than the trigger threshold (N2) with which the environ-

mental capacitance is not due to any proximity.

[0040] That the actual value (CONT2) equals the number of activation cycles (N3), with which the increase in capacitance detected is unequivocally due to the proximity of a body or object to the plaque (3). In this case the situation of the environment due to the proximity of an object has been modified that could be a user of the lock with a card or not, it could be for example an object that has stuck to the lock or a decorative element that has been placed close to the door. In case it is a nearby body or object that is not going to be removed in a brief time lapse, a situation will be produced in which the system will be constantly sensing continuous proximity, keeping the communication circuit active and therefore consuming energy and drastically reducing the autonomy of the lock. To avoid this, the first calibration (B9) of the values of the comparison variables described in the restart (B1) and calibration (B2) process to the new situation given by the last complete variation measurement of the environmental capacitance, that will correspond to the values with the proximity of a body or object. These values, in case the proximity is of a user that moves away from the lock after its normal operation will readjust to similar values to the initial ones in later variation of the environmental capacitance measurement process. After this calibration the moment in which the new measurement process of the environmental capacitance (B11) variation is initiated is determined and the automatic activation system (B12) is deactivated, that after the pre-programmed time period reactivates (B13). After this activation the communication circuit is checked to see if it is activated or not (B14). In case it continues to be activated, the automatic activation system considers that the last communication process has not finalized and returns to program the next activation (B11). In case the communications circuit is not activated the process restarts from the environmental capacitance measure (B3).

[0041] Meanwhile both the recently activated communication system is transmitting a signal, without being disturbed by the field that could be created by the automatic activation system plaque (30) since it is inactive, in search of a card or key object that incorporates the communication technology compatible with the communications system integrated in the automatic activation and communications module of the lock of the present invention. If in the proximity of the lock there does not exist said card or key object, after a set time the communication system will return to inactive until the automatic activation system detects a new proximity. On the other hand, if said key object is in the proximity of the lock, the communication system will exchange information with this element and in case of corresponding with the key object that corresponds with the lock, the communication circuit will transmit a signal to the lock's control circuit, which will correspond by performing and operation corresponding to the nature of the information exchanged, for example by opening the lock.

[0042] At the same time, the present invention includes

a solution to one of the basic problems that affect the combination of an automatic activation system based in capacitive principals and a communication system without contact such as radio frequency. This problem is the distortion of the communications electromagnetic field that can produce by the presence of a conductive plaque (3) whose mission is to serve as a sensor to detect the capacitance variations. By definition, this plaque (3) must have sufficient conductive surface to be able to create with the environment a fictitious condenser (4). Also, by definition, by submitting the conductive plaque (3) to an electromagnetic field, a series of internal parasite currents will be generated in it that will generate a second electromagnetic field that oppose the electromagnetic field that generates it, distorting it. This is precisely the case in which the present invention finds itself, since we must integrate a conductive plaque (3) and an antenna (12) that generates a communication electromagnetic field in a reduced space due to instability and viability of the electronic lock as shown in figure 6. The present invention solves the present problems in two fronts:

[0043] The first, by means of the work method previously described, in which at no time is the parallel functioning of the automatic activation system and the communication system permitted in such a manner that the plaque (3) does not receive charge from the tension (VCC) is the communication system is in operation.

[0044] The second, by means of the incorporating of a plaque(3) whose surface is divided into thing conductive nerves, close to a millimetre of width, electronically interconnected between themselves by means of a common nerve conductor also thin so that as a set they make up a metallic surface sufficient for the plaque (3) to have the adequate features for its use as a captive sensor and at the same time offers a great resistance to the generating of internal closed circuits that promote the generation of internal parasite currents when submitting the plaque (3) to the electromagnetic field generated by the communications antennae (12). In this manner the parasite currents generated are minimized and also their negative effect in the communication field, making it effective even in case the plaque (3) is located in front of the antennae (12) as shown in figure 6. This circumstance is very dramatic in those low power devices feed by conventional batteries, which is precisely the field in which the present invention falls.

[0045] In respect to the advantages of the present invention in respect to the prior art, if the features of the invention are compared in respect to those offered by the locks that incorporate systems of mechanical activation, the main advantage is that, in the case of the mechanical systems a first contact is always required to activate the communication circuit and the present invention does not require contact at any time. Furthermore, the existence of mobile parts for the mechanical activation is an origin of possible faults or sabotage, for example inserting strange elements into the unavoidable slots of the mechanical system, that with the present invention

are saved by the non need for contact.

[0046] In respect to the locks with optical automatic activation system, despite that from the functionality point of view these solutions already offer non contact lock operation, they have a series of disadvantages that make them improvable. The main disadvantages of these systems are due to the automatic activation system detection principal itself. It deals with systems that require optical signs to be transmitted, therefore they depend on the cleaning of the transmitting or receiving surface which is essential for its function, making them specially sensitive to sabotage, and on the other hand, the transmission field of the optical signal must be perfectly adjusted in position and angle in the space since an non precise adjustment can produce that the swept field is excessive wide, detecting any type of presence with or without the intention of interacting with the lock and producing a higher lock consumption, on the contrary it can be to narrow impeding the correct function, in such a manner that they require a very precise assembly and a frequent and costly maintenance. In the case of the present invention these problems are solved since the detection is performed without the need of transmitting any optical signal and in case of sabotage, for example by sticking a substance on the reader, the automatic activation system itself is the one that adapts itself to the variables of the new situation and continues to function. Finally the proximity capacitive detection requires less energy consumption so that the autonomy of the lock for the batteries is higher in the present invention.

[0047] In respect to the solutions with programmed activation of the communication system, despite that these solutions improve the weak points of the mechanical and optical solutions, it completely depends in the success of the activation programming of the communication system achieve a good relationship between response time and features offered to the user, so that they result in a higher consumption and a better autonomy of the lock, in this way missing the basic objective that motivates the development of the solution. On the other hand, the fact that the automatic activation and communications and the proximity lock of the present invention incorporate a programming function of the moments in which the proximity capacitive detection system performs the measurement of the environmental capacity, makes it possible to incorporate to its algorithm the same functions as the solution with programmed activation of the communication system, but with the difference that what is activated is the low consumption automatic activation system and not the increased energy consumption communication system.

[0048] Finally, the main advantage contributed by the present invention in respect to the solutions based in oscillation and resonance circuits from the variation of the environmental capacity, is that the main detection used is simpler and the use of a microcontroller (6) in the circuit widely amplifies the flexibility of the device and its control capacity, improving the lock features and reducing at the

same time the possible error focuses when simplifying the necessary circuits. At the same time, in these solutions we have not dealt with the problematic generated by the introduction of a conductive plaque (3) as a sensor in the same device as the antennae that is required by the communication system and in the present invention more than solves this problem.

Explanation of the figures

[0049]

Figure 1 shows a theoretical circuit that operates as a charging pump destined for the measurement of the environmental capacitance of the plaque (3).

Figure 2 shows an evolution of the circuit with the same functionality as in figure 1 but with a relocation of the switch (2) more in agreement with the application of the present invention.

Figure 3 shows a charging pump circuit commanded by a microcontroller (6) with the same functionality as the circuits in figures 1 and 2.

Figure 4 shows the basic system of the automatic activation system by means of detection of the variations in environmental capacitance of the present invention.

Figure 5 shows the diagram of the operations of the method followed by the present invention to determine the proximity of a body by variation of the environmental capacitance of a plaque (3)..

Figure 6 shows a general diagram of the main construction elements and the internal elements of the proximity lock of the present invention.

Figure 7 shows the proximity (21) and communication (23) detection areas.

Figure 8 shows the main angles to keep in mind for the plaque (3) placement in function to the most probable approximation angle of the card (22)

Figure 9 shows the main external distances to the lock to keep in mind for its operation.

[0050] In these figures the following references are indicated:

- VCC.- Fixed tension by which the plaque is charged (3).
- VREF - Reference tension as comparison with the condenser (5) tension
- CX. Variable capacitance of the fictitious condenser (4)
- CP. Known capacitance of the reference condenser (5)
- 1.- First switch of the charging pump circuit
- 2.- Second switch of the charging pump circuit
- 3.- Plaque that with its environment and grounding creates the fictitious condenser (4).
- 4.- Fictitious condenser created by the plaque (3), its environment and grounding.

5.- Reference condenser of known capacitance
 6.- Microcontroller that commands the automatic activation by capacitive variation
 7.- First protection diode of the automatic activation system of the invention
 8.- Second protection diode of the automatic activation system of the invention
 9.- First adjustment resistance of the automatic activation system of the invention
 10.- Second adjustment resistance of the automatic activation system of the invention
 11.- Third adjustment resistance of the automatic activation system of the invention
 12.- Antenna from the communication system of the invention
 13.- Non metallic material part that covers the plaque (3).
 14.- External metallic casing of the electronic proximity lock
 15.- Handle of the electronic proximity lock
 16.- Plaque that supports the communications antenna and plaque (3).
 17.- Plaque that supports the automatic activation and communication circuits.
 18.- Location of the control system of the proximity lock operations
 19.- Location of the electromechanical elements of the proximity lock
 20.- Location of the batteries that feed the proximity lock
 21.- Field for detecting effective proximity.
 22.- Proximity card
 23.- Field for effective communication with card
 B1.- Restart event of the automatic activation system
 B2.- Calibration action of the automatic activation comparison variables
 B3.- Action of measurement of the variation of the environmental capacitance of the plaque (3)
 B4.- Comparison of the measurement in respect to the trigger threshold (N2)
 B5.- Comparison of the difference between (N2) and the measurement in respect to the sensitivity (S)
 B6.- Action of non activation of the communication system.
 B7.- Recalibration action of the automatic activation comparison variables
 B8.- Comparison of the number of consecutive measures that indicate proximity.
 B9.- Recalibration action of the automatic activation comparison variables
 B10.- Action of activation of the communication system.
 B11.- Programming action of the following execution of the automatic activation system
 B12.- Deactivation event of the automatic activation system
 B13.- Activation event of the automatic activation system

B14.- Comparison of the activity situation of the communication system.
 α - Vertical positioning angle of the plaque (3)
 β - Probably approach angle of the card in respect to the vertical plaque.
 D1.- Distance of the plaque (3) in respect to the metallic lock carcass.
 D2.- Nominal distance of the proximity card for the operation of the lock

Exposure of a preferential performance

[0051] Figure 6 shows the exterior aspect and the general elements contained in a preferential performance of the electronic proximity lock of the present innovation. In the exterior of the preferential performance the following are highlighted, the metallic carcass of the electronic proximity lock (14), the handle on the proximity lock (15) and a non metallic element (13), for example in plastic, that covers the plaque (3) that acts as a sensor element. This non metallic (13) cover allows the communication field created by the lock communications system is not screened by the metallic carcass (14) of the proximity lock.

[0052] In the interior of the lock the first highlighted item is the conductive plaque (3) by proximity sensor by variation of the environmental capacitance and the antenna of the communications system (12). Plaque (3) and antenna (12) are physically found assembled on a single support plaque (16) or PCB, one on each face of said support plaque (16), and with the plaque (3) situated on its most external face. Due to the special surface of the plaque (3) in parallel nerves approximately one millimetre wide with a transversal nerve that electronically connects them, the communications field created by the antenna (12) when the communications system is active is not distorted when passing through the plaque (3) and the whole group can adopt its maximum compactness reducing the space necessary in the lock and therefore reducing its total size. This group of plaque (3), antenna (12) and common support plaque (16) are fixed to a second plaque (17) that houses at the same time, the microcontroller (6) necessary for the automatic activation, the additional electronics necessary for the automatic activation circuit and the necessary electronics for the communication system.

[0053] At the same time, it is worth noting the location of the general operation control (18) electronics common to all the electronic locks whether of proximity or not, whose function is the execution of the actions adequate to the nature of the information received from the key card, for example open the lock, the location of the electromechanical elements (19) of the lock and the location is the batteries (20) that supply the energy necessary for the lock to be energy autonomous.

[0054] With this performance, in figure 7 a transversal cut is shown of the top part of the electronic proximity lock that houses the proximity detection plaque (3) and

the antenna of the communications system (12). In figure 7 effective area for the detection of proximity (21), a possible approach by a proximity card (22) and the effective communication areas (23) with the proximity card. As shown in figure 7, these effective detection (21) and communication (23) areas are concentrated around the area in which the electronic proximity lock does not have external metallic carcass (14), but a non metallic covering (13), for example plastic. In the rest of the areas around the metallic carcass (14), said carcass produces a screening effect on the detection and communication fields therefore the user must approach the area covered by plastic (13) with the card.. In said covering (13) indication signs are recorded of this mode of interacting with the lock. However, the screening of the communication field by the metallic carcass (14) produces a desirable effect in the back part of the lock. This back part usually corresponds with the interior part of the room closed by the electronic lock. If this screening did not exist on the back part, there would also exist an effective communication area in the interior of the room, with the subsequent risk of the lock opening without intending to.

[0055] As seen in figure 7, the effective communication area is larger than the proximity detection effective area. This is done like this so that, in the possibility that the user lightly moves the card (22) on the proximity of the lock and he communications field is able to interact with the card even if the movement is of lightly leaving after the proximity detection. In general terms, the card (22) can be read in any position it is in within the effective communication areas (23), even though a parallel approach between the surface of the card (22) and the surface of the non metallic carcass (13) of the approach with the largest guarantee of function of the lock.

[0056] In this respect figure 8 is shown with a transversal cut on the top part of the electronic proximity lock that houses the proximity detection plaque (3) and the antenna of the communications system (12). In this figure two angles are highlighted: angle (α) for the positioning of the plaque (3) and the antenna (12) located in the same support plaque (16) in respect to the vertical, and angle (β) which is the probable angle of approach of the proximity card in respect to the vertical.

[0057] We have seen that the lecture of the proximity card by the communication system integrated in the electronic lock is better when there is parallelism between the antenna (12) and the card (22). Therefore, once the value has been determined of angle (β) most probable in respect to the vertical in which the user approached the proximity card (22) to the non metallic cover (13) that covers the proximity detection plaque (3) and the antenna (12), the angle (β) with which the group made up of by the proximity sensor group (3), antenna (12) and the support plaque (16) must be located in respect to the vertical will be the same as angle (β). In the preferential performance of the present invention said angle is of 45°. As a consequence of the frontal surface of the non metallic cover (13) that covers the sensor plaque (13) and the

antenna (12) must have this same angle to induce the user to approach the card with said angle.

[0058] Finally in figure 9 another transversal cut is shown on the top part of the electronic proximity lock that houses the proximity detection plaque (3) and the antenna of the communications system (12). In this figure the distance (D1) towards the exterior of the metallic carcass (14) is highlighted in which the group made up by the proximity detection plaque (3) and the antenna (12) and the plaque (16) that supports it in respect to the point which mostly stands out on the lock's metallic carcass (14). We have seen that the bigger the distance, meaning the further out the group is from this external metallic lock carcass (14), the bigger the effective communications distance (D2) is between the communication system integrated in the lock and the card (22). In the present description of the preferential performance it has been seen that parting from a distance (D1) of more than 30 millimetres, the screening effect that is produced by the metallic carcass (14) on the communication field is not worthy.

Claims

1. An electronic lock operated by the proximity of a key object that contains the adequate means to establish and maintain an information exchange without contact with said lock, the adequate means to store the necessary information for said exchange and the information to be exchanged, in such a manner that said lock is able to determine the subsequent actions of said exchange of information as a function of the nature of the exchanged information whereby it comprises an automatic activation system by detection of variations of the capacitance in the proximity of the lock which comprises:

a detection plaque (3), that together with its environment generates a capacity element (4) whose capacitance varies as a function of the environmental conditions and the proximity of a body or object;

an reference capacity element (5) with a stable capacitance in time or whose variation as a function to the environmental conditions is low;

an electronic system (6) that allows at least to discharge both the element of detection of capacity (4) as well as the reference capacity element (5) positioning them in an initial state and that afterwards alternatively allows, to disconnect among them the element of capacity of detection (4) and the elements of reference capacity (5), to connect the detection capacity element (4) to an initial voltage source charging said capacity element with a charge in function of its capacitance at that moment, to disconnect the detection capacity element (4) from the source

of the first predefined voltage, to connect between them the changed detection capacity element (4) and the reference capacity element (5) if such a manner that the charge of the detection capacity element (4) passes to the reference capacity element (5) to discharge the detection capacity element (4), generating in this manner a cycle of charge and discharge; an electronic system (6) that counts the number of charge and discharge cycles necessary so that the reference capacity element (5) reached a total charge that generates a second reference voltage and compares this number of cycles in respect to a number of reference cycles; an electronic system (6) that once a body or object is detected in the proximity to the detection plaque (3) activates an electronic communication system to recognize if the body or object is a key object or in its case initiate and maintain the exchange of information with it that leads to performing the corresponding actions to the nature of the interchangeable information;

characterized in that the electronic lock further comprises means for adjustment of the number of reference cycles after each complete charge process and posterior charge of the capacity element (5) through the charge and discharge cycles of the detection capacity element (4) until the stored charge in the capacity reference element (5) generates a second reference voltage in such a manner that the new number of reference cycles is in function of the number of cycles obtained in the complete discharge process of the capacity element (5) and posterior charge of it once finished.

Patentansprüche

1. Elektronisches Schloss, das durch die Nähe eines Schlüsselobjekts betätigt wird, das die angemessenen Mittel zum Herstellen und Aufrechterhalten eines Informationsaustauschs ohne Kontakt mit dem Schloss enthält, wobei die angemessenen Mittel zum Speichern der notwendigen Informationen für den Austausch und der auszutauschenden Informationen dient, dergestalt, dass das Schloss in der Lage ist, die nachfolgenden Aktionen des Austauschs von Informationen als Funktion der Beschaffenheit der ausgetauschten Informationen zu bestimmen, wobei es ein automatisches Aktivierungssystem durch Detektion von Schwankungen der Kapazität in der Nähe des Schlosses umfasst, das Folgendes umfasst:

eine Detektionsplakette (3), die zusammen mit ihrer Umgebung ein Kapazitätselement (4) erzeugt, dessen Kapazität als Funktion der Um-

gebungsbedingungen und der Nähe eines Körpers oder Objekts schwankt; ein Referenzkapazitätselement (5) mit einer zeitlich stabilen Kapazität oder dessen Schwankung als Funktion der Umgebungsbedingungen gering ist; ein elektronisches System (6), das mindestens das Entladen sowohl des Elements der Detektion der Kapazität (4) als auch des Referenzkapazitätselements (5) erlaubt, wobei diese in einen anfänglichen Zustand versetzt werden, und das danach alternativ Folgendes erlaubt: Trennen des Elements der Kapazität der Detektion (4) und der Elemente der Referenzkapazität (5) untereinander, Verbinden des Detektionskapazitätselements (4) mit einer Anfangsspannungsquelle, wodurch das Kapazitätselement in Funktion seiner Kapazität in diesem Moment mit einer Ladung geladen wird, Trennen des Detektionskapazitätselements (4) von der Quelle der ersten vordefinierten Spannung, Verbinden des geänderten Detektionskapazitätselements (4) und des Referenzkapazitätselements (5) untereinander dergestalt, dass die Ladung des Detektionskapazitätselements (4) auf das Referenzkapazitätselement (5) übergeht, Entladen des Detektionskapazitätselements (4), um **dadurch** auf diese Weise einen Zyklus von Ladung und Entladung zu erzeugen; ein elektronisches System (6), das die Anzahl der Ladungs- und Entladungszyklen zählt, die notwendig sind, so dass das Referenzkapazitätselement (5) eine Gesamtladung erreicht, die eine zweite Referenzspannung erzeugt, und diese Anzahl von Zyklen mit Bezug auf eine Anzahl von Referenzzyklen vergleicht; ein elektronisches System (6), das, sobald ein Körper oder Objekt in der Nähe der Detektionsplakette (3) detektiert wird, ein elektronisches Kommunikationssystem aktiviert, um zu erkennen, ob der Körper oder das Objekt ein Schlüsselobjekt ist, oder in seinem Fall den Austausch von Informationen damit einzuleiten und aufrechtzuerhalten, der zu dem Durchführen der entsprechenden Aktionen bezüglich der Beschaffenheit der austauschbaren Informationen führt;

dadurch gekennzeichnet, dass das elektronische Schloss ferner Mittel zur Einstellung der Anzahl von Referenzzyklen nach jedem vollständigen Ladungsprozess und späterer Ladung des Kapazitätselements (5) durch die Ladungs- und Entladungszyklen des Detektionskapazitätselements (4), bis die gespeicherte Ladung in dem Kapazitätsreferenzelement (5) eine zweite Referenzspannung erzeugt, dergestalt, dass die neue Anzahl von Referenzzyklen in Funktion der Anzahl von Zyklen ist, die in dem

vollständigen Entladungsprozess des Kapazitäts-
elements (5) und späterer Ladung dieses nach Be-
endigung erhalten wird, umfasst.

Revendications

1. Verrou électronique actionné par la proximité d'un
objet formant clé qui contient les moyens appropriés
pour établir et maintenir un échange d'informations
sans contact avec ledit verrou, les moyens appro-
priés étant destinés à stocker les informations né-
cessaires audit échange et les informations à échan-
ger, de telle manière que ledit verrou soit capable
de déterminer les actions ultérieures dudit échange
d'informations en fonction de la nature des informa-
tions échangées, celui-ci comprenant un système
d'activation automatique par détection de variations
de la capacité à proximité du verrou, qui comprend :

une plaque de détection (3) qui, en association
avec son environnement, génère un élément ca-
pacitif (4) dont la capacité varie en fonction des
conditions ambiantes et de la proximité d'un
corps ou d'un objet ;

un élément capacitif de référence (5) ayant une
capacité stable dans le temps et dont la variation
en fonction des conditions ambiantes est faible ;

un système électronique (6) qui permet au
moins de décharger à la fois l'élément de détec-
tion de capacité (4) ainsi que l'élément capacitif
de référence (5) en les faisant passer dans un
état initial et qui permet ensuite en variante de
déconnecter parmi ceux-ci l'élément capacitif de
détection (4) et les éléments capacitifs de réf-
érence (5), de connecter l'élément capacitif de
détection (4) à une source de tension initiale
chargeant ledit élément capacitif avec une char-
ge qui est fonction de sa capacité à ce moment,
de déconnecter l'élément capacitif de détection
(4) de la source de la première tension prédéfi-
nie, de connecter entre ceux-ci l'élément capa-
citif de détection modifié (4) et l'élément capacitif
de référence (5) de telle manière que la charge
de l'élément capacitif de détection (4) passe
vers l'élément capacitif de référence (5) afin de
décharger l'élément capacitif de détection (4),
en générant de cette manière un cycle de charge
et de décharge ;

un système électronique (6) qui compte le nom-
bre de cycles de charge et de décharge néces-
saires pour que l'élément capacitif de référence
(5) atteigne une charge totale qui génère une
seconde tension de référence et qui compare
ce nombre de cycles à un nombre de cycles de
référence ;

un système électronique (6) qui, lorsqu'un corps
ou un objet a été détecté à proximité de la plaque

de détection (3), active un système de commu-
nication électronique afin de déterminer si le
corps ou l'objet est un objet formant clé ou, si
tel est le cas, de déclencher et de maintenir
l'échange d'informations avec celui-ci, cela con-
duisant à la mise en oeuvre des actions corres-
pondant à la nature des informations pouvant
être échangées ;

caractérisé en ce que le verrou électronique com-
prend en outre des moyens d'ajustement du nombre
de cycles de référence après chaque processus de
charge complet et postérieurement à la charge de
l'élément capacitif (5) par les cycles de charge et de
décharge de l'élément capacitif de détection (4) jus-
qu'à ce que la charge stockée dans l'élément capa-
citif de référence (5) génère une seconde tension de
référence, de telle manière que le nouveau nombre
de cycles de référence soit obtenu en fonction du
nombre de cycles lors du processus de décharge
complet de l'élément capacitif (5) et de sa charge
postérieure une fois que celle-ci est terminée.

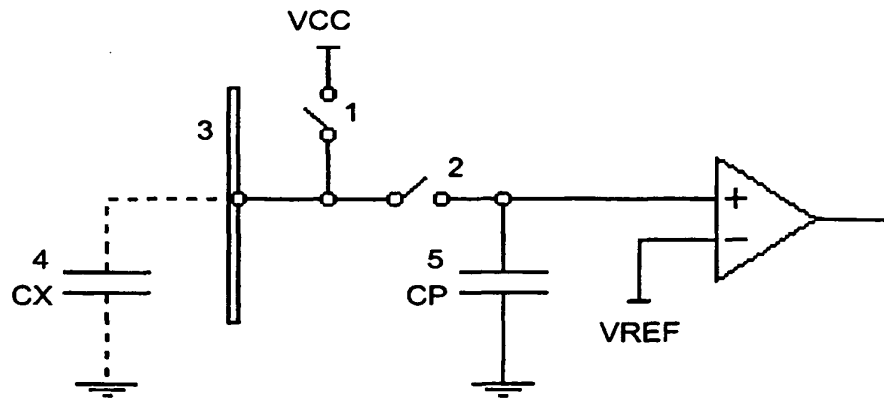


FIGURE 1

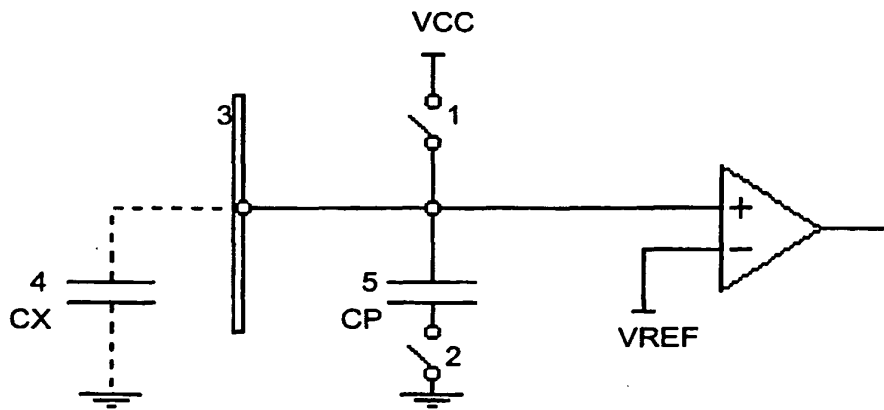


FIGURE 2

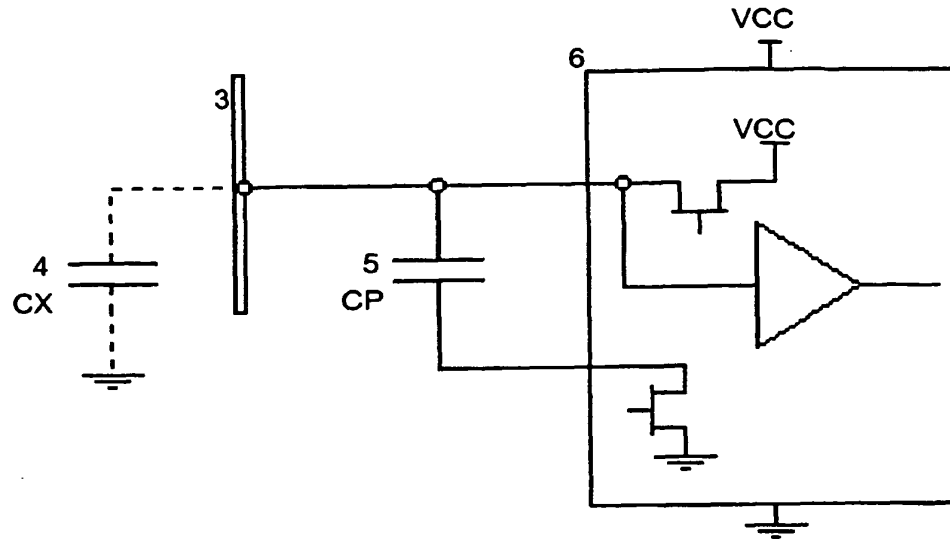


FIGURE 3

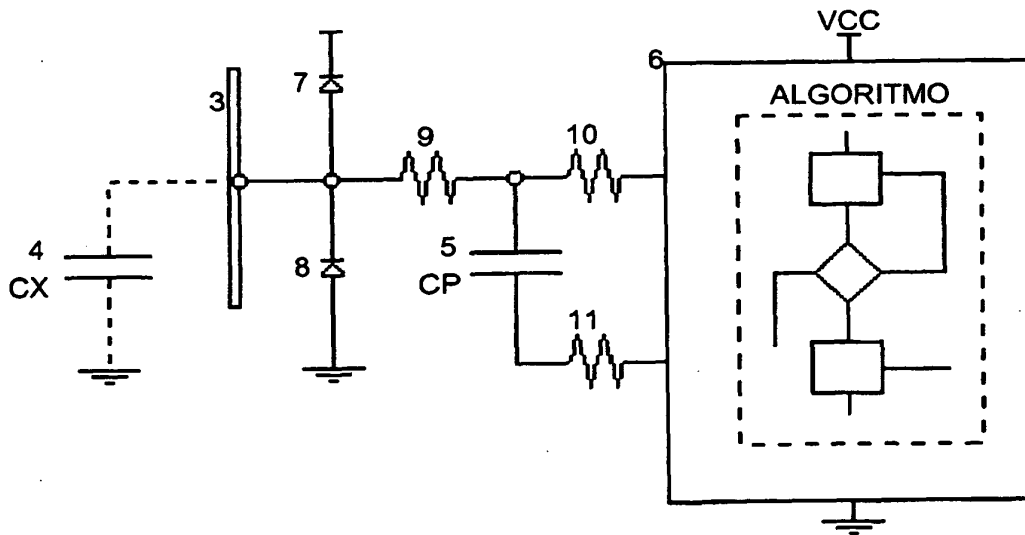


FIGURE 4

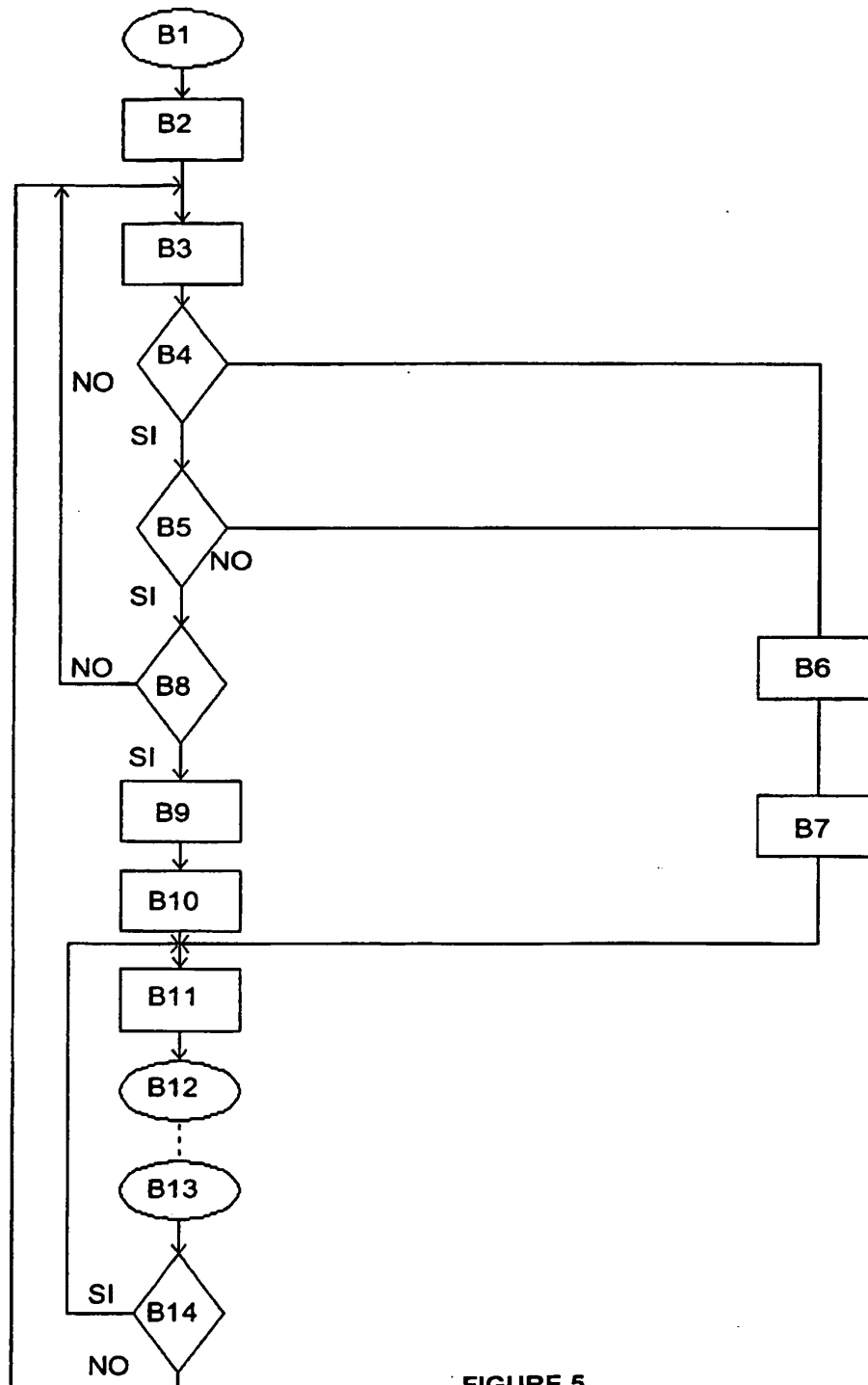


FIGURE 5

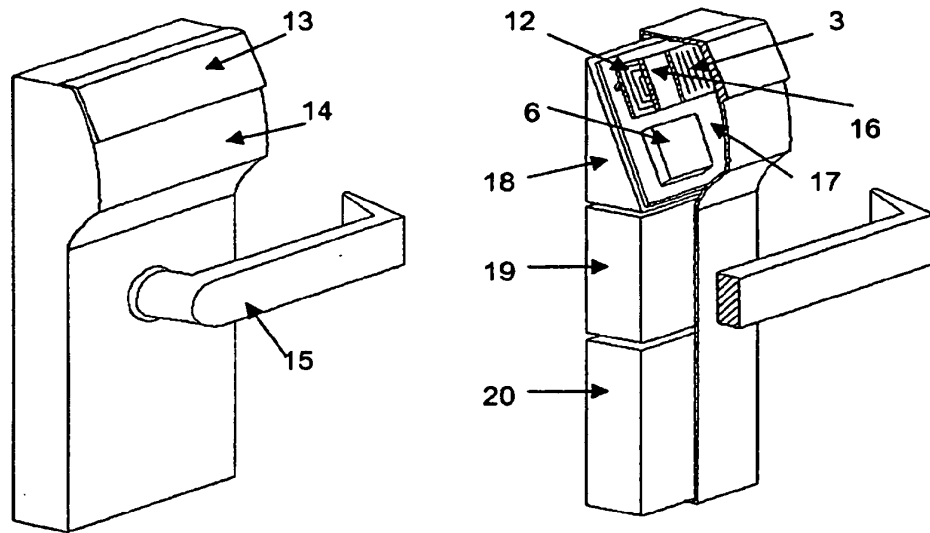


FIGURE 6

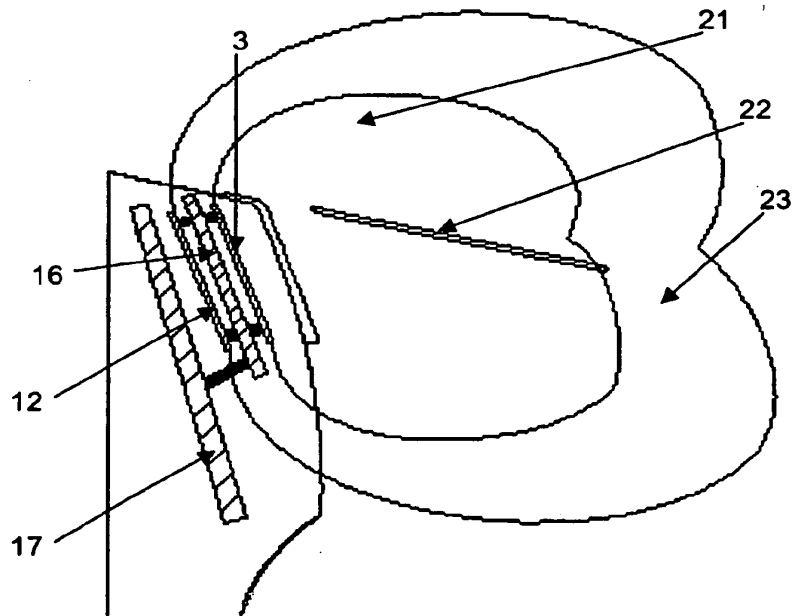


FIGURE 7

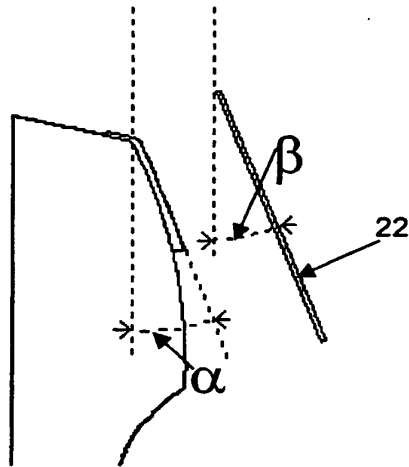


FIGURE 8

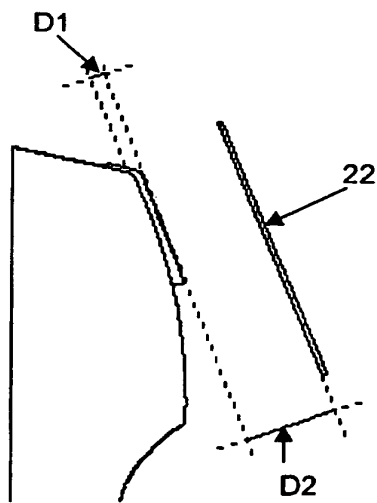


FIGURE 9

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 4717816 A [0002]
- ES 2112152 A1 [0005]
- EP 1026617 A1 [0006]
- JP 2001055852 B [0008]
- US 6362632 B [0009]

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
1 September 2005 (01.09.2005)

PCT

(10) International Publication Number
WO 2005/080720 A1

(51) International Patent Classification⁷: **E05B 49/00**

(21) International Application Number:
PCT/SE2005/000233

(22) International Filing Date: 21 February 2005 (21.02.2005)

(25) Filing Language: Swedish

(26) Publication Language: English

(30) Priority Data:
0400425-5 24 February 2004 (24.02.2004) SE

(71) Applicant (for all designated States except US): **TAG-MASTER AB** [SE/SE]; Kronborgsgränd 1, S-164 87 Kista (SE).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **WILLGERT, Mikael** [SE/SE]; Skiljevägen 23, S-163 54 Spånga (SE).

(74) Agents: **ÖRTENBLAD, Bertil** et al.; Noréns Patentbyrå AB, Box 10198, S-100 55 Stockholm (SE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

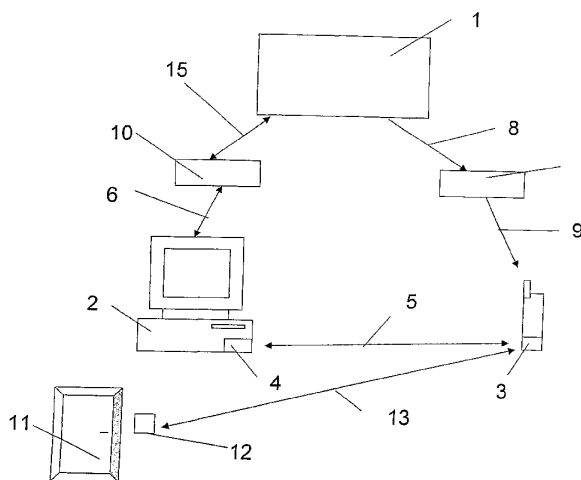
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD OF AUTHORIZATION



(57) Abstract: A method for granting access to arrangements (2; 11) such as computers, doors, vehicles or other arrangements to which access is required for a user, comprising the transmission of a code over a short-range radio link (5; 13). The invention is characterized in that an access code (an ID-code) is transmitted from a central computer (1) via radio waves to a radio terminal (3) that the user possesses, in that the radio terminal (3) is caused to transmit the said ID-code over the said short-range radio link (5; 13) to the said arrangement (2; 11), in that the said arrangement (2; 11) or a transmitter unit in the said arrangement is caused to transmit the said ID-code to the said central computer (1), and in that the said computer (1) is caused to compare the received code with the code that the computer (1) transmitted to the radio terminal (3).

Method for Authorization.

The present invention concerns a method for granting access.

5 Computers and mobile telephones are currently used as
equipment for carrying out transactions and for giving a
signature of different types. Furthermore, computers are used
to an ever greater degree to collect information with
different degrees of confidentiality. It is often sufficient
10 to log in with a password or a PIN code in order to
subsequently be able to carry out transactions or to handle
information during a limited period. This means that a
terminal may be open for unauthorised use if it is left
unmonitored or if it is stolen within a certain time from the
15 user having logged in.

In order to prevent this, there are requirements for codes or
for the use of a magnetic card or what is known as a "smart
card" as a means of identification. One disadvantage of such
20 systems is that the user often experiences these as awkward
and as a result of this often seeks to exploit shortcuts,
which reduces the level of security.

One problem with codes is that these can be read by
25 eavesdropping unless the information has been encrypted,
which may create a demand for particular software, hardware
or a password that is to be distributed such that it can be
used by the user.

30 The present invention solves this problem and offers a method
in which the identity of a user can be established with high
security.

The present invention thus relates to a method for granting access to devices such as computers, doors, vehicles or other arrangements to which access for a user is desired, comprising the transmission of a code over a short-range radio link, and it is characterised in that an access code (an ID-code) is transmitted from a central computer using radio waves to a radio terminal in the possession of the user, in that the radio terminal is caused to transmit the said ID-code over the said short-range radio link to the said arrangement, in that the said arrangement or a transmitter unit in the said arrangement is caused to transmit the said ID-code to the said central computer, and in that the said computer is caused to compare the received code with the code that the computer transmitted to the radio terminal.

The invention will be described in more detail below, partially in association with the embodiment of the invention shown in the attached drawing, where

- Figure 1 shows a block diagram in order to illustrate the invention.

The present invention thus concerns a method for granting access for arrangements such as computers, doors, vehicles or other arrangements to which it is desired that a user have access. The invention will be described below in association with an example in which access to a computer is desired and an example in which access to a locked door is desired. However, the invention can be exploited for all arrangements to which it is desired to grant access, such as vehicles, telephones, etc.

The method comprises the transmission to the arrangement of an ID-code over a short-range radio link.

According to the invention, an access code (an ID-code) is transmitted from a central computer 1 over radio waves to a radio terminal 3 in the possession of the user. The radio
5 terminal may be, for example and preferably, a mobile telephone. It may, however, for certain applications be constituted by a communication radio of the type, for example, that is used by the rescue services. For the example in which the radio terminal is a mobile telephone, the
10 transmission takes place over a telephone network 8, via a base station 7 to the telephone via radio 9.

Furthermore, the radio terminal 3 is caused to transmit the said ID-code over the said short-range radio link to the said
15 arrangement 2, as is illustrated by means of the arrow 5.

The said arrangement 2; 11, 12 or a transmitter unit in the said arrangement is thereafter caused to transmit the said ID-code to the said central computer 1 over a computer
20 network 6, 10, 15.

The said computer 1 is subsequently caused to compare the code that has been received with the code that the computer transmitted to the radio terminal.
25

A circuit has in this way been created in which a transmitted code can be compared with a received code. In the case that the codes agree with each other, the central computer 1 can, in the next stage, be caused to transmit a second code to the
30 arrangement 2 that makes it possible for the arrangement to be used in the manner intended by the user.

Since the central computer transmits an ID-code to a certain mobile telephone or other radio terminal, it can be assumed that the user of this mobile telephone is the person who transmits the code to the said arrangement over the said
5 short-range radio link. Alternatively, the circuit thus can be used in such a manner that a registration of whether the codes agree is made, which in this way can be assumed to specify that the correct person is using the arrangement, or that the use of the arrangement is unauthorised.

10

According to one preferred embodiment, the central computer 1 is initiated to transmit an ID-code to the radio terminal through either the arrangement or the radio terminal transmitting a request for a code to the central computer 1.
15 With respect to the arrangement, the request can be transmitted over the computer network 10, or, with respect to a mobile telephone, over the mobile telephone network 7, 8, 9.

20 It is naturally possible to initiate the said circuit at any freely chosen point, i.e. in the central computer 1, with the mobile telephone 3, or in the arrangement 2.

According to one preferred design, the said short-range radio
25 link is what is known as an "RFID" link of known type. Such links may work in two directions with two transmitting units and two receiving units, or they may work in one direction only such that one unit transmits an enquiry signal that is received by, modulated by, and reflected by the second part
30 in the form of a transponder. The said ID-code can, for example, be transmitted in this manner by means of the modulation.

According to an alternative preferred embodiment, the said short-range radio link is what is known as a "Bluetooth" link.

- 5 The said arrangement 2, 11 and the said radio terminal 3 have in both cases a transmitter/receiver unit 3, 4; 12 for the radio link.

10 According to one preferred design, the said radio terminal is a mobile telephone comprising one part of the said short-range radio link. The radio terminal is preferably a mobile telephone with an integral Bluetooth function.

15 A Bluetooth module is thus built into the arrangement 2, 11. It is also possible to use another radio technology such as WLAN (Wireless Local Area Network). However, it is important that the range of the radio link can be made sufficiently short, independently of the technology used, in order to activate only the arrangements that are intended.

20 According to one example, the said arrangement is a computer (2) or a computer terminal to which access is required.

25 In this design, the user can request via the computer 2 a code from the central computer 1 in order to be able to use the computer 2. This request can contain the ID number of the user. The central computer 1 thus transmits a code to the mobile telephone 7 of the user, which subsequently transmits the code over the radio link 5 to the computer 2. The
30 computer 2 transmits the code to the central computer 1. The central computer in this way receives confirmation that the correct code has been received by the computer, whereby the user can use the computer in the manner that is granted by

the said code. This may be a question of full or limited use, such as carrying out financial transactions.

According to a second example, the said arrangement is a door
5 11 or a gateway to which access is required such that it can be opened. In this case it is preferred that the said arrangement comprises a communicator 12 connected to the central computer 1, which communicator 12 is arranged to communicate with the said radio terminal 3 over a short
10 distance using an RFID link or a bluetooth link.

According to this example, it may be a question of rescue personnel being equipped with a radio terminal 3 in the form of a mobile telephone with an integral RFID link or bluetooth
15 link 13. The communicator 12 is also equipped with such a link. When a fire-fighter, for example, wishes to open the door, he rings to the central computer 1 over the telephone network 7, 8, 9 and transmits information about the door that is concerned. This can take place through a numerical
20 designation or through another unique identity. Alternatively, the telephone 3 communicates through the said link with the communicator whereby the number of the mobile telephone is transmitted to the communicator 12. In the latter case, the information is transmitted from the
25 communicator 12 to the central computer 1. In both cases, the central computer 1 subsequently transmits a code to the mobile telephone that, once it has received the code, transmits it to the communicator 12 over the said link, whereby the door can be opened.

30

It is clear that, both in the case with a computer 2 and in the case with a door 11, that the code can vary with time, in the case in which the central computer transmits the code to

the radio terminal 3 and to the arrangement 2; 11. Variation in time makes unauthorised use through eavesdropping of the code significantly more difficult.

5. According to one preferred embodiment the arrangement 2; 11 may be arranged to compare the codes received from the computer 1 and from the radio terminal 3.

According to one preferred design, the code transmitted to
10 the central computer comprises a network address belonging to the arrangement 2; 11. This means that the arrangement is identified for the central computer, and this not only facilitates the transmission of a code from the central computer 1 to the arrangement, it also increases the security
15 in the system against unauthorised use.

According to one design, the system can be used to ensure that, for example, the right people enter a meeting room. In this case, a person's transponder in the form of an RFID
20 circuit or a bluetooth circuit in the mobile telephone of the person is read by a communicator at the door of the room. The communicator transmits to the central computer a code that refers to the transponder. The central computer transmits a temporary code to the mobile telephone of the person, which
25 mobile telephone sends the code onwards to the central computer through the communicator. A circuit has in this way been created, in which the central computer has information about the said temporary code, the person's mobile telephone number coupled to that code that was initially read, and the
30 name of the person.

According to another preferred embodiment the said code is used to encrypt information that is transmitted from the

arrangement to the central computer. The code can in this way comprise an encryption key. This further increases the security against the unauthorised use of a code that has been read by eavesdropping.

5

According to a further preferred embodiment, the said arrangement 2; 11 comprises a reading arrangement 4; 12 in order to read biometric data from the said user and in order to cause the said arrangement 2; 11 to transmit biometric data to the central computer 1. Such biometric data is transmitted to the central computer 1 for comparison with reference data previously stored in the central computer in order to further increase the security that it is the correct person that is using the radio terminal or the computer 2.

10

The said reading arrangement 4; 12 for reading biometric data from the said user may be a reading arrangement known per se of suitable type, such as for reading fingerprints or the iris of the eye.

20

A number of designs have been described above. It is, however, clear that the invention can be varied, for example with respect to the location at which the circuit is initiated and started, as can the number of different arrangements that form the said circuit be varied.

25

The present invention, therefore, is not to be seen as limited to the embodiments specified above, since the invention can be varied within the scope of the attached claims.

Claims.

1. A method for granting access to arrangements (2; 11) such as computers, doors, vehicles or other arrangements to which
5 access is required for a user, comprising the transmission of a code over a short-range radio link (5; 13),
c h a r a c t e r i z e d in that an access code (an ID-code) is transmitted from a central computer (1) via radio waves to a radio terminal (3) that the user possesses, in
10 that the radio terminal (3) is caused to transmit the said ID-code over the said short-range radio link (5; 13) to the said arrangement (2; 11), in that the said arrangement (2; 11) or a transmitter unit in the said arrangement is caused to transmit the said ID-code to the said central computer
15 (1), and in that the said computer (1) is caused to compare the received code with the code that the computer (1) transmitted to the radio terminal (3).
2. A method according to claim 1, c h a r a c t e r i z e d
20 in that the central computer (1) is caused to transmit an ID-code to the radio terminal (3) through either the arrangement (2; 11) or the radio terminal (3) being caused to transmit an enquiry for a code to the central computer (1).
- 25 3. A method according to claim 1 or 2,
c h a r a c t e r i z e d in that the said radio terminal (3) is a mobile telephone comprising one part of the said short-range radio link (5; 13).
- 30 4. A method according to claim 1, 2 or 3,
c h a r a c t e r i z e d in that the said short-range radio link (5; 13) is what is known as an "RFID" link.

5. A method according to claim 1, 2, 3 or 4,
c h a r a c t e r i z e d in that the said short-range radio
link (5; 13) is what is known as a "Bluetooth" link.

5 6.. A method according to claim 1, 2, 3, 4 or 5,
c h a r a c t e r i z e d in that the said arrangement is a
computer (2) or a computer terminal to which access is
desired.

10 7. A method according to claim 1, 2, 3, 4 or 5,
c h a r a c t e r i z e d in that the said arrangement is a
door (11) or gateway to which access is desired such that it
can be opened.

15 8. A method according to claim 1, 2, 3, 4, 5 or 6,
c h a r a c t e r i z e d in that the arrangement (2; 11) is
arranged to compare the code received from the computer (1)
and that received from the radio terminal (3).

20 9. A method according to claim 7, c h a r a c t e r i z e d
in that the said arrangement (11) comprises a communicator
(12) connected to the central computer (1), which
communicator is arranged to communicate at short range with
the said radio terminal (3) by RFID link or by Bluetooth
25 link.

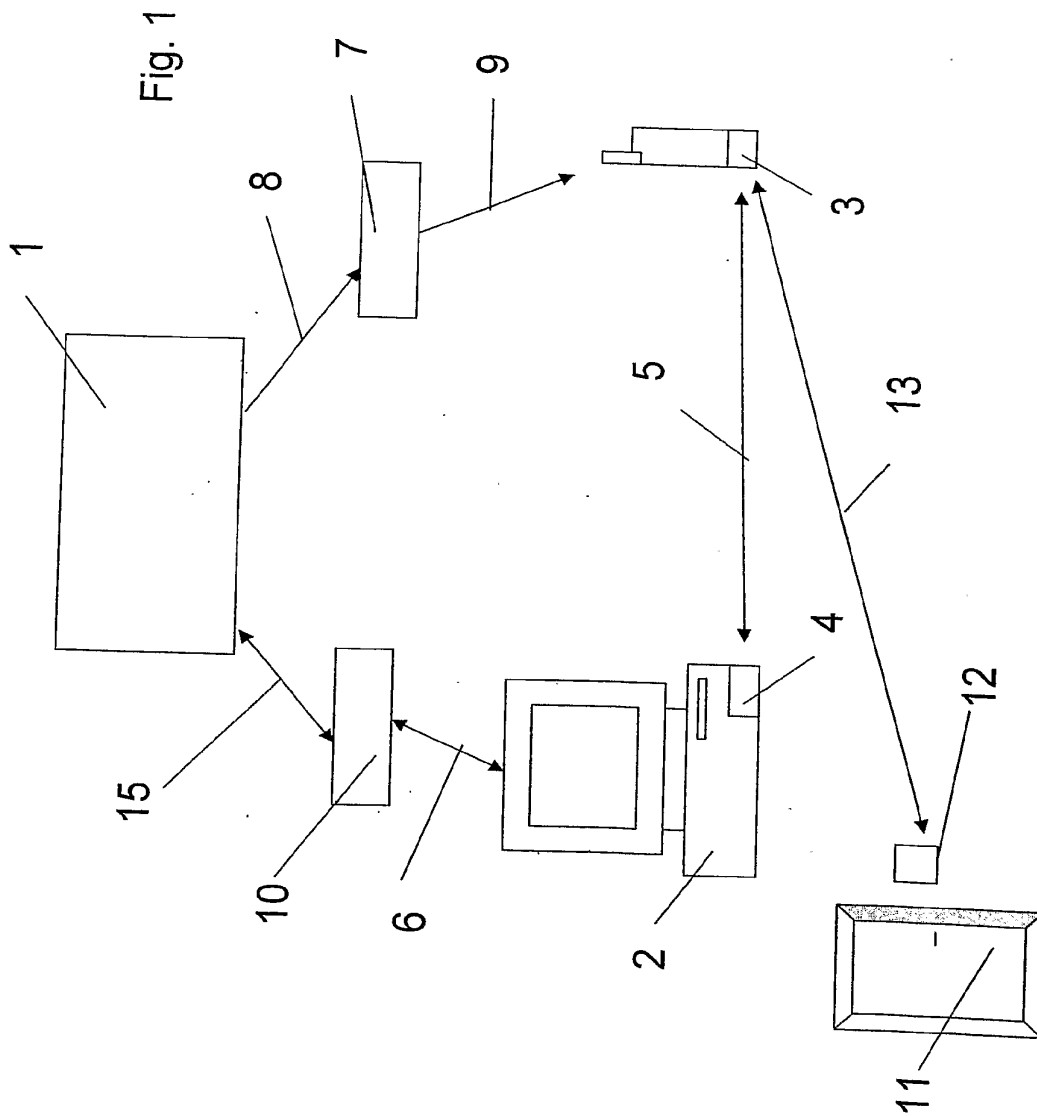
10. A method according to claim 1, 2, 3, 4, 5, 7, 8 or 9,
c h a r a c t e r i z e d in that the code transmitted from
the arrangement (2; 11) to the central computer (1) comprises
30 a network address belonging to the arrangement (2;11).

11. A method according to any one of the preceding claims,
c h a r a c t e r i z e d in that the said code is used to

encrypt information that is transmitted from the arrangement (2; 11) to the central computer (1).

12. A method according to any one of the preceding claims,
5 c h a r a c t e r i z e d in that the arrangement (2; 11) comprises a reading arrangement (4; 12) for the reading of biometric data from the said user, and in that the said arrangement (2; 11) is caused to transmit biometric data to the central computer(1).

//



INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 2005/000233

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: E05B 49/00
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)

IPC7: E05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5134392 A (TAKEUCHI, M ET AL), 28 July 1992 (28.07.1992), the whole document --	1-12
A	WO 0123694 A1 (TACTEL AB), 5 April 2001 (05.04.2001), the whole document --	1-12
A	WO 02084896 A1 (TAGMASTER AB), 24 October 2002 (24.10.2002), the whole document -- -----	1-12

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search
16 May 2005

Date of mailing of the international search report
19 -05- 2005

Name and mailing address of the ISA/
Swedish Patent Office
Box 5055, S-102 42 STOCKHOLM
Facsimile No. +46 8 666 02 86

Authorized officer
Rune Bengtsson /LR
Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 2005/000233

US	5134392	A	28/07/1992	DE	3820248 A,C	05/01/1989
				JP	2546842 B	23/10/1996
				JP	63312480 A	20/12/1988
				JP	64054643 U	04/04/1989

WO	0123694	A1	05/04/2001	AU	7697300 A	30/04/2001

WO	02084896	A1	24/10/2002	AU	6646301 A	13/03/2002
				EP	1380118 A	14/01/2004
				SE	521480 C	04/11/2003
				SE	0101357 A	19/10/2002
				US	6836154 B	28/12/2004
				US	20030155947 A	21/08/2003
				US	20050042986 A	24/02/2005

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 16/034,278	
APPLICATION AS FILED - PART I							
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	75		N/A	
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	330		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	380		N/A	
TOTAL CLAIMS (37 CFR 1.16(j))	7	minus 20 = *	x 50 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1	minus 3 = *	x 230 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
			TOTAL	785		TOTAL	
* If the difference in column 1 is less than zero, enter "0" in column 2.							
APPLICATION AS AMENDED - PART II							
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY	
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=
	Application Size Fee (37 CFR 1.16(s))						
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	
(Column 1)		(Column 2)		(Column 3)		OTHER THAN SMALL ENTITY	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=
	Application Size Fee (37 CFR 1.16(s))						
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	
						TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.							



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
16/034,278	07/12/2018		785	LBT0010-CON3	7	1

CONFIRMATION NO. 8554

FILING RECEIPT



0000000101871040

67050
KASHA LAW LLC
14532 Dufief Mill Road
North Potomac, MD 20878

Date Mailed: 08/15/2018

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Chris Outwater, Carpinteria, CA;
William Gibbens Redmann, Glendale, CA;

Applicant(s)

Liberty PlugIns, Inc., Santa Barbara, CA;

Assignment For Published Patent Application

Liberty PlugIns, Inc., Santa Barbara, CA

Power of Attorney: The patent practitioners associated with Customer Number 67050

Domestic Priority data as claimed by applicant

This application is a CON of 15/609,055 05/31/2017 PAT 10049514
which is a CON of 15/178,849 06/10/2016 PAT 9911258
which is a CON of 14/603,434 01/23/2015 PAT 9373205
which is a CON of 13/582,467 09/04/2012 PAT 8996876
which is a 371 of PCT/US11/26781 03/02/2011
which claims benefit of 61/309,813 03/02/2010

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: No

Permission to Access Search Results: No

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 08/13/2018

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 16/034,278**

Projected Publication Date: 11/22/2018

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

Access Control System and Method for Use by an Access Device

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

page 2 of 4

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA/82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	
Filing Date	
First Named Inventor	Chris Outwater
Title	An Access Control System and Method for Use by an Access Device
Art Unit	
Examiner Name	
Attorney Docket Number	LBT0010-CON

SIGNATURE of Applicant or Patent Practitioner

Signature	/John R. Kasha/	Date (Optional)	
Name	John R. Kasha	Registration Number	53100
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.



*Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number

Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)



I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above:

67050

OR



I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter to:



The address associated with the above-mentioned Customer Number

OR



The address associated with Customer Number:

OR

Firm or
Individual Name

Address

City

State

Zip

Country

Telephone

Email

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

Liberty PlugIns, Inc.



Inventor or Joint Inventor (title not required below)



Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)



Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)



Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature

Date (Optional)

Name

Chris Outwater

Title

President, Liberty PlugIns, Inc.

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.



Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

POWER OF ATTORNEY BY APPLICANT

No more than ten (10) patent practitioners total may be appointed as set forth below by name and registration number. This page need not be submitted if appointing the Patent Practitioner(s) associated with a Customer Number (see form PTO/AIA/82B):

Name	Registration Number

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	LBT0010-CON3
		Application Number	
Title of Invention	Access Control System and Method for Use by an Access Device		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor	1				Remove	
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	Chris		Outwater			
Residence Information (Select One) • US Residency Non US Residency Active US Military Service						
City	Carpinteria	State/Province	CA	Country of Residence	US	
Mailing Address of Inventor:						
Address 1	3340 Foothill Rd.					
Address 2						
City	Carpinteria	State/Province	CA			
Postal Code	93013	Country	US			
Inventor	2				Remove	
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	William	Gibbens	Redmann			
Residence Information (Select One) • US Residency Non US Residency Active US Military Service						
City		State/Province		Country of Residence		
Mailing Address of Inventor:						
Address 1	1202 Princeton Dr.					
Address 2						
City	Glendale	State/Province	CA			
Postal Code	91205	Country	US			
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.						
Add						

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	LBT0010-CON3
		Application Number	
Title of Invention	Access Control System and Method for Use by an Access Device		

☐ An Address is being provided for the correspondence information of this application.

Customer Number	67050		
Email Address	john.kasha@kashalaw.com	Add Email	Remove Email

Application Information:

Title of the Invention	Access Control System and Method for Use by an Access Device		
Attorney Docket Number	LBT0010-CON3	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	7	Suggested Figure for Publication (if any)	4

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not be** the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	67050		

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	LBT0010-CON3
		Application Number	
Title of Invention	Access Control System and Method for Use by an Access Device		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the application number blank.

Prior Application Status	Pending				Remove
Application Number	Continuity Type		Prior Application Number	Filing Date (YYYY-MM-DD)	
	Continuation of		15609055	2017-05-31	
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15609055	Continuation of	15178849	2016-06-10	9911258	2018-03-06
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15178849	Continuation of	14603434	2015-01-23	9373205	2016-06-21
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14603434	Continuation of	13582467	2012-09-04	8996879	2015-03-31
Prior Application Status	Expired				Remove
Application Number	Continuity Type		Prior Application Number	Filing Date (YYYY-MM-DD)	
13582467	a 371 of international		PCT/US11/26781	2011-03-02	
Prior Application Status	Expired				Remove
Application Number	Continuity Type		Prior Application Number	Filing Date (YYYY-MM-DD)	
PCT/US11/26781	Claims benefit of provisional		61309813	2010-03-02	
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.					Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)ⁱ the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

				Remove
Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	LBT0010-CON3
		Application Number	
Title of Invention	Access Control System and Method for Use by an Access Device		
Additional Foreign Priority Data may be generated within this form by selecting the Add button. Add			

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013. NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices
If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application. In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application. In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	LBT0010-CON3
		Application Number	
Title of Invention	Access Control System and Method for Use by an Access Device		

Applicant	1 Remove		
If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section. Clear			
☒ Assignee		Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.		Person who shows sufficient proprietary interest	
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:			
Name of the Deceased or Legally Incapacitated Inventor :			
If the Applicant is an Organization check here. ☒			
Organization Name	Liberty Plugins, Inc.		
Mailing Address Information For Applicant:			
Address 1	1482 East Valley Road, Suite 329		
Address 2			
City	Santa Barbara	State/Province	CA
Country	US	Postal Code	93108
Phone Number		Fax Number	
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button. Add			

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.			
Assignee	1 Remove		
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.			
If the Assignee or Non-Applicant Assignee is an Organization check here. ☒			

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	LBT0010-CON3
		Application Number	
Title of Invention	Access Control System and Method for Use by an Access Device		

Organization Name	Liberty PlugIns, Inc.
-------------------	-----------------------

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1	1482 East Valley Road, Suite 329		
Address 2			
City	Santa Barbara	State/Province	CA
Country i	US	Postal Code	93108
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Signature	/Kelly L. Kasha/		Date (YYYY-MM-DD)	2018-07-12	
First Name	Kelly L.	Last Name	Kasha	Registration Number	47743

Additional Signature may be generated within this form by selecting the Add button.

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		Access Control System and Method for Use by an Access Device		
First Named Inventor/Applicant Name:		Chris Outwater		
Filer:		John Kasha/Kelly Kasha		
Attorney Docket Number:		LBT0010-CON3		
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
UTILITY FILING FEE (ELECTRONIC FILING)	4011	1	75	75
UTILITY SEARCH FEE	2111	1	330	330
UTILITY EXAMINATION FEE	2311	1	380	380
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				785

Electronic Acknowledgement Receipt	
EFS ID:	33167082
Application Number:	16034278
International Application Number:	
Confirmation Number:	8554
Title of Invention:	Access Control System and Method for Use by an Access Device
First Named Inventor/Applicant Name:	Chris Outwater
Customer Number:	67050
Filer:	John Kasha/Kelly Kasha
Filer Authorized By:	John Kasha
Attorney Docket Number:	LBT0010-CON3
Receipt Date:	12-JUL-2018
Filing Date:	
Time Stamp:	20:17:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$785
RAM confirmation Number	071318INTEFSW20184300
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Specification	LBT0010-CON3_specification_final.pdf	138545	no	20
			71382170a0602f2f427b3124e78f2cbae6b257c9		
Warnings:					
Information:					
2	Drawings-only black and white line drawings	LBT0010-CON3_drawings_pct.pdf	169273	no	7
			c678e02d2ab13683a7488d728970a4f75dec3b25d		
Warnings:					
Information:					
3	Oath or Declaration filed	LBT0010-CON_dec_signed.pdf	735879	no	2
			d0e22911e55b78e4c926f817836288f691d95070		
Warnings:					
Information:					
4	Power of Attorney	LBT0010-CON_poa_signed.pdf	424556	no	3
			5d807b18a354b9acc0eed8ab8cd15f11391cd95c		
Warnings:					
Information:					
5	Application Data Sheet	LBT0010-CON3_app_data_sheet.pdf	1895228	no	7
			03f21cccd92ac4750399690f260469d758a6efd6		
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	35168	no	2
			9b454776a87dc54c080638da125b3ecae4db0d75		
Warnings:					
Information:					

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

ACCESS CONTROL SYSTEM AND METHOD FOR USE BY AN ACCESS DEVICE

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application is a continuation of U.S. Patent Application No. 15/609,055, filed May 31, 2017, which is a continuation of U.S. Patent Application No. 15/178,849, filed June 10, 2016, now U.S. Patent No. 9,911,258, which is a continuation of U.S. Patent Application No. 14/603,434, filed January 23, 2015, now U.S. Patent No. 9,373,205, which is a continuation of U.S. Patent Application No. 13/582,467, filed September 4, 2012, now U.S. Patent No. 8,996,879, which is a national stage application of PCT Application No. PCT/US11/26781, filed March 2, 2011, which claims the benefit of U.S. Provisional Patent Application No. 61/309,813, filed March 2, 2010. All of the above mentioned applications are incorporated by reference herein in their entireties.

INTRODUCTION

[0002] Electric vehicles are rapidly gaining in popularity. With these electric vehicles, charge points, or 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.

[0003] 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.

[0004] 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 cellular 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.

[0005] Burger in U.S. Published Patent Application number 2010/0031043 teaches a portable 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.

[0006] 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 cellular telephone which could then further transfer this token to the charger to authorize charging.

SUMMARY OF THE INVENTION

[0007] The present invention relates to the use of a web site and a cellular 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 cellular 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 cellular telephone. This certificate may comprise a unique ID and/or a date/time stamp.

[0008] 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.

[0009] 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.

[0010] 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.

[0011] If a wireless device, such as a laptop or smart phone, is used to carry the certificate, it can be running an application that turns on short-range wireless capability as the reservation time approaches. For simplicity in the following discussion, the term `smart phone` is used, but will be understood to include any portable computer or PDA, having a wireless communication ability.

[0012] As the smart phone approaches the charger or access device, a wireless connection is made (e.g., via Bluetooth.TM., Zigbee.TM., or IRDA); 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 inopportunistically placed truck 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.)

[0013] 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.

[0014] 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.TM. 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 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

- [0015] Attention is now directed to several illustrations that show some of the features of the present invention.
- [0016] FIG. 1 shows a flow diagram of a reservation and charge from a web-enabled charger.
- [0017] FIG. 2 shows an embodiment of a digital token or certificate.
- [0018] FIG. 3 shows a similar flow diagram to that of FIG. 1, except that the charger is not web-enabled.
- [0019] FIG. 4 shows the flow with a web-enabled hotel room lock.
- [0020] FIG. 5 shows the flow of FIG. 3 with a hotel room lock that is not web-enabled.
- [0021] FIG. 6 shows a block diagram of a charger that might be used with the present invention.
- [0022] FIG. 7 shows a block diagram of an embodiment of a smart phone application.
- [0023] 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

[0024] 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 cellular telephone or smart phone.

[0025] 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 smart phone 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.

[0026] 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.

[0027] 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 portable terminal, e.g., a cellular telephone or smart phone 4 that the user

specifies (which may be 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 should 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).

[0028] 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 cellular 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.

[0029] 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, passcodes, 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.

[0030] 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.

[0031] FIG. 2 shows a sample certificate 14 (one embodiment of certificate 5) containing several fields of data representative of the reservation:

[0032] 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;

[0033] Start Time: this can be in plaintext so that the smart phone application can read it also;

[0034] Duration/End Time: if the reservation is not just for a predetermined time like all day for example;

[0035] Service Type: for example level 1 charging vs. level 2, if the charger supports multiple services.

[0036] 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.

[0037] 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.

[0038] 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.

[0039] 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.

[0040] 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 cellular telephone 4, laptop 2, computer or other Internet device. The room can be paid for in the usually 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. 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.

[0041] 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 cellular 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 cellular telephone call or with Wi-Fi or the like.

[0042] Optionally, the application on a smart phone 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.

[0043] In US Patent Application Publication 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. FIG. 7 shows how the present invention represents an improvement to the system and method of Rollert et al., enabled by a smart phone application that could, for example, run on an iPhone by Apple, Inc. of Cupertino, Calif. or other smart phone. 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.

[0044] 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.

[0045] 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 micropayments 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 micropayment accounts for each patron and apply their funds to charges for parking. The micropayment accounts would be settled daily or with a different period, or whenever the pre-charged amount has been consumed.

[0046] Once the patron's account has been enabled, the patron can access the views for creating a new reservation.

- [0047] The New Reservations 23 screen accepts a start-time, an end-time (or duration), and a destination.
- [0048] 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.
- [0049] 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.
- [0050] 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.
- [0051] Alternatively, the spots may be shown in a list, which may be sorted by their distance from the indicated destination, or by price, or a combination thereof.
- [0052] 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).

[0053] 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.

[0054] 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.

[0055] 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.

[0056] 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.

[0057] 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.

[0058] 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.

[0059] 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.

WHAT IS CLAIMED IS:

1. An access control system comprising:

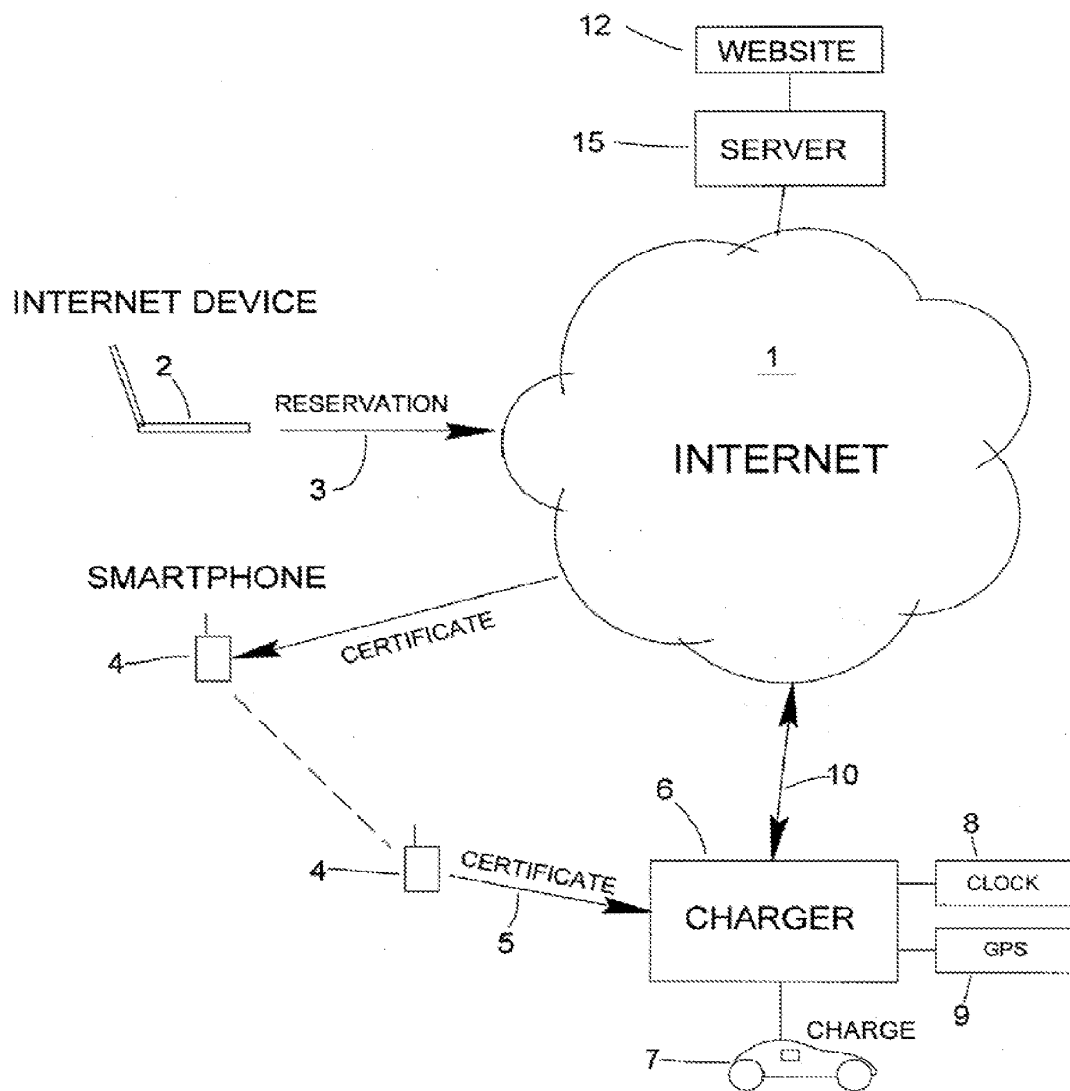
- a) an access device comprising a communication module connected to a processor having control of a door lock;
- b) a secure reservation interface to receive a reservation request from a first device for a reservation at a given destination;
- c) a reservation server, in communication with the reservation interface via a network, to:
 - receive the reservation request for the destination;
 - present a destination map for the destination, the destination map comprising markings for a plurality of selectable locations at the destination;
 - receive a request for a given selectable location at the destination;
 - issue a reservation certificate describing an interval of a reservation based on the reservation request and the selected location; and
 - transmit, from the reservation server to a second device distinct from the first device, the reservation certificate and a communication setting corresponding to the access device;
- d) an application installed on the second device to receive the reservation certificate and the communication setting corresponding to the access device, wherein the application wirelessly transmits the reservation certificate to the access device using the communication setting upon receipt of a command to activate the door lock; and
- e) wherein the access device receives the reservation certificate from the application based on use by the application of the communication setting, and the processor activates the door lock based on at least the receipt of the reservation certificate.

2. The system of claim 1 wherein the access device comprises a unique identifier, and wherein at least the reservation certificate or the communication setting contains the unique identifier.
3. The system of claim 2 wherein at least a portion of the reservation certificate is encrypted and wherein the access device decrypts the encrypted portion of the reservation certificate.
4. The system of claim 1 wherein the reservation server receives a request for one or more amenities at the destination.
5. The system of claim 1 wherein the access device generates a record indicating that the processor activated the door lock.
6. The system of claim 1 wherein the reservation certificate automatically expires at the end of the interval of the reservation.
7. The system of claim 1 wherein the second device comprises a smartphone.

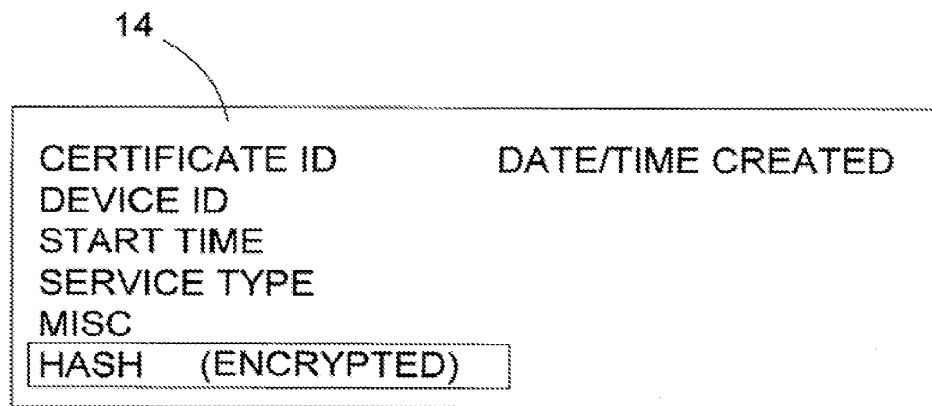
ABSTRACT OF THE DISCLOSURE

Systems and methods are provided to allow a smart phone or any terminal to activate a door lock 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 a processor and a communication module. The process has control of a door lock and is able to receive a reservation certificate presented by a portable terminal through the communication module. The processor activates the door lock when a current reservation certificate has been presented.

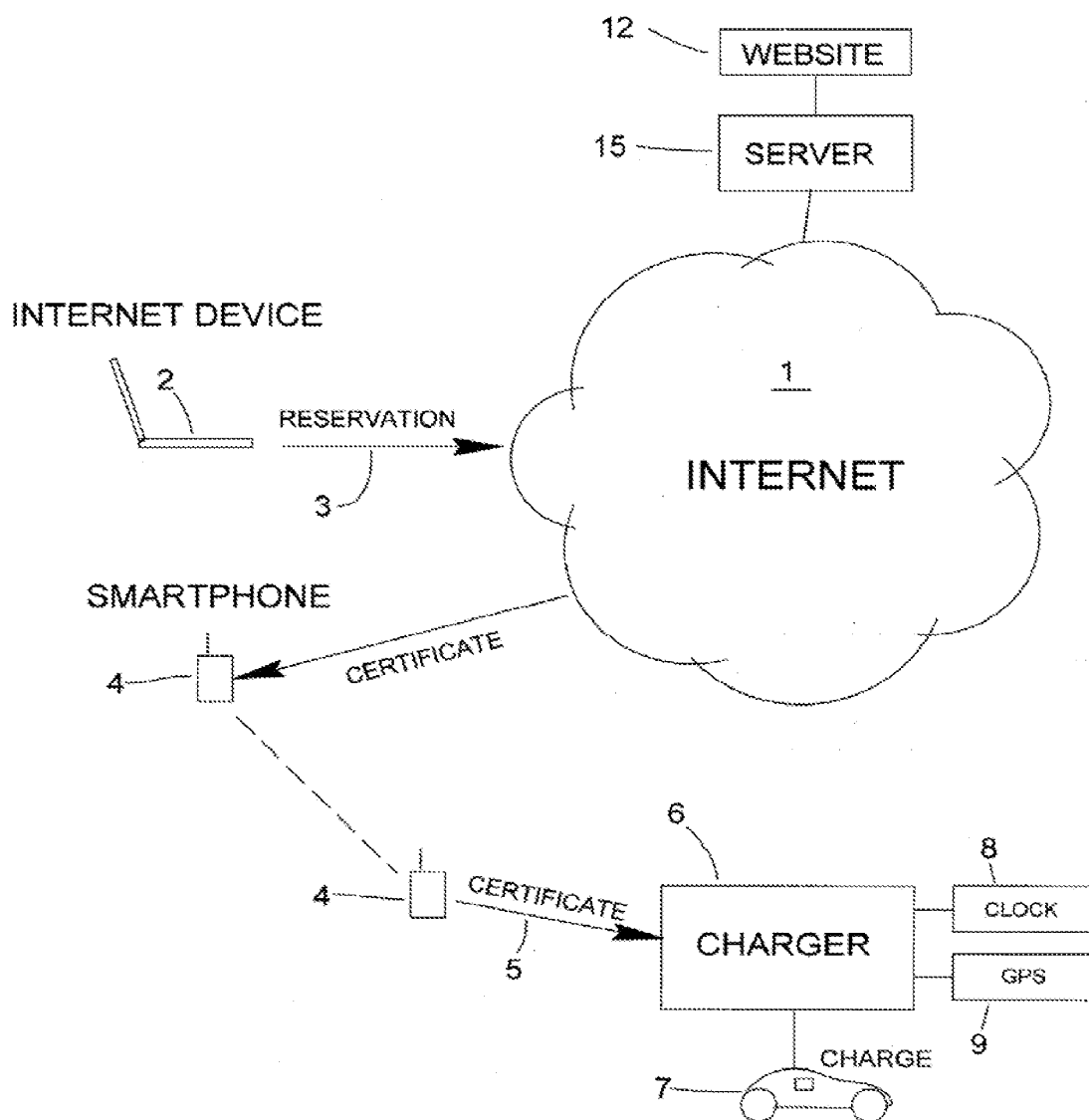
1/7

**FIG. 1**

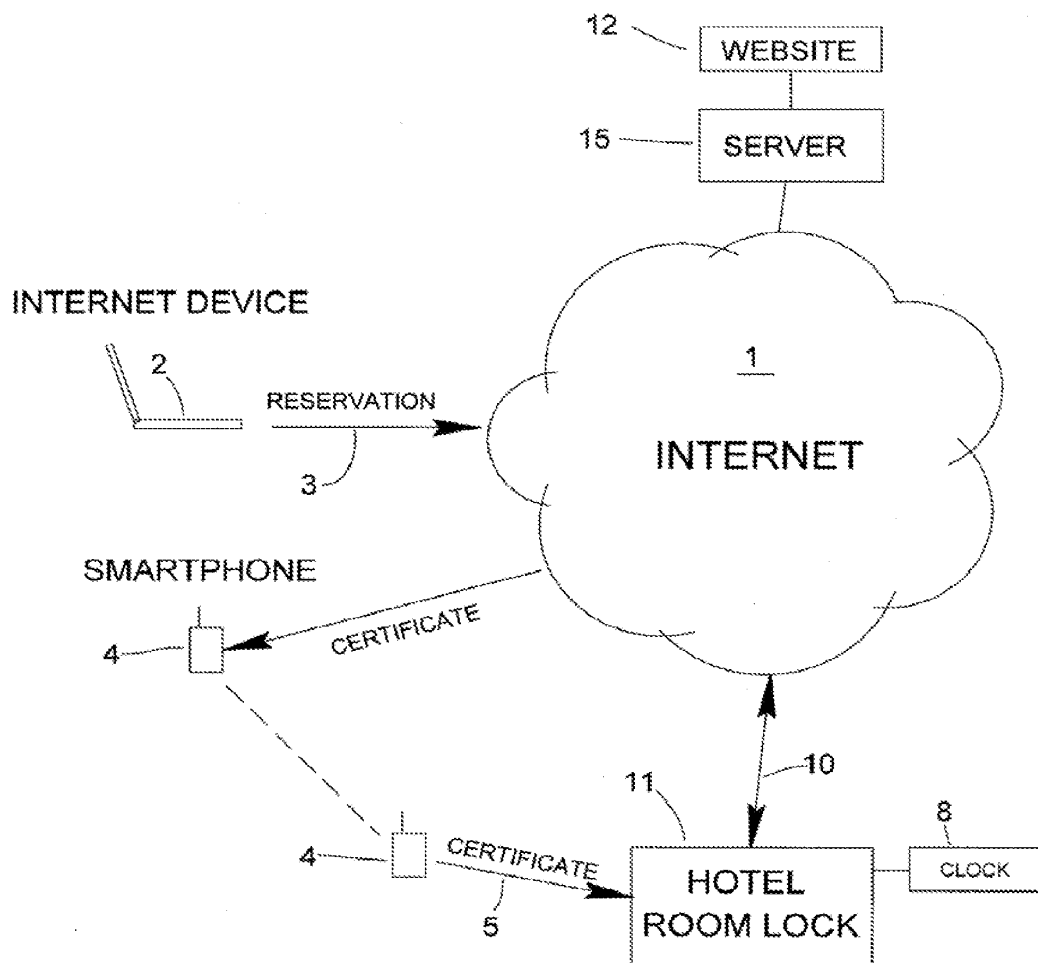
2/7

**FIG. 2**

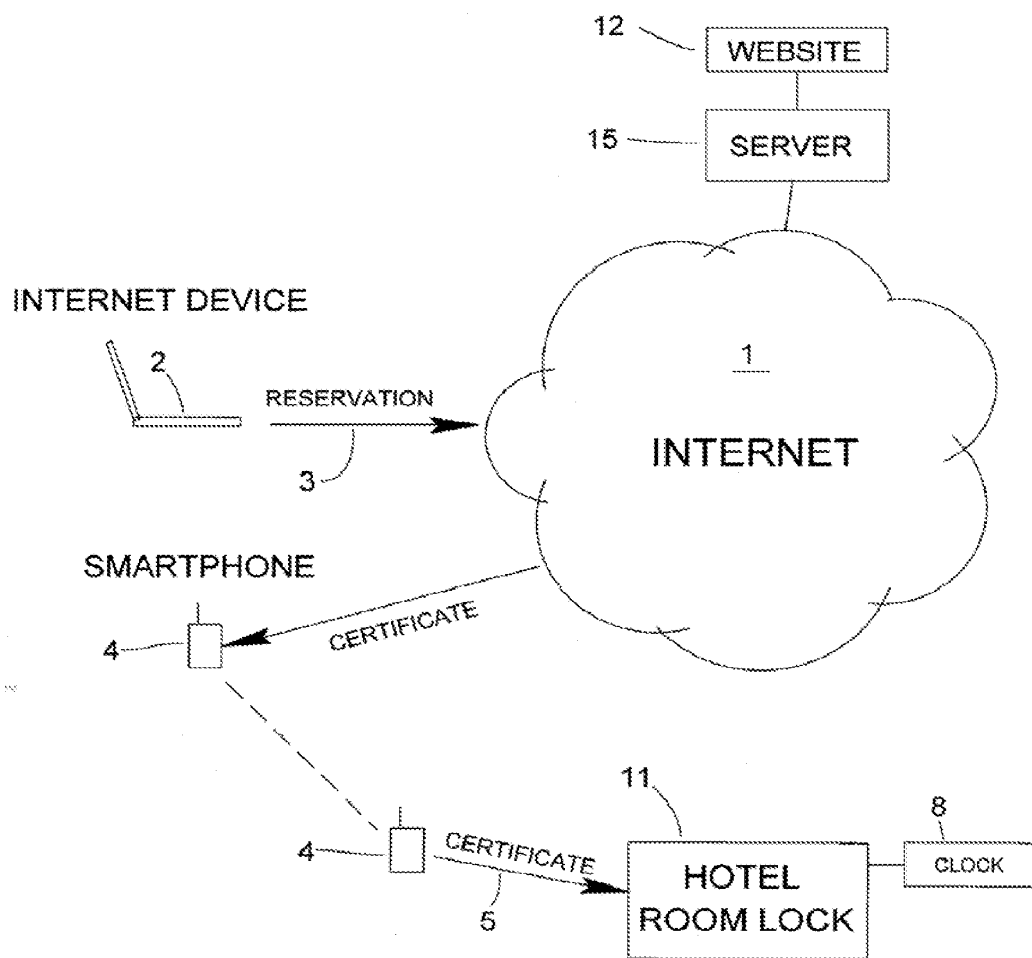
3/7

**FIG. 3**

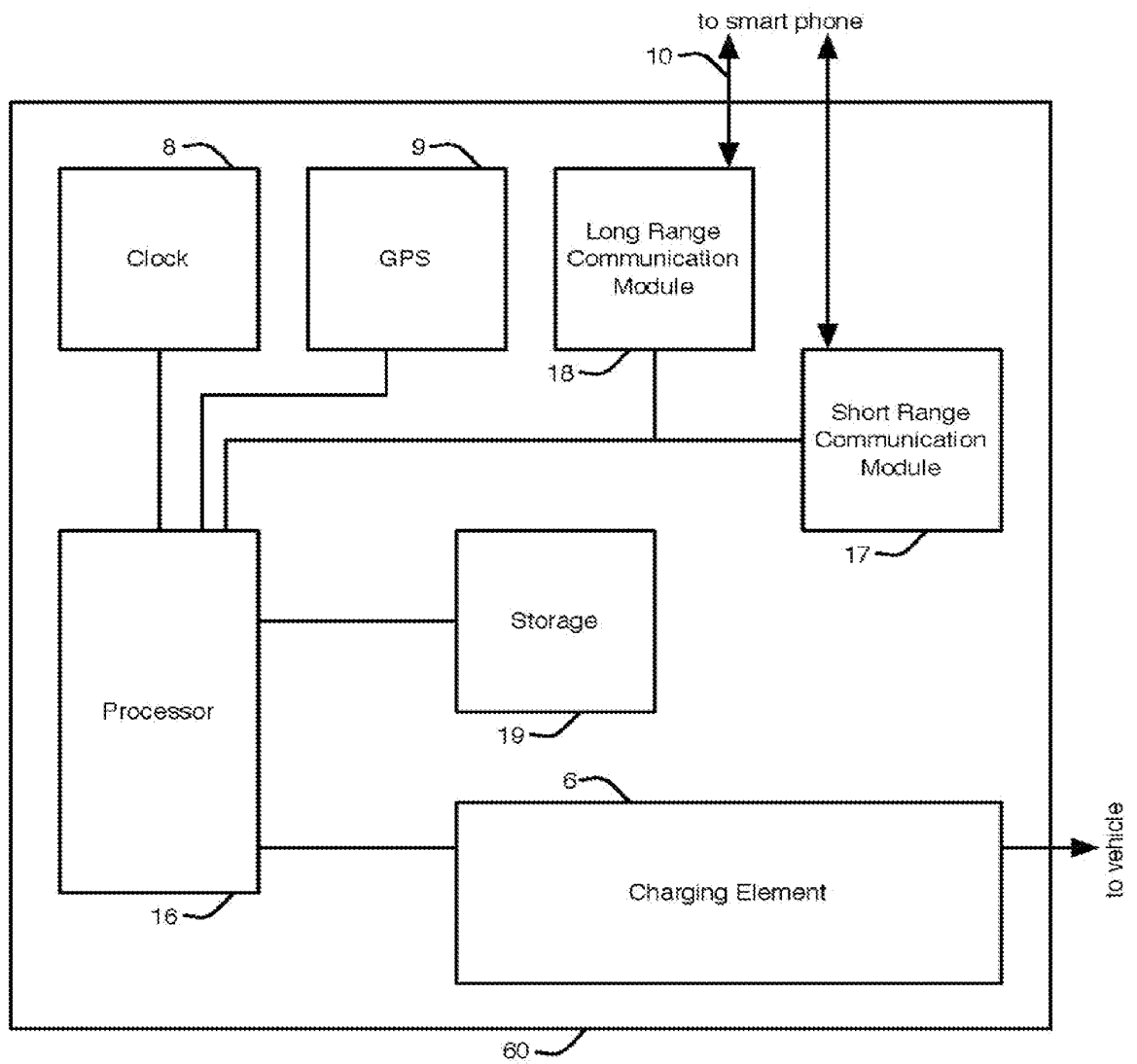
4/7

**FIG. 4**

5/7

**FIG. 5**

6/7

**FIG. 6**

7/7

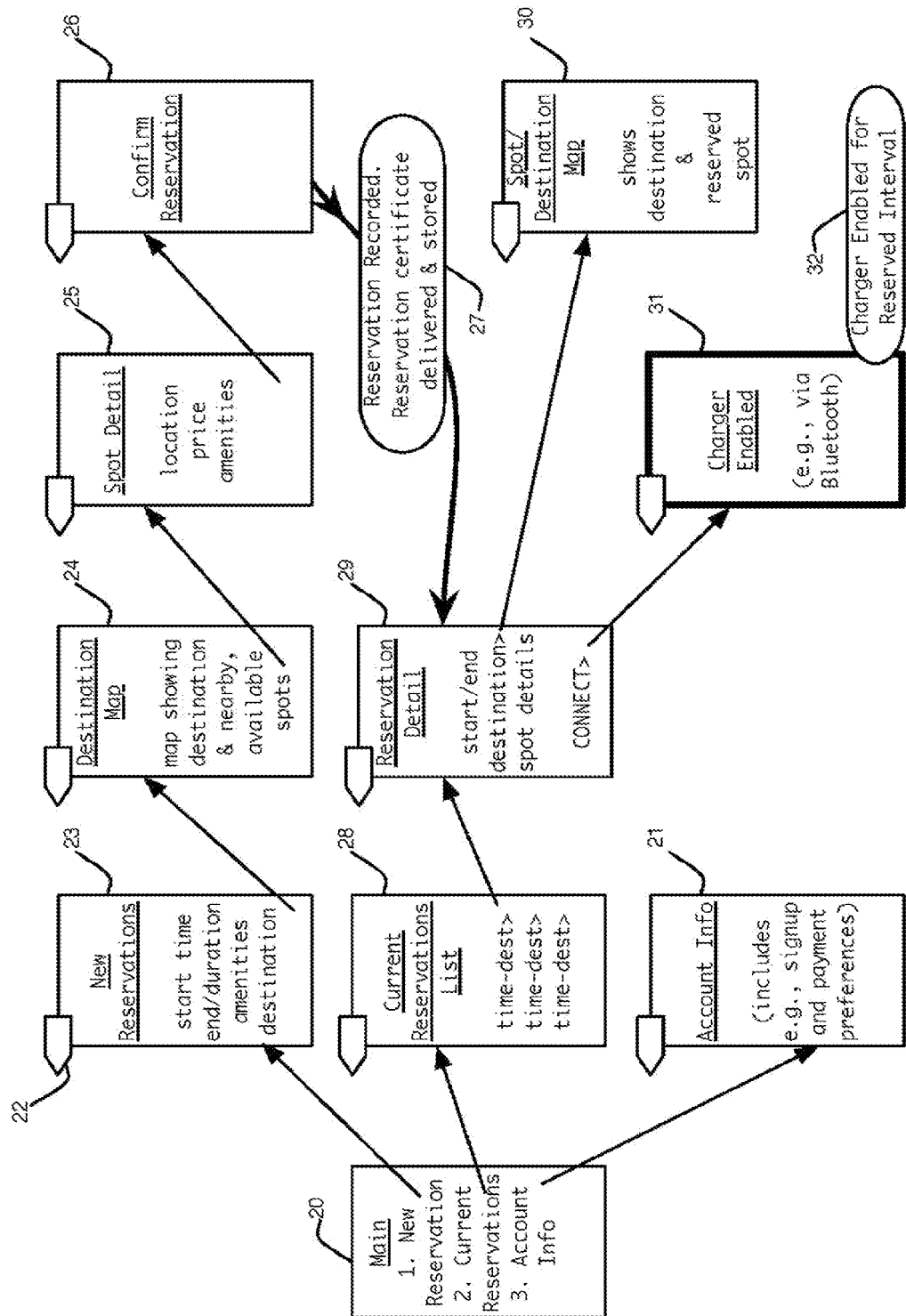
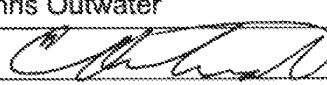


FIG. 7

SUBSTITUTE SHEET (RULE 26)

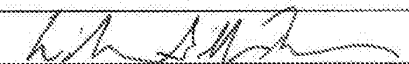
DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	An Access Control System and Method for Use by an Access Device
As the below named inventor, I hereby declare that: This declaration is directed to: ☒ The attached application, or ☐ United States application or PCT international application number _____ filed on _____ The above-identified application was made or authorized to be made by me. I believe that I am the original inventor or an original joint inventor of a claimed invention in the application. I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both. WARNING: Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.	
LEGAL NAME OF INVENTOR Inventor: <u>Chris Outwater</u> Date (Optional): _____ Signature: 	
Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9198 and select option 3.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	An Access Control System and Method for Use by an Access Device
As the below named inventor, I hereby declare that: This declaration is directed to: ☒ The attached application, or ☐ United States application or PCT international application number _____ filed on _____ The above-identified application was made or authorized to be made by me. I believe that I am the original inventor or an original joint inventor of a claimed invention in the application. I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both. WARNING: Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available. LEGAL NAME OF INVENTOR Inventor: <u>William Gibbens Redmann</u> Date (Optional): <u>20 Jan 2015</u> Signature: <u></u> Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.