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:	
Filer:	John Kasha
Attorney Docket Number:	LBT0010-CON-SE
Filed as Large Entity	
Filing Fees for Supplemental Examination	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
REQUEST FOR SUPPLEMENTAL EXAMINATION	1826	1	4620	4620
REEXAM ORDERED BASED ON SUPP EXAM	1827	1	12700	12700
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

ASSA ABLOY-HID EXHIBIT 1023
ASSA ABLOY-HID v. LIBERTY
IPR2023-00816

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**17320**

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.
96/000,367		9373205	LBT0010-CON-SE	7090

67050 7590 07/28/2021

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

EXAMINER	
ART UNIT	PAPER NUMBER

MAIL DATE	DELIVERY MODE
07/28/2021	PAPER

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 Noncompliant Supplemental Examination Request (37 CFR 1.610(d))	Application No. 96/000,367	Patent Under Reexamination 9373205	
	Examiner N/A	Central Reexamination Unit 3900	AIA Status No

The Central Reexamination Unit (CRU) in the United States Patent and Trademark Office (USPTO) has received a request for supplemental examination on 26 July 2021. The request cannot be processed, because the below-identified requirements for a supplemental examination request have not been satisfied. If a fully compliant request is not received within 15 days of the mailing date of this notice, then 1) the processing of the request will be terminated, and 2) the request will not be considered, will not be made part of the official record, and will remain closed from public view. **A filing date will NOT be assigned** to the request until the deficiencies noted below are corrected (37 CFR 1.610(d)), and the filing date of the request will be the receipt date of the corrected request that meets all applicable requirements:

The following items required by 37 CFR 1.610(a) and (b) are missing:

☐ 1. The fee for filing the request, as set forth in 37 CFR 1.20(k)(1).

☐ 2. The fee for reexamination ordered as a result of a supplemental examination proceeding, as set forth in 37 CFR 1.20(k)(2).

☐ 3. The applicable document size fees for non-patent documents as set forth in 37 CFR 1.20(k)(3). Specifically:

- ☐ (i). The fee set forth in 37 CFR 1.20(k)(3)(i) for each non-patent document between 21 - 50 pages in length.
- ☐ (ii). The fee set forth in 37 CFR 1.20(k)(3)(ii) for each additional 50 pages of the non-patent document, or a fraction thereof. This fee is charged in addition to the fee under 37 CFR 1.20(k)(3)(i).

☐ 4. An identification of the number of the patent for which supplemental examination is requested.

☐ 5. A list of the items of information that are requested to be considered, reconsidered or corrected. Where appropriate, the list must meet the requirements of § 1.98(b).

☐ 6. A list identifying any other prior or concurrent post-patent Office proceedings involving the patent for which supplemental examination is being requested.

☐ 7. An identification of each claim of the patent for which supplemental examination is being requested.

☑ 8. A separate, detailed explanation of the relevance and manner of applying each item of information to each claim of the patent for which supplemental examination is being requested.

☐ 9. A legible copy of the patent for which supplemental examination is requested and a legible copy of any disclaimer or certificate issued for the patent.

☐ 10. A legible copy of each item of information submitted as part of the request (other than U.S. patents or U.S. patent application publications, or items of information that form part of the discussion within the body of the request pursuant to 37 CFR 1.605(b)), accompanied by an English language translation of all the necessary and pertinent parts of any non-English language item of information.

☐ 11. A summary of the relevant portions of any submitted document, other than the request, that is over 50 pages in length. The summary must include citations to the particular pages containing the relevant portions.

☐ 12. An identification of the owner(s) of the entire right, title, and interest in the patent requested to be examined.

☐ 13. A submission by the patent owner in compliance with 37 CFR 3.73(c) establishing the entirety of the ownership in the patent requested to be examined.

☐ 14. Other: _____

☑ 15. Explanation of above item(s) and/or identification and explanation of other additional defects: See attached.

For inquiries regarding this supplemental examination, contact the Central Reexamination Unit at (571) 272-7705.

/MICHAEL FUELLING/ Supervisory Patent Examiner, Art Unit 3992	

The request does not comply with rule 1.610(b)(5).

A. The 3 CIP prosecution documents have not been applied to the claims. At most, these documents have been referenced, within the required detailed explanation, to argue that a certain patent does not apply to the claims. By combining that discussion, with the required detailed explanation, patent owner obscures the "detailed explanation." Such an obscured explanation results in the Office finding the "detailed explanation" was not provided, and therefore a determination that the request failed to comply with the filing date requirements, and a loss of the date of the original deposit of the request as the filing date.

The best way to correct this defect is to entirely delete the 3 CIP prosecution documents from the request. To the extent that the optional discussion is fully separated from the detailed explanation, the 3 CIP prosecution documents could be generally referenced in the optional discussion. However, the optional discussion does not allow for one to then provide the 3 CIP prosecution documents, as exhibits. Per rule 1.610(c): “The request may also include: (1) A cover sheet itemizing each component submitted as part of the request; (2) A table of contents for the request; (3) An explanation of how the claims patentably distinguish over the items of information; and (4) An explanation of why each item of information submitted with the request does or does not raise a substantial new question of patentability.”

B. The Brondrup reference has not been fairly applied to the dependent claims. Patent owner is reminded if the patent owner relies on a proper, detailed explanation of an independent claim as the detailed explanation for the dependent claims, then a review of the dependent claims may be limited to the detailed explanation of the independent claim provided by the patent owner.

C. The request does not follow best practices. MPEP 2811.01 I. describes: “The explanation should include citations to particular portions or figures in the item of information in which the teachings are located. Ideally, the required explanation can be provided using an appropriately detailed claim chart that compares, limitation by limitation, each claim for which supplemental examination is requested with the teachings of each item of information cited in the request.”

Note(s): “The patent owner must submit a complete, corrected request that will replace the originally-filed request. In other words, the patent owner must not submit a “supplemental” or corrected portion of the request ....” See MPEP §2812.03. However, if all applicable fees have already been paid, these fees do not have to be resubmitted with the corrected request.

Rule 1.620(e): Interviews are prohibited in a supplemental examination proceeding.

APPENDIX D

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 OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	14603434
Filing Date	23-Jan-2015
First Named Inventor	Chris Outwater
Attorney Docket Number	LBT0010-CON
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
Liberty PlugIns, 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)

8996876

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 47743 ○ 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:	14603434
Filing Date:	23-Jan-2015
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-CON

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	1814	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.: 14603434

Filing Date: 23-Jan-2015

Applicant/Patent under Reexamination: Outwater et al.

Electronic Terminal Disclaimer filed on December 14, 2015

☒ 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

APPENDIX E

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. 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 displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: URBAN INTEL, INC.

Application No./Patent No.: 9473205 Filed/Issue Date: June 21, 2016

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

URBAN INTEL, INC., a Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose one of options 1, 2, 3 or 4 below):

1. [✓] The assignee of the entire right, title, and interest.

2. [ ] An assignee of less than the entire right, title, and interest (check applicable box):

   [ ] The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   [ ] There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. [ ] The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. [ ] The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose one of options A or B below):

A. [ ] An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. [✓] A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Chris Outwater and William Gibbens Redmann To: Liberty Plugins, Inc.

   The document was recorded in the United States Patent and Trademark Office at Reel 034801, Frame 0482, or for which a copy thereof is attached.

2. From: Liberty Plusgins, Inc. To: Urban Intel, Inc.

   The document was recorded in the United States Patent and Trademark Office at Reel 055881, Frame 0376, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). 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 12 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.

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. 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 displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Chris Outwater — Signature

July 22, 2021 — Date

Chris Outwater — Printed or Typed Name

Director — Title or Registration Number

[Page 2 of 2]

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.

UNITED STATES
PATENT AND TRADEMARK OFFICE

Assignment abstract of title for Application 14603434

Invention title/Inventor	Patent	Publication	Application	PCT	International registration
Access Control System and Method for Use by an Access Device Chris Outwater, William Gibbens Redmann	9373205 Jun 21, 2016	20150134968 May 14, 2015	14603434 Jan 23, 2015		

Assignments (3 total)

Assignment 3

Reel/frame	Execution date	Date recorded	Properties	Pages
048942/0162	Apr 19, 2019	Apr 19, 2019	10	4

Conveyance
ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignors
LIBERTY PLUGINS, INC

Correspondent
CLIFFORD H KRAFT
320 ROBIN HILL DR.
NAPERVILLE, IL 60540

Assignee
URBAN INTEL, INC
6527 SEWARD PARK AVE S.
C/O EDWARD GOMEZ
SEATTLE, WASHINGTON 98118

Assignment 2

Reel/frame	Execution date	Date recorded	Properties	Pages
055881/0376	Apr 19, 2019	Mar 31, 2021	10	6

Conveyance
CORRECTIVE ASSIGNMENT TO CORRECT THE CONVEYING NAME AND RECEIVING NAME PREVIOUSLY RECORDED AT REEL: 48942 FRAME: 162. ASSIGNOR(S) HEREBY CONFIRMS THE ASSIGNMENT.

Assignors
LIBERTY PLUGINS, INC.

Correspondent
KELLY L. KASHA
14532 DUFIEF MILL RD
KASHA LAW LLC
NORTH POTOMAC, MD 20878

Assignee
URBAN INTEL, INC.
6527 SEWARD PARK AVE S.
C/O EDWARD GOMEZ
SEATTLE, WASHINGTON 98118

Assignment 1

Reel/frame	Execution date	Date recorded	Properties	Pages
034801/0482	Oct 29, 2014	Jan 23, 2015	1	10

Conveyance
ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignors
OUTWATER, CHRIS
REDMANN, WILLIAM GIBBENS

Correspondent
JOHN KASHA
14532 DUFIEF MILL ROAD
KASHA LAW LLC
NORTH POTOMAC, MD 20878

Assignee
LIBERTY PLUGINS, INC.
1482 EAST VALLEY ROAD, SUITE 329
SANTA BARBARA, CALIFORNIA 93108

Electronic Acknowledgement Receipt	
EFS ID:	43426970
Application Number:	96000367
International Application Number:	
Confirmation Number:	7090
Title of Invention:	Access Control System and Method for Use by an Access Device
First Named Inventor/Applicant Name:	9373205
Customer Number:	67050
Filer:	John Kasha
Filer Authorized By:	
Attorney Docket Number:	LBT0010-CON-SE
Receipt Date:	04-AUG-2021
Filing Date:	
Time Stamp:	16:07:48
Application Type:	Supplemental Examination
Patent Number:	

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	Misc Item of Information	LBT0010-CON-SE_supp_exam_req_08_04_2021_final.pdf	621647 d6b5bfe2b89a7fed948fc786b1cde88fc9da6dbd	no	43
Warnings:					
Information:					
2	Transmittal Letter	LBT0010-CON-SE_corr_trans_08_04_2021.pdf	91851 5b5b3b25b4f95d07d3cb22c665db864982a7cb03	no	2
Warnings:					
Information:					
3	Misc Item of Information	Appendix_A_US9373205B2.pdf	213037 bf93253ae24cb1726e6a88db970db395e3b97960	no	14
Warnings:					
Information:					
4	Misc Item of Information	Appendix_B_brondrup.pdf	337335 b209893fbb600b5d096084f87c403d5a8b8d1202	no	16
Warnings:					
Information:					
5	Transmittal of New Application	Appendix_C_supp_exam_req_sb0059_form.pdf	229241 d006b385ade3cc5833c39a022da640d64009ce04	no	6
Warnings:					
Information:					
6	Misc Item of Information	Appendix_D_Terminal_disclaimer.pdf	117806 733173c78c3474938ad4df1bb1bd70a3d045e483	no	6
Warnings:					
Information:					
7	Assignee showing of ownership per 37 CFR 3.73	Appendix_E_stmt_under_373_1.pdf	195550 b7d30ead865ca8035e72998420f969e2a7fa3c9a	no	6
Warnings:					
Information:					
			Total Files Size (in bytes):	1806467	

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Supplemental Examination of

U.S. Patent No.	9,373,205
Control No.	96/000,367
Confirm No.	7090
Inventors:	Chris Outwater et al.
Issued:	June 21, 2016
For:	ACCESS CONTROL SYSTEM AND METHOD FOR USE BY AN ACCESS DEVICE
Attorney Docket No.	LBT0010-CON-SE

CORRECTED REQUEST FOR SUPPLEMENTAL EXAMINATION OF U.S. PATENT NO. 9,373,205

MAIL STOP: SUPPLEMENTAL EXAMINATION
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Urban Intel, Inc. ("Requester") submits this Request for Supplemental Examination of U.S. Patent No. 9,373,205 (the "'205 Patent," copy enclosed as Appendix A). In accordance with 35 U.S.C. § 257 and 37 C.F.R. §§ 1.601, 1.605, 1.610, 1.615, 1.620, and 1.625, Requester, through its undersigned counsel, requests supplemental examination of Claims 1-24 of the '205 Patent, which issued on June 21, 2016, to Outwater *et al.* from application 14/603,434, filed June 23, 2015. The Requester is the owner of the entire right, title, and interest in the '205 Patent 37 C.F.R. § 1.610(b)(9)) (See Statement under 37 C.F.R. § 3.73(c) filed herewith as Appendix E).

I. INTRODUCTION

The '205 Patent issued on June 21, 2016, from Application Serial No. 14/603,434 filed June 23, 2015. The first maintenance fees have been paid on December 18, 2019. The '205 Patent is thus currently enforceable, and is, therefore, eligible for supplemental examination.

A continuation-in-part (CIP) application, Serial No. 15/900,374 ("the CIP Application") was filed on February 20, 2018, and later issued as Patent No. 10,826,885 on November 3, 2020. Brondrup, U.S. Publication No. 2003/0208386 ("Brondrup"; copy enclosed as Appendix B) was cited in the prosecution of the CIP Application. The Office might consider there to exist a substantial new question of patentability for one or more of Claims 1-24 of the '205 Patent in view of Brondrup. The individual requirements of 37 C.F.R. § 1.610 are addressed below.

II. § 1.610(A)

The required fee of $17,320 is was previously submitted, which includes the request filing fee of $4,620 and the reexamination fee of $12,700.

The Commissioner is hereby authorized to charge any deficiency or credit any overpayment to Deposit Account No. 504075.

III. § 1.610(B)(1)

Supplemental examination under 35 U.S.C. § 257 is requested for Claims 1-24 of the '205 Patent, entitled "ACCESS CONTROL SYSTEM AND METHOD FOR USE BY AN ACCESS DEVICE," which issued June 21, 2016, to Outwater et al., from application 14/603,434 filed June 23, 2015.

IV. § 1.610(B)(2)

Pursuant to 37 C.F.R. §§ 1.605(a) and 1.610(b)(2), below is a listing and discussion of the items of information to be considered in this supplemental examination. These same items are also cited in the Form PTO/SB/59 filed herewith as Appendix C:

(1) Brondrup (copy enclosed as Appendix B)

Item (1) is the Brondrup reference.

V. § 1.610(B)(3)

The Requester is not aware of any prior or concurrent post-Patent Office proceedings associated with the '205 Patent.

VI. § 1.610(B)(4)

Supplemental examination is requested for Claims 1-24 of the '205 Patent.

VII. § 1.610(B)(5)

As described in the Abstract, the '205 Patent is directed to systems and methods to allow a smart phone to open a processor-controlled door lock (access device) using a reservation certificate. When the smart phone presents a ***current*** reservation certificate to the access device, the processor of the access device activates or opens the door lock of the access device as depicted below in Fig. 5 of the '205 Patent.

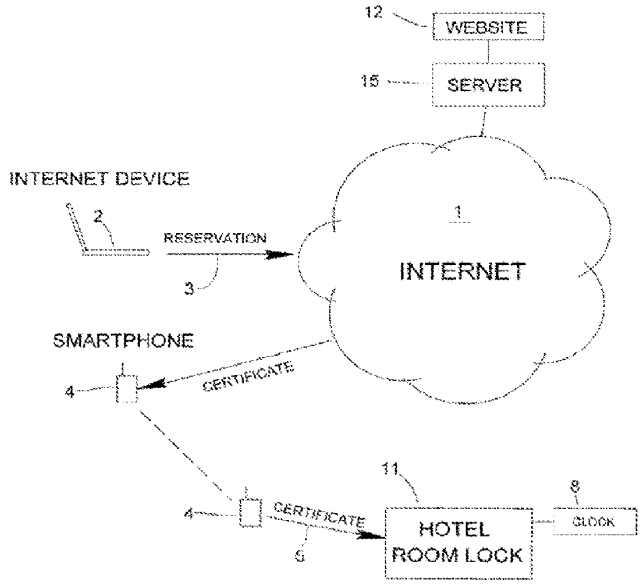
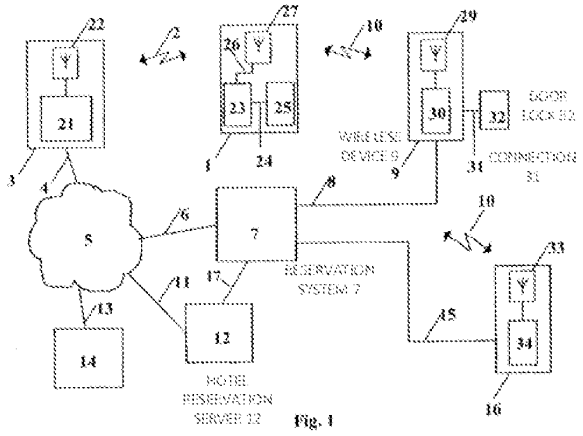
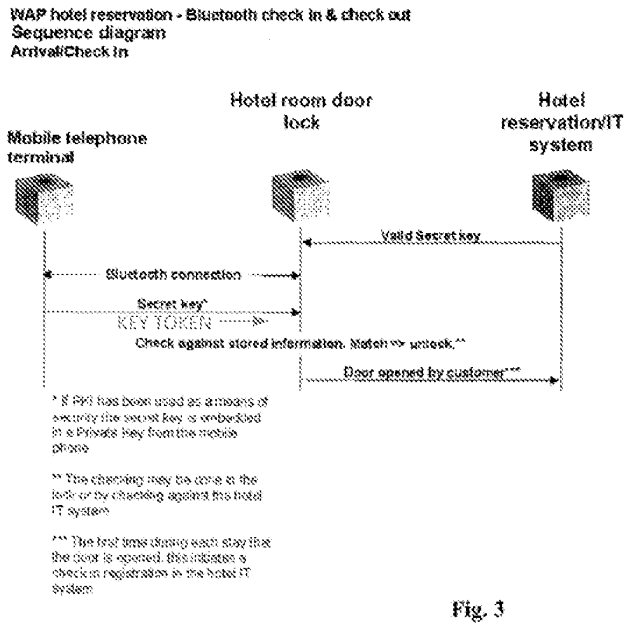
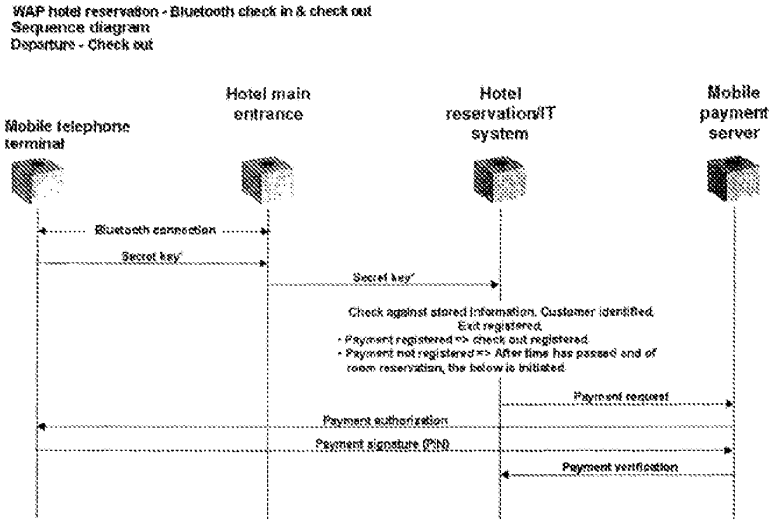


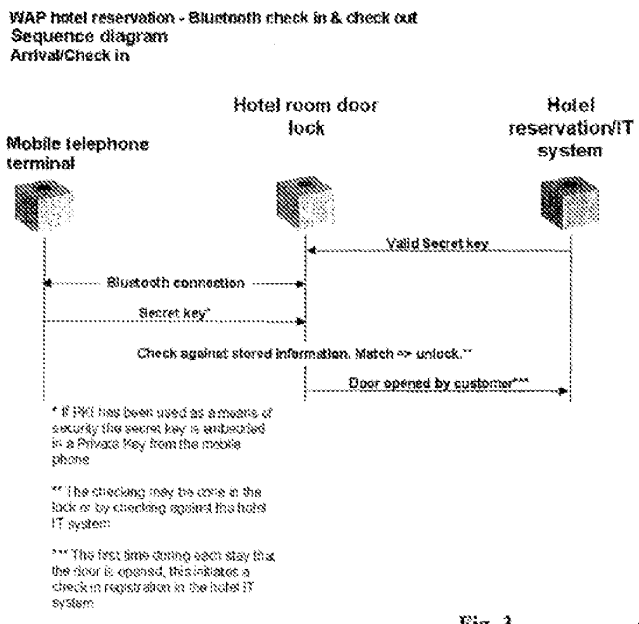
FIG. 5

Supplemental examination is requested for claims 1-24 of the '205 patent in view of the one item of information cited above (Brondrup). The claims are addressed individually in the following claim chart.

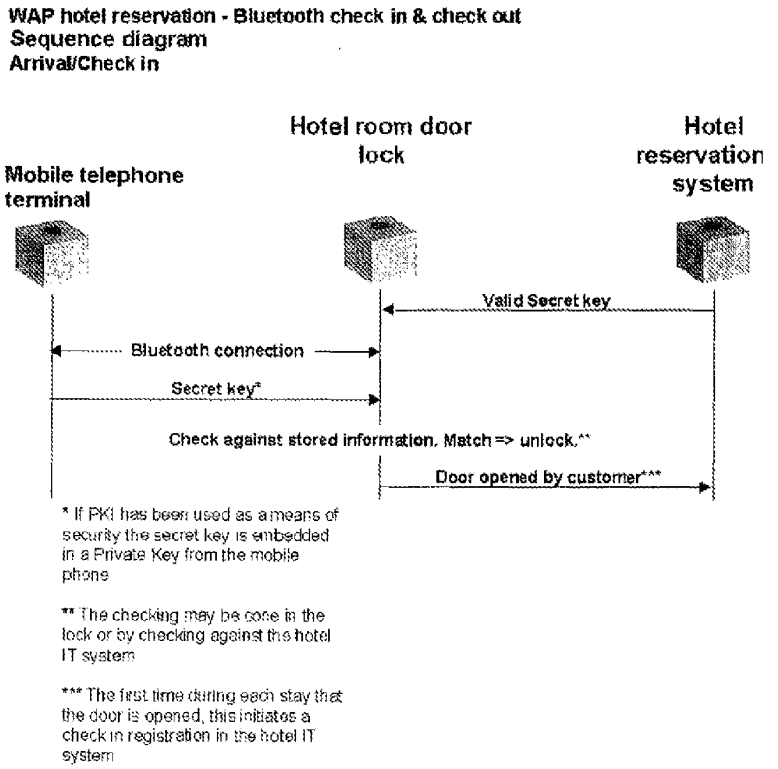
The '205 patent	**Brondrup**
Claim 1 - An access device for use in an access control system, the access device comprising:	Brondrup teaches wireless door lock (**9**,**32**) for use in room access control. (Title, Abstract, ¶ 0023, FIG. 1).
a processor **(16)** having control of a door lock **(11);** and	Brondrup teaches a hotel reservation/IT system **7** with connection to short range wireless devices **9**, wherein each device **9** uses connection **31** to connect to and operate door lock **32**. (¶ 0036, FIG. 1). System **7** has at least one connection to hotel reservation server **12**. (¶ 0036, FIG. 1).

	 (Annotated).
a communication module **(17)** connected to the processor, the processor able to receive a reservation certificate **(5)** presented by a portable terminal **(4)** through the communication module;	Brondrup teaches that "the key token is transmitted to nearby wireless devices associated with electrically operable door locks." (¶ 0043, FIG. 3).  (Annotated).
wherein the processor activates the door lock when a current reservation	Brondrup teaches that "[o]n receiving the appropriate key token from the wireless device in the mobile wireless terminal, the door lock wireless device of the reserved room … unlocks the door." (¶

certificate has been presented.	0043, FIG. 3).
Claim 2 - The access device of claim **1** wherein the processor activates the door lock for up to a predetermined duration.	Brondrup teaches an additional aspect of hotel check out in FIG. 5 that "is the triggering of automatic check-out or generation of a payment request from the hotel reservation/IT system to the payment server after exit registration or expiration of the reservation period." (¶ 0049, FIG. 5).  Fig. 5
Claim 3 - The access device of claim **2** wherein the predetermined duration is all day.	Brondrup teaches that "the invention can be set to terminate the function of the Bluetooth phone as a key for the hotel room door lock … after a certain time of the departure day." (¶ 0059).
Claim 4 - The access device of claim **1** wherein the reservation certificate comprise data representative of a duration and the processor activates the door lock for up to the duration.	Brondrup teaches that "the method can include steps of encryption, whereby the key token is encrypted to become an encrypted secret key." (¶ 0026). The "hotel reservation system contains a key token such as e.g. a reference number which can be directly used for obtaining access to the reserved room upon arrival at the hotel." (¶ 0041). "Optionally, as shown in FIG. 2, security can added to the above, e.g. through the use of PKI (Public Key Infrastructure)." (¶ 0042).
Claim 5 – The access device of claim **1** wherein the processor has access to the current time, the	Same Brondrup citations as for **Claims 2, 4**.

reservation certificate comprises data representative of an interval of the reservation, and the processor activates the door lock during the interval.	
Claim 6 – The access device of claim **5** wherein the interval is specified by a start time and one of an end time and a duration.	Same Brondrup citations as for **Claims 2, 3**.
Claim 7 – The access device of claim **1** further comprising: a memory to which the processor has access, the memory containing a public key for a server authorized to issue the reservation certificate;	Brondrup discloses in FIG. 3 that "[i]f PKI has been used as a means of security the secret key is embedded in a Private Key from the mobile phone." (FIG. 3).  Fig. 3 (Annotated).
wherein at least a portion of the reservation certificate is encrypted by the server using a private key and the processor verifies that the	Brondrup discloses in FIG. 3 that "[i]f PKI has been used as a means of security the secret key is embedded in a Private Key from the mobile phone." (FIG. 3).

reservation certificate is genuine by decrypting the portion with the public key.	
Claim 8 – The access device of claim **1** further comprising: a memory to which the processor has access, the memory containing a symmetric key;	Brondrup teaches that "the method can include steps of encryption, whereby the key token is encrypted to become an encrypted secret key." (¶ 0026).
wherein at least a portion of the reservation certificate is encrypted by a server using the symmetric key and the processor verifies that the reservation certificate is genuine by decrypting the portion with the symmetric key.	Brondrup teaches that "the method can include steps of encryption, whereby the key token is encrypted to become an encrypted secret key." (¶ 0026).
Claim 9 – The access device of claim **1** wherein the processor verifies that the reservation certificate is genuine.	In FIG. 3, Brondrup teaches that comparing a secret key from the mobile telephone terminal to a valid secret key from the reservation/IT system. (FIG. 3).

	 **Fig. 3**
Claim 10 – The access device of claim **1** further comprising: an identification to which the processor has access, the identification corresponding to one of the access device and the door lock, wherein the processor determines that the reservation certificate comprises data representative of the identification.	Brondrup teaches that the "hotel reservation system contains a key token such as e.g. a reference number which can be directly used for obtaining access to the reserved room upon arrival at the hotel." (¶ 0041).
Claim 11 – The access device of claim **1** further comprising: a memory to	Same Brondrup citations as for **Claim 7**.

which the processor has access, the memory containing a private key of the access device;	
wherein at least a portion of the reservation certificate is encrypted by a server using a corresponding public key for the access device and the processor decrypts the portion with the private key.	Same Brondrup citations as for **Claim 7**.
Claim 12 – The access device of claim **1** wherein the processor has access to a server through the communication module and the processor reports to the server that door lock was activated on the basis of the reservation certificate.	Brondrup teaches that "[o]n receiving the appropriate key token from the wireless device in the mobile wireless terminal, the door lock wireless device of the reserved room can notify the associated hotel reservation/IT system of the arrival of the user for check-in." (¶ 0043).
Claim 13 – A method for use by an access device in an access control system, the method comprising:	Brondrup teaches wireless door lock (**9**,**32**) for use in room access control. (Title, Abstract, ¶ 0023, FIG. 1).
a) accepting, by a processor through a communication module, a reservation certificate presented with a portable terminal;	Brondrup teaches that "the key token is transmitted to nearby wireless devices associated with electrically operable door locks." (¶ 0043, FIG. 3).
b) determining, by the processor, that the reservation certificate is current; and	Brondrup teaches that "[o]n receiving the appropriate key token from the wireless device in the mobile wireless terminal, the door lock wireless device of the reserved room … unlocks the door." (¶ 0043, FIG. 3).
c) activating, by the processor on the basis of the reservation certificate being current, a door lock.	Brondrup teaches that "[o]n receiving the appropriate key token from the wireless device in the mobile wireless terminal, the door lock wireless device of the reserved room … unlocks the door." (¶ 0043, FIG. 3).

Claim 14 – The method of claim **13** wherein the certificate is current for up to a predetermined duration.	Same Brondrup citations as for **Claim 2.**
Claim 15 – The method of claim **14** wherein the predetermined duration is all day.	Same Brondrup citations as for **Claim 3.**
Claim 16 – The method of claim **13** wherein the reservation certificate comprises data representative of a duration and the certificate is current for up to the duration.	Same Brondrup citations as for **Claim 4.**
Claim 17 – The method of claim **13** wherein the processor has access to the current time and the reservation certificate comprises data representative of an interval of the reservation, and the certificate is current for up to the interval.	Same Brondrup citations as for **Claim 5.**
Claim 18 – The method of claim **17** wherein the interval is specified by a start time and one of an end time and a duration.	Same Brondrup citations as for **Claim 6.**
Claim 19 – The method of claim **13** wherein at least a portion of the reservation certificate is encrypted by a server using a private key for which the corresponding public key is stored in a	Same Brondrup citations as for **Claim 7**.

memory accessible to the processor,	
wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the public key,	Same Brondrup citations as for **Claim 7.**
and the c) activating is on the further basis of the reservation certificate being genuine.	Same Brondrup citations as for **Claim 7.**
Claim 20 – The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a symmetric key stored in a memory accessible to the processor,	Same Brondrup citations as for **Claim 8.**
wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the symmetric key,	Same Brondrup citations as for **Claim 8.**
and the c) activating is on the further basis of the reservation certificate being genuine.	Same Brondrup citations as for **Claim 8.**
Claim 21 – The method of claim **13** wherein the b) determining by the processor is further that the reservation certificate is genuine,	Same Brondrup citations as for **Claim 9.**
and the c) activating is on the further basis of the reservation certificate	Same Brondrup citations as for **Claim 9.**

being genuine.	
Claim 22 – The method of claim **13** wherein the processor has access to an identification, the identification corresponding to one of the access device and the door lock,	Same Brondrup citations as for **Claim 10.**
wherein the b) determining by the processor is further that the reservation certificate comprises data representative of the identification,	Same Brondrup citations as for **Claim 10.**
and the c) activating is on the further basis of the reservation certificate comprising data representative of the identification.	Same Brondrup citations as for **Claim 10.**
Claim 23 – The method of claim **13** wherein at least a portion of the reservation certificate is encrypted by a server using a public key for which the corresponding private key is stored in a memory accessible to the processor,	Same Brondrup citations as for **Claim 11.**
the method further comprising the step of: d) decrypting the portion, by the processor, with the private key.	Same Brondrup citations as for **Claim 11.**
Claim 24 – The method of claim **13** wherein the processor has access to a server through the communication module,	Same Brondrup citations as for **Claim 12.**

the method further comprising the step of: d) reporting to the server that the door lock was activated on the basis of the reservation certificate.	Same Brondrup citations as for **Claim 12.**

VIII. § 1.610(B)(6)

As noted above, a copy of the '205 Patent is being submitted herewith as Appendix A. A terminal disclaimer was filed on December 14, 2015, disclaiming the terminal part of the statutory term of the '205 Patent which would extend beyond the expiration date of the full statuary term of prior patent number 8,996,876. The terminal disclaimer is submitted herewith as Appendix D.

IX. § 1.610(B)(7)

A copy of each cited item of information is being submitted herewith. All documents are in English; hence, no translations are required.

X. § 1.610(B)(8)

No item of information is over 50 pages in length.

XI. § 1.610(B)(9)

The Requester, Urban Intel, Inc., is the owner of the entire right, title, and interest in the '205 Patent, as evidenced by the Statement under 37 C.F.R. § 3.73(c) filed herewith as Appendix E.

XII. OPTIONAL EXPLANATION UNDER § 1.610(C)(3) & (4)

A. § 1.610(C)(3) – Claims 1-24 of the '205 Patent are patentably distinct from Brondrup

1. Claim 1 – Brondrup's ***appropriate*** key token is distinct from a ***current*** reservation certificate.

The last limitation of claim 1 recites that the processor of the access device activates the door lock when a current reservation certificate has been presented by a portable terminal (smart phone). In other words, when a smart phone presents a ***current*** reservation certificate to the access device, the processor of the access device activates or opens the door lock of the access device as depicted below in Fig. 5 of the '205 Patent.

As a result, the term "current reservation certificate" is key to interpreting the last limitation of claim 1.

According to MPEP § 2111.01 I, an examiner is entitled to give the words of the claim their plain meaning unless such meaning is inconsistent with the specification.

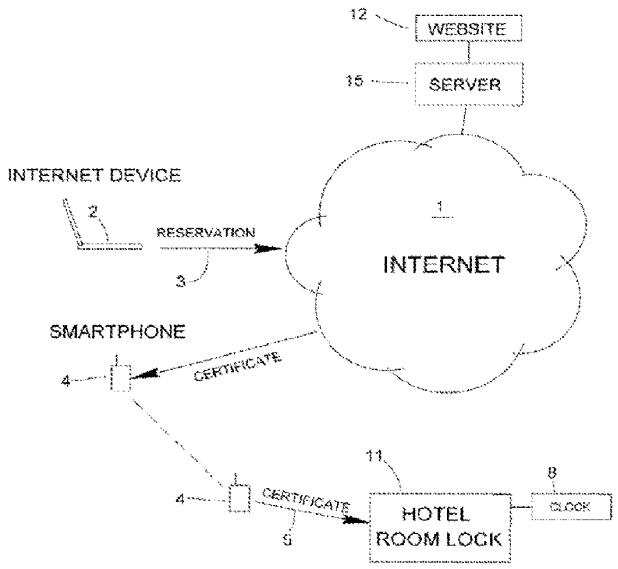


FIG. 5

The term "current" in "current reservation certificate" is an adjective modifying "reservation certificate." The plain meaning or definition of the adjective current is "occurring in or existing at the present time." See https://www.merriam-webster.com/dictionary/current as of 5/27/2021. Thus, the plain meaning of a "current reservation certificate" is a reservation certificate occurring in or existing at the present time.

Accordingly, the last limitation of claim 1 provides that the processor activates the door lock when the reservation certificate presented is occurring in or existing at the present time. In other words, the last limitation of claim 1 is determining when or if the reservation certificate presented is current or occurring in or existing at the present time. More simply, the last limitation of claim 1 describes performing a time comparison with the present time. Indeed,

independent claim 13, which is a method claim version of claim 1, explicitly describes that the processor determines if the reservation certificate is current and activates a door lock based on that determination.

Thus, the plain meaning of the last limitation of independent claim 1 is that the processor of the access device determines if the presented reservation certificate is current or occurring in or existing at the present time and activates a door lock based on that determination.

As described by MPEP § 2111.01 I, the plain meaning of a claim must also be consistent with the specification. FIG. 5 of the '205 Patent, depicted above, shows that hotel room lock **11** has access to clock **8**. Column 4, lines 53-61 of the '205 Patent, referencing both FIG. 3 and FIG. 5, provide that "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." (Emphasis added). Also, column 2, lines 53-55 of the '205 Patent describe that "***if the reservation time from the certificate approximately agrees with its internal time-of-day/date clock***, the device can allow charging." (Emphasis added). Note that these passages refer to an access device that is an electric vehicle charger. However, column 1, lines 64-67 of the '205 Patent provide that the present invention relates "to any access device such as a hotel room lock."

As a result, finding the plain meaning of the last limitation of independent claim 1 to be that ***the processor of the access device determines if the presented reservation certificate is current or occurring in or existing at the present time and activates a door lock based on that determination*** is entirely consistent with the specification.

Brondrup, in contrast, simply does ***not*** teach or suggest a processor of an access device that determines if the presented reservation certificate is current or occurring in or existing at the present time and activates a door lock based on that determination. Instead, at most, Brondrup teaches a door lock wireless device that simply compares two key tokens and activates a door lock if they match.

As described above, Brondrup, in the Abstract, discloses that, when a mobile terminal is in range of a wireless door lock, a hotel room key token is transferred to the wireless door lock from the mobile terminal to unlock a door. More specifically, after a reservation is made, the booking receipt received by a mobile terminal from a hotel reservation/IT system contains a key token such as e.g., a reference number that can be directly used for obtaining access to the reserved room. See Brondrup at ¶¶ 0040-0041. Also, after a reservation is made, a wireless door lock device of the reserved room receives a key token, or secret key, from the hotel reservation/IT system. See Brondrup at ¶ 0043.

Then, as shown in FIG. 3, reproduced below, the mobile telephone terminal (smartphone) of Brondrup transmits the key token, or secret key, to the wireless door lock device (hotel room door lock). The wireless door lock device determines if the secret key sent by the mobile terminal ***matches*** the key token sent previously by the hotel reservation/IT system to unlock the

door. In other words, ***the wireless door lock device of Brondrup simply compares two key tokens to unlock a door***.

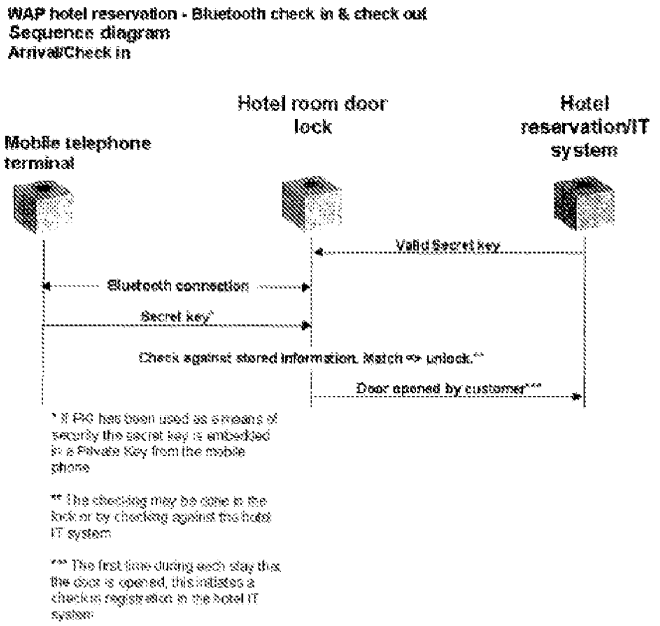


Fig. 3

Brondrup similarly describes a hotel room door lock that wirelessly senses a security code from a mobile terminal (smartphone). See Brondrup at ¶ 0062. The hotel room door lock then compares the security code to "a security code automatically programmed into the lock through the WAP hotel room reservation service, and opens the door." *Id.*

Therefore, the wireless door lock device of Brondrup does ***not*** determine if a key token is ***current*** or occurring in or existing at the present time in order to unlock a door. The wireless door lock device of Brondrup performs no time comparison with the present time. The wireless door lock device only ***compares*** two key tokens to unlock a door.

As described above in the claim chart, ¶ 0043 of Brondrup provides that "[o]n receiving the appropriate key token from the wireless device in the mobile wireless terminal, the door lock wireless device of the reserved room … unlocks the door." Thus, in Brondrup, an "appropriate" key token is a key token that matches the key token already placed on the wireless door lock device. Brondrup does not teach or suggest that an "appropriate" key token is a "current" key token or key token occurring in or existing at the present time.

Determining whether or not a key token is current on the wireless door lock device is not contemplated by Brondrup because it relies on the hotel reservation/IT system to determine the status of a reservation. The hotel reservation/IT system sends an appropriate key token to either the mobile terminal or the wireless door lock device based on this status.

For example, ¶ 0043 of Brondrup describes that at the end of a reservation "the hotel reservation/IT system can send a key token deactivation message to the door lock associated wireless device of the reserved room." If Brondrup's wireless door lock device (access device) determined whether or not a key token is current, the hotel reservation/IT system would not need to send a key token deactivation message to the wireless door lock device. The activation of the door lock would simply expire with the reservation certificate as it does in the '205 Patent. Therefore, the key token deactivation message of Brondrup clearly shows that determining whether or not a key token is current is simply ***not*** contemplated by Brondrup.

In summary, claim 1 of the '205 Patent is patentably distinct from Brondrup because it recites an access device that activates a door lock when a current reservation certificate is received. The plain meaning of the term ***current*** provides that the activation is conditional on

access device determining that the reservation certification is occurring in or existing at the present time. In contrast, Brondrup teaches a wireless door lock device that unlocks a door on receiving an appropriate key token. The specification of Brondrup provides that the term ***appropriate*** means that the unlocking is conditional on the wireless door lock determining that the key token received matches a key token already sent to the wireless door lock by the hotel reservation/IT system.

2. Claim 2 – Brondrup's *reservation period* is not a predetermined duration used for door lock activation.

Claim 2 of the '205 Patent recites that the processor of the access device activates the door lock for up to a predetermined duration.

As described above in the claim chart, Brondrup does disclose a reservation period. Specifically, Brondrup teaches "triggering of automatic check-out … from the hotel reservation/IT system to the payment server after exit registration or expiration of the reservation period." Brondrup at ¶ 0049, FIG. 5.

Brondrup, however, does not teach or suggest that the wireless door lock device does anything with the reservation period. The wireless door lock device of Brondrup is an access device of Brondrup. Brondrup only teaches using the reservation period in relation to the hotel reservation/IT system and the payment server during check-out. Indeed, FIG. 5 of Brondrup, shown below, does not even include the wireless door lock device in the check-out process.

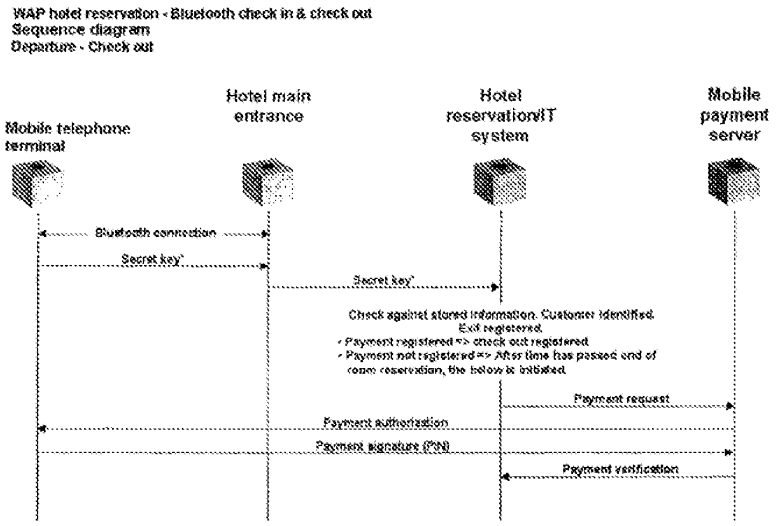


Fig. 5

Also, Brondrup only teaches using the reservation period in relation to check-out and not in relation to the activation of the door lock. Brondrup at ¶ 0049, FIG. 5.

In summary, claim 2 of the '205 Patent is patentably distinct from Brondrup because it recites an access device that activates the door lock for up to a predetermined duration. In contrast, Brondrup does not teach or suggest that its wireless door lock device does anything with the reservation period. Also, Brondrup does not teach or suggest that the reservation period is used in the activation of a door lock.

Claim 2 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 1, from which it depends, is patentably distinct from Brondrup.

3. Claim 3 – Brondrup's *a certain time of the departure day* is an end time and not a duration of activation.

Claim 3 of the '205 Patent recites that the predetermined duration of claim 2 is all day. In other words, it provides along with claim 2 that the duration of activation is all day.

As described above in the claim chart, Brondrup's only reference to a day is to a certain time of the departure day. Specifically, Brondrup teaches that "the invention can be set to terminate the function of the Bluetooth phone as a key for the hotel room door lock … after a certain time of the departure day." Brondrup at ¶ 0059. Thus, a certain time of the departure day is an end time.

As described above, an examiner is entitled to give the words of the claim their plain meaning unless such meaning is inconsistent with the specification.

The plain meaning of a duration is the length of time or period during which something exists, lasts, or is in progress. See https://www.merriam-webster.com/thesaurus/duration as of 8/02/2021. A duration cannot simply be determined by an end time.

In summary, claim 3 of the '205 Patent is patentably distinct from Brondrup because it recites a specific length of time for the duration of activation. In contrast, Brondrup's reference to a certain time of the departure day is simply an end time.

Claim 3 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 1, from which it depends, is patentably distinct from Brondrup.

4. Claim 4 – Brondrup's *reference number* is not a duration.

Claim 4 of the '205 Patent recites that the reservation certificate of claim 1 includes data that is a duration and the door lock is activated for the duration. In other words, the door lock is activated for the duration specified by the reservation certificate data.

As described above in the claim chart, Brondrup suggests that its key token can be a certificate by disclosing that the key token can be secured using public key infrastructure (PKI). Specifically, Brondrup teaches that "the method can include steps of encryption, whereby the key token is encrypted to become an encrypted secret key." Brondrup at ¶ 0026. The "hotel reservation system contains a key token such as e.g. a reference number which can be directly used for obtaining access to the reserved room upon arrival at the hotel." Brondrup at ¶ 0041. "Optionally, as shown in FIG. 2, security can [be] added to the above, e.g. through the use of PKI (Public Key Infrastructure)." Brondrup at ¶ 0042.

Although Brondrup suggests that the key token can be a PKI certificate, it does not teach or suggest the key token can include a duration. Brondrup's only disclosure regarding a key token is that it can be a reference number, which can be directly used for obtaining access to the reserved room upon arrival at the hotel. Note that Brondrup is describing that the key token is a reference number and not that its data includes a reference number. In any event, however, a reference number is ***not*** a duration. As described above, a duration is the length of time or period during which something exists, lasts, or is in progress, for example.

In summary, claim 4 of the '205 Patent is patentably distinct from Brondrup because it recites that the reservation certificate includes a duration used in the activation of the door lock.

In contrast, Brondrup only discloses that a key token can be a reference number and a reference number is not a duration.

Claim 4 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 1, from which it depends, is patentably distinct from Brondrup.

5. Claim 5 – Brondrup's *reservation period* is not disclosed in relation to its wireless door lock or to activation of a door lock and Brondrup's *reference number* is not an interval of the reservation.

Claim 5 of the '205 Patent recites that processor of the access device has access to the current time, the reservation certificate of claim 1 includes data that is an interval of the reservation, and the door lock is activated for the duration. In other words, the access device can get the current time, receives an interval from the reservation certificate, and activates the door lock for interval using the current time.

As described above in the claim chart, Brondrup's disclosures related to claims 2 and 4 apply here as well. As described with regard to claim 2, Brondrup discloses a reservation period. However, Brondrup does not teach or suggest that the reservation period is used by the wireless door lock device to activate the door lock. Also, Brondrup only teaches using the reservation period in relation to check-out and not in relation to activation of the door lock. Brondrup at ¶ 0049, FIG. 5.

As described with regard to claim 4, although Brondrup suggests that the key token can be a PKI certificate, it does not teach or suggest the key token includes an interval of the reservation. Brondrup's only disclosure regarding a key token is that it can be a reference

number, which can be directly used for obtaining access to the reserved room upon arrival at the hotel. A reference number is ***not*** an interval of the reservation.

Brondrup also does not teach or suggest that its wireless device has access to the current time.

In summary, claim 5 of the '205 Patent is patentably distinct from Brondrup because it recites that the access device can access the current time and that the reservation certificate includes an interval of the reservation used by the access device in the activation of the door lock. In contrast, Brondrup does not teach or suggest that its wireless door lock device has access to current. It does not teach or suggest that its wireless door lock device does anything with the reservation period. It does not teach or suggest that the reservation period is used in the activation of a door lock. Finally, Brondrup only discloses that a key token can be a reference number and a reference number is not an interval of the reservation.

In addition, as described below, the Office has previously considered Brondrup in regard to an interval of the reservation in the CIP Application. The claims of the CIP Application recite a reservation certificate describing an interval of a reservation like claim 5 of the '205 Patent. The Office initially rejected these claims, asserting that Brondrup discloses a reservation certificate describing an interval of a reservation. The Office initially rejected these claims, asserting that Brondrup discloses a reservation certificate describing an interval of a reservation. The Applicant of the CIP Application argued that Brondrup fails to teach a reservation certificate describing an interval of a reservation. The Office accepted the argument and found that the claims were allowable over Brondrup.

Claim 5 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 1, from which it depends, is patentably distinct from Brondrup.

6. Claim 6 – Brondrup does not teach or suggest a start time in relation to its reservation period or even a start time at all.

Claim 6 of the '205 Patent recites that the interval of the reservation of claim 5 is specified by a start time and one of an end time and a duration. In other words, the interval can be (1) a start time and an end time or (2) a start time and a duration. In both cases, an interval includes a start time.

As described above in the claim chart, Brondrup's disclosures related to claims 2 and 3 apply here as well. As described with regard to claim 2, Brondrup discloses a reservation period. As described with regard to claim 3, Brondrup discloses a certain time of the departure day that is an end time. However, Brondrup does not teach or suggest a start time in relation to the reservation period. In fact, Brondrup is silent with regard to a start time.

In summary, claim 6 of the '205 Patent is patentably distinct from Brondrup because it recites an interval of the reservation that must include a start time. In contrast, Brondrup does not teach or suggest a start time in relation to the period of the reservation or a start time at all.

In addition, as described below, the Office has previously considered Brondrup in regard to an interval of the reservation in the CIP Application. The claims of the CIP Application recite a reservation certificate describing an interval of a reservation like claim 6 of the '205 Patent. The Office initially rejected these claims, asserting that Brondrup discloses a reservation certificate describing an interval of a reservation. The Office initially rejected these claims, asserting that Brondrup discloses a reservation certificate describing an interval of a reservation.

The Applicant of the CIP Application argued that Brondrup fails to teach a reservation certificate describing an interval of a reservation. The Office accepted the argument and found that the claims were allowable over Brondrup.

Claim 6 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 1, from which it depends, is patentably distinct from Brondrup.

7. Claim 7 – Brondrup's *mobile phone* is not the server issuing the key token.

Claim 7 of the '205 Patent recites that the access device stores a public key for the server issuing the reservation certificate of claim 1, at least a portion of the reservation certificate is encrypted with the private key of the server, and the access device decrypts the portion using the public key. In other words, the access device decrypts a portion of the reservation certificate using a public key of a server that issued the certificate. More simply a portion of the reservation certificate is encrypted and decrypted with the private and public keys, respectively, of the server issuing the certificate.

As described above in the claim chart, Brondrup discloses in FIG. 3 that "[i]f PKI has been used as a means of security the secret key is embedded in a Private Key from the mobile phone." FIG. 3, shown below, also provides that the hotel room door lock checks the secret key against the valid secret key stored on the hotel room door lock.

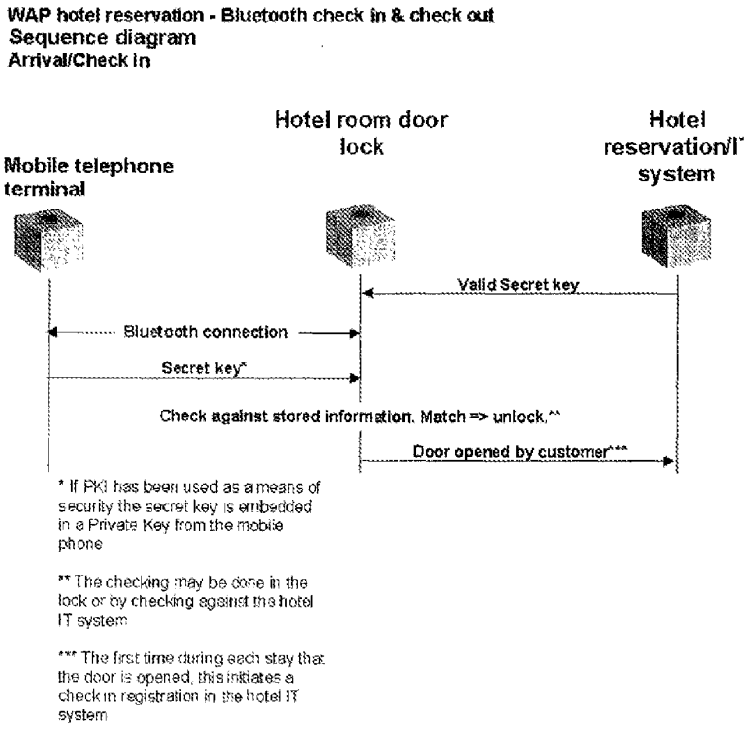


Fig. 3

Thus, FIG. 3 is suggesting that, when PKI is used, the secret key is embedded in a private key from the mobile phone and is sent to the hotel room door lock. In order to compare the secret key to the valid secret key stored on the hotel room door lock, the hotel room door lock has to decrypt the secret key embedded in the private key of the mobile phone. According to PKI, this is done with a public key of the mobile phone.

Consequently, Brondrup suggests storing a public key for the mobile phone on the wireless door lock device, encrypting the key token (secret key) sent to the wireless door lock device with a private key of the mobile phone, and decrypting the key token with the stored public key for the mobile phone using the wireless door lock device. More simply, Brondrup

suggests encrypting and decrypting key tokens with the private and public keys, respectively, of the mobile phone.

In contrast to claim 7, therefore, Brondrup does not use the private and public keys of the server issuing the key token. Instead, Brondrup discloses using the private and public keys of the intermediate mobile phone. Brondrup in ¶ 0026, for example, discloses that a wireless mobile terminal (mobile phone) receives from a hotel reservation booking server "a reservation/booking request confirmation including a key token." Thus, the hotel reservation booking server is the issuing server of the key token in Brondrup and not the mobile phone.

In summary, claim 7 of the '205 Patent is patentably distinct from Brondrup because it recites encrypting and decrypting a portion of the reservation certificate with the private and public keys, respectively, of the server issuing the certificate. In contrast, Brondrup discloses encrypting and decrypting the key token with the private and public keys, respectively, of the mobile phone, which is not the server issuing the key token.

Claim 7 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 1, from which it depends, is patentably distinct from Brondrup.

8. Claim 8 – Brondrup's *PKI encryption* does not use a symmetric key.

Claim 8 of the '205 Patent recites that the access device stores a symmetric key, at least a portion of the reservation certificate is encrypted by a server using the symmetric key, and the access device decrypts the portion using the symmetric key. In other words, the access device decrypts a portion of the reservation certificate using a symmetric key. More simply a portion of the reservation certificate is encrypted and decrypted with a symmetric key.

As described above in the claim chart, Brondrup discloses that "the method can include steps of encryption, whereby the key token is encrypted to become an encrypted secret key." Brondrup at ¶ 0026. As described above in regard to claim 7, Brondrup suggests encrypting and decrypting key tokens with the private and public keys, respectively, of the mobile phone. However, Brondrup does not teach or suggest encrypting and decrypting a key token with a symmetric key.

In FIG. 2, Brondrup mentions that in addition to PKI, security can be added "by use of the subscribers IMSI number (SIM identity) (request to subscriber's mobile phone)." The subscriber's IMSI number is not a symmetric key and Brondrup does not suggest that it is used for encryption.

In summary, claim 8 of the '205 Patent is patentably distinct from Brondrup because it recites encrypting and decrypting a portion of the reservation certificate with a symmetric key. In contrast, Brondrup only discloses encrypting and decrypting the key token with the private and public keys, respectively.

Claim 8 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 1, from which it depends, is patentably distinct from Brondrup.

9. Claim 9 – Brondrup's wireless door lock device does not verify if a *key token certificate* is genuine or includes a digital authorization of a trusted party and Brondrup's *reference number* is not a digital authorization of a trusted party.

Claim 9 of the '205 Patent recites that the processor of the access device verifies that the reservation certificate is genuine.

As described above, an examiner is entitled to give the words of the claim their plain meaning unless such meaning is inconsistent with the specification.

The term "genuine" in claim 9 is an adjective modifying "reservation certificate." The plain meaning or definition of the adjective genuine is "actually having the reputed or apparent qualities or character." See https://www.merriam-webster.com/dictionary/current as of 8/01/2021. Thus, the plain meaning of a "genuine reservation certificate" is a reservation certificate actually having the reputed or apparent qualities or character of a reservation certificate.

One of ordinary skill in the art understands that this plain meaning of genuine in the context of digital certificates is too broad. Digital certificates are known to be authentic or genuine if they are digitally signed by a trusted party. Indeed, the '205 Patent explicitly defines the term genuine in this context. The '205 Patent provides that 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." See the '205 Patent at column 2, lines 19-21.

As a result, the term "genuine" should be construed in the context of digital certificates as including a digital authorization of a trusted party.

As described with regard to claim 4, although Brondrup suggests that the key token can be a PKI certificate, it does not teach or suggest the key token includes a digital authorization of a trusted party. Brondrup's only disclosure regarding a key token is that it can be a reference number, which can be directly used for obtaining access to the reserved room upon arrival at the hotel. A reference number is ***not*** a digital authorization of a trusted party. Further, Brondrup does not teach or suggest that the wireless door lock verifies that the key token is genuine or includes a digital authorization of a trusted party.

In summary, claim 9 of the '205 Patent is patentably distinct from Brondrup because it recites that the access device verifies that the reservation certificate includes a digital authorization of a trusted party. In contrast, Brondrup does not teach or suggest that its wireless door lock verifies that the key token is genuine or includes a digital authorization of a trusted party. Also, Brondrup only discloses that a key token can be a reference number and a reference number is not a digital authorization of a trusted party.

Claim 9 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 1, from which it depends, is patentably distinct from Brondrup.

10. Claim 10 – Brondrup's *reference number* is an identifier of the booking or reservation and does not correspond to the wireless door lock device or the door lock.

Claim 10 of the '205 Patent recites that the access device has an identification (ID) corresponding to the access device or the door lock and determines if the reservation certificate

includes the ID. In other words, the access device determines if the reservation certificate includes the device ID of the access device or door lock. Indeed, the '205 Patent provides that "FIG. **2** shows a sample certificate **14** (one embodiment of certificate **5)** containing several fields of data representative of the reservation: 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"). See the '205 Patent at column 5, lines 7-13.

As described above in the claim chart, Brondrup teaches that the "hotel reservation system contains a key token such as e.g. a reference number which can be directly used for obtaining access to the reserved room upon arrival at the hotel." Brondrup at ¶ 0041. The reference number of Brondrup, however, is not a device ID of the wireless door lock device or the door lock. Instead, the reference number is a booking token "that both serves as a receipt for accepted payment and as a key parameter in the communication protocol for door lock opening." See Brondrup at ¶ 0022. In other words, the reference number of Brondrup is an identifier of the booking or reservation. It is ***not*** an identifier of the wireless door lock device or the door lock.

In summary, claim 10 of the '205 Patent is patentably distinct from Brondrup because it recites an ID corresponding to the access device or the door lock and determines if the reservation certificate includes the ID. In contrast, Brondrup discloses a reference number that is an identifier of the booking or reservation and does not correspond to the wireless door lock device or the door lock.

Claim 10 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 1, from which it depends, is patentably distinct from Brondrup.

11. Claim 11 – Brondrup's *mobile phone* is not the access device.

Claim 11 of the '205 Patent recites that the access device stores a private key for the access device, at least a portion of the reservation certificate is encrypted by a server with the public key of the access device, and the access device decrypts the portion using the private key. In other words, the access device decrypts a portion of the reservation certificate using its own private key. More simply, a portion of the reservation certificate is encrypted and decrypted with the public and private keys, respectively, of the access device.

As described above in regard to claim 7, Brondrup suggests storing a public key for the mobile phone on the wireless door lock device, encrypting the key token (secret key) sent to the wireless door lock device with a private key of the mobile phone, and decrypting the key token with the stored public key for the mobile phone using the wireless door lock device. More simply, Brondrup suggests encrypting and decrypting key tokens with the private and public keys, respectively, of the mobile phone.

In contrast to claim 11, therefore, Brondrup does not use the public and private keys of the access device. Instead, Brondrup discloses using the private and public keys of the intermediate mobile phone.

In summary, claim 11 of the '205 Patent is patentably distinct from Brondrup because it recites encrypting and decrypting a portion of the reservation certificate with the public and private keys, respectively, of the access device. In contrast, Brondrup discloses encrypting and

decrypting the key token with the private and public keys, respectively, of the mobile phone, which is ***not*** the wireless door lock device (access device).

Claim 11 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 1, from which it depends, is patentably distinct from Brondrup.

12. Claim 12 – Is patentably distinct from Brondrup for the same reasons as independent claim 1.

Claim 12 of the '205 Patent is patentably distinct from Brondrup for the same reasons independent claim 1, from which it depends, is patentably distinct from Brondrup.

13. Claim 13 – Brondrup's *appropriate* key token is distinct from a reservation certificate being current.

As described above, claim 13 is a method claim version of claim 1, which is a system claim. Claim 13, however, is even more explicit in describing that the processor determines if the reservation certificate is "current" and activates a door lock based on that determination.

As a result, claim 13 of the '205 Patent is patentably distinct from Brondrup for the same reasons independent claim 1 is patentably distinct from Brondrup.

14. Claim 14 – Brondrup's *reservation period* is not a predetermined duration used for door lock activation.

Claim 14 of the '205 Patent is a method claim version of dependent claim 2.

As a result, claim 14 of the '205 Patent is patentably distinct from Brondrup for the same reasons dependent claim 2 is patentably distinct from Brondrup.

Claim 14 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 13, from which it depends, is patentably distinct from Brondrup.

15. Claim 15 – Brondrup's *a certain time of the departure day* is an end time and not a duration of activation.

Claim 15 of the '205 Patent is a method claim version of dependent claim 3.

As a result, claim 15 of the '205 Patent is patentably distinct from Brondrup for the same reasons dependent claim 3 is patentably distinct from Brondrup.

Claim 15 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 13, from which it depends, is patentably distinct from Brondrup.

16. Claim 16 – Brondrup's *reference number* is not a duration.

Claim 16 of the '205 Patent is a method claim version of dependent claim 4.

As a result, claim 16 of the '205 Patent is patentably distinct from Brondrup for the same reasons dependent claim 4 is patentably distinct from Brondrup.

Claim 16 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 13, from which it depends, is patentably distinct from Brondrup.

17. Claim 17 – Brondrup's *reservation period* is not disclosed in relation to its wireless door lock or to activation of a door lock and Brondrup's *reference number* is not an interval of the reservation.

Claim 17 of the '205 Patent is a method claim version of dependent claim 5.

As a result, claim 17 of the '205 Patent is patentably distinct from Brondrup for the same reasons dependent claim 5 is patentably distinct from Brondrup.

In addition, as described below, the Office has previously considered Brondrup in regard to an interval of the reservation in the CIP Application. The claims of the CIP Application recite a reservation certificate describing an interval of a reservation like claim 17 of the '205 Patent.

The Office initially rejected these claims, asserting that Brondrup discloses a reservation certificate describing an interval of a reservation. The Office initially rejected these claims, asserting that Brondrup discloses a reservation certificate describing an interval of a reservation. The Applicant of the CIP Application argued that Brondrup fails to teach a reservation certificate describing an interval of a reservation. The Office accepted the argument and found that the claims were allowable over Brondrup.

Claim 17 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 13, from which it depends, is patentably distinct from Brondrup.

18. Claim 18 – Brondrup does not teach or suggest a start time in relation to its reservation period or even a start time at all.

Claim 18 of the '205 Patent is a method claim version of dependent claim 6.

As a result, claim 18 of the '205 Patent is patentably distinct from Brondrup for the same reasons dependent claim 6 is patentably distinct from Brondrup.

In addition, as described below, the Office has previously considered Brondrup in regard to an interval of the reservation in the CIP Application. The claims of the CIP Application recite a reservation certificate describing an interval of a reservation like claim 18 of the '205 Patent. The Office initially rejected these claims, asserting that Brondrup discloses a reservation certificate describing an interval of a reservation. The Office initially rejected these claims, asserting that Brondrup discloses a reservation certificate describing an interval of a reservation. The Applicant of the CIP Application argued that Brondrup fails to teach a reservation certificate describing an interval of a reservation. The Office accepted the argument and found that the claims were allowable over Brondrup.

Claim 18 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 13, from which it depends, is patentably distinct from Brondrup.

19. Claim 19 – Brondrup's *mobile phone* is not the server issuing the key token.

Claim 19 of the '205 Patent is a method claim version of dependent claim 7.

As a result, claim 19 of the '205 Patent is patentably distinct from Brondrup for the same reasons dependent claim 7 is patentably distinct from Brondrup.

Claim 19 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 13, from which it depends, is patentably distinct from Brondrup.

20. Claim 20 – Brondrup's *PKI encryption* does not use a symmetric key.

Claim 20 of the '205 Patent is a method claim version of dependent claim 8.

As a result, claim 20 of the '205 Patent is patentably distinct from Brondrup for the same reasons dependent claim 8 is patentably distinct from Brondrup.

Claim 20 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 13, from which it depends, is patentably distinct from Brondrup.

21. Claim 21 – Brondrup's wireless door lock device does not verify if a *key token certificate* is genuine or includes a digital authorization of a trusted party and Brondrup's *reference number* is not a digital authorization of a trusted party.

Claim 21 of the '205 Patent is a method claim version of dependent claim 9.

As a result, claim 21 of the '205 Patent is patentably distinct from Brondrup for the same reasons dependent claim 9 is patentably distinct from Brondrup.

Claim 21 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 13, from which it depends, is patentably distinct from Brondrup.

22. Claim 22 – Brondrup's *reference number* is an identifier of the booking or reservation and does not correspond to the wireless door lock device or the door lock.

Claim 22 of the '205 Patent is a method claim version of dependent claim 10.

As a result, claim 22 of the '205 Patent is patentably distinct from Brondrup for the same reasons dependent claim 10 is patentably distinct from Brondrup.

Claim 22 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 13, from which it depends, is patentably distinct from Brondrup.

23. Claim 23 – Brondrup's *mobile phone* is not the access device.

Claim 23 of the '205 Patent is a method claim version of dependent claim 11.

As a result, claim 23 of the '205 Patent is patentably distinct from Brondrup for the same reasons dependent claim 11 is patentably distinct from Brondrup.

Claim 23 of the '205 Patent is also patentably distinct from Brondrup for the same reasons independent claim 13, from which it depends, is patentably distinct from Brondrup.

24. Claim 24 – Is patentably distinct from Brondrup for the same reasons as independent claim 13.

Claim 24 of the '205 Patent is patentably distinct from Brondrup for the same reasons independent claim 13, from which it depends, is patentably distinct from Brondrup.

B. § 1.610(C)(4) – No SNQ of patentability because Brondrup's wireless door lock does not determine if a key token is "current"

Brondrup does not raise a substantial new question (SNQ) of patentability because claims 1-24 of the '205 Patent are patentably distinct from Brondrup as described above.

Primarily, in regard to claims 1-24, Brondrup does not raise an SNQ of patentability because the wireless door lock device of Brondrup does ***not*** determine if a key token is ***current*** in order to unlock a door. As described above, determining whether or not a key token is current on the wireless door lock device is not contemplated by Brondrup because it relies on the hotel reservation/IT system to determine the status of a reservation. For example, ¶ 0043 of Brondrup describes that at the end of a reservation "the hotel reservation/IT system can send a key token deactivation message to the door lock associated wireless device of the reserved room." If Brondrup's wireless door lock device (access device) determined whether or not a key token is current, the hotel reservation/IT system would not need to send a key token deactivation message to the wireless door lock device. The activation of the door lock would simply expire with the reservation certificate as it does in the '205 Patent. Therefore, the key token deactivation message of Brondrup clearly shows that determining whether or not a key token is current is simply ***not*** contemplated by Brondrup.

In addition, in regard to dependent claims 2-11 and 14-23, Brondrup does not raise an SNQ of patentability because Brondrup does not teach or suggest the additional features of each of these dependent claims.

Also, the Office has previously considered Brondrup in the CIP Application. The claims of the CIP Application additionally recite a reservation certificate describing an interval of a reservation like claims 5-6 and 17-18 of the '205 Patent. The Office initially rejected these claims, asserting that Brondrup discloses a reservation certificate describing an interval of a reservation. The Applicant of the CIP Application argued that Brondrup fails to teach a reservation certificate describing an interval of a reservation. The Office accepted the argument and found that the claims were allowable over Brondrup.

XIII. CONCLUSION

For the reasons discussed above, the Requester respectfully requests that supplemental examination of Claims 1-24 of the '205 Patent be performed with respect to the one item of information (Brondrup) submitted herewith and that a supplemental examination certificate be issued.

Respectfully submitted,

By: /John R. Kasha/
John R. Kasha
Registration No. 53,100
KASHA LAW LLC
14532 Dufief Mill Rd.
North Potomac, MD 20878
Customer No. 67050
Tel. 703-867-1886
Date: August 4, 2021

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Supplemental Examination of

U.S. Patent No.	9,373,205
Control No.	96/000,367
Confirm No.	7090
Inventors:	Chris Outwater et al.
Issued:	June 21, 2016
For:	ACCESS CONTROL SYSTEM AND METHOD FOR USE BY AN ACCESS DEVICE
Attorney Docket No.	LBT0010-CON-SE

TRANSMITTAL OF CORRECTED REQUEST FOR SUPPLEMENTAL EXAMINATION OF U.S. PATENT NO. 9,373,205

In response to Notice of Noncompliant Supplemental Examination Request (hereinafter the "Notice") mailed July 28, 2021:

A. As suggested in the Notice, the 3 CIP prosecution documents have been deleted from the corrected request and the optional discussion has been made only under a separate subheading (XII) entitled "Optional Explanation under § 1.610(c)(3) & (4)" as recommended in MPEP 2811.01 I;

B. As suggested in the Notice, the Brondrup reference has been fairly applied to the dependent claims in the detailed explanation; and

C. As suggested in the Notice, to follow best practices under MPEP 2811.01, the detailed explanation now includes citations to particular portions or figures in the Brondrup reference using an appropriately detailed claim chart.

Also, as directed, submitted herewith is a complete, corrected request that will replace the originally-filed request that now includes exhibits A-E, also submitted herewith.

Respectfully submitted,

By: /John R. Kasha/
John R. Kasha
Registration No. 53,100
KASHA LAW LLC
14532 Dufief Mill Rd.
North Potomac, MD 20878
Customer No. 67050
Tel. 703-867-1886
Date: August 4, 2021

APPENDIX A

US009373205B2

(12) **United States Patent**
Outwater et al.

(10) **Patent No.: US 9,373,205 B2**
(45) **Date of Patent: *Jun. 21, 2016**

(54) **ACCESS CONTROL SYSTEM AND METHOD FOR USE BY AN ACCESS DEVICE**

(71) Applicant: **Liberty PlugIns, Inc.**, Santa Barbara, CA (US)

(72) Inventors: **Chris Outwater**, Carpinteria, CA (US); **William Gibbens Redmann**, Glendale, CA (US)

(73) Assignee: **Liberty PlugIns, Inc.**, Santa Barbara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/603,434**

(22) Filed: **Jan. 23, 2015**

(65) **Prior Publication Data**

US 2015/0134968 A1 May 14, 2015

Related U.S. Application Data

(63) Continuation of application No. 13/582,467, filed as application No. PCT/US2011/026781 on Mar. 2, 2011, now Pat. No. 8,996,876.

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

(51) **Int. Cl.**

H04L 9/32	(2006.01)
G07C 9/00	(2006.01)
G06Q 20/04	(2012.01)
G06Q 20/32	(2012.01)
G06Q 20/38	(2012.01)
G06Q 30/06	(2012.01)
G07F 5/26	(2006.01)
G07F 15/00	(2006.01)
H04L 29/06	(2006.01)
B60L 11/18	(2006.01)

(52) **U.S. Cl.**

CPC ***G07C 9/00007*** (2013.01); ***B60L 11/1846*** (2013.01); ***B60L 11/1848*** (2013.01); ***G06Q 20/045*** (2013.01); ***G06Q 20/32*** (2013.01); ***G06Q 20/3223*** (2013.01); ***G06Q 20/38215*** (2013.01); ***G06Q 30/06*** (2013.01); ***G07F 5/26*** (2013.01); ***G07F 15/005*** (2013.01); ***H04L 9/3247*** (2013.01); ***H04L 9/3263*** (2013.01); ***H04L 63/0428*** (2013.01); *B60L 2230/40* (2013.01); *H04L 2209/56* (2013.01); *H04L 2209/80* (2013.01); *H04L 2209/84* (2013.01); *Y02T 10/7005* (2013.01); *Y02T 10/7088* (2013.01); *Y02T 90/12* (2013.01); *Y02T 90/121* (2013.01); *Y02T 90/128* (2013.01); *Y02T 90/14* (2013.01); *Y02T 90/16* (2013.01); *Y02T 90/163* (2013.01); *Y02T 90/169* (2013.01); *Y04S 30/14* (2013.01)

(58) **Field of Classification Search**

None

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2003/0154169	A1*	8/2003	Yanai	G06Q 10/02 705/65
2006/0179299	A1*	8/2006	Tanimoto	G06Q 10/107 713/158

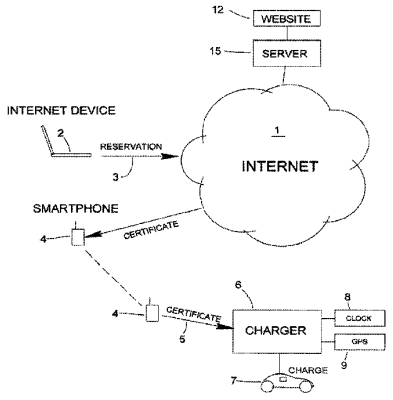
Primary Examiner — Brandon Hoffman

(74) *Attorney, Agent, or Firm* — John R. Kasha; Kelly L. Kasha; Kasha Law LLC

(57) **ABSTRACT**

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.

24 Claims, 7 Drawing Sheets



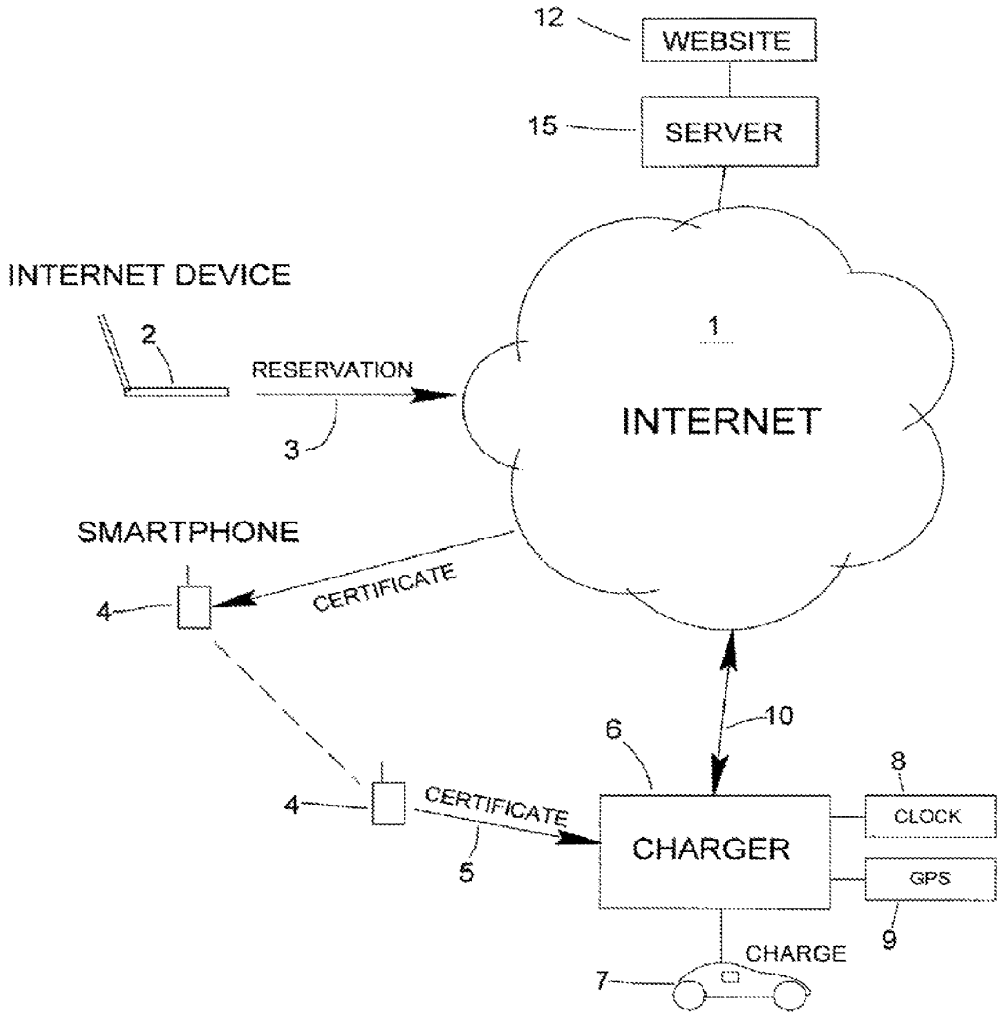

12
WEBSITE
15
SERVER
INTERNET DEVICE
2
RESERVATION
3
1
INTERNET
SMARTPHONE
4
CERTIFICATE
10
6
8
4
CERTIFICATE
5
CHARGER
CLOCK
GPS
9
CHARGE
7

FIG. 1

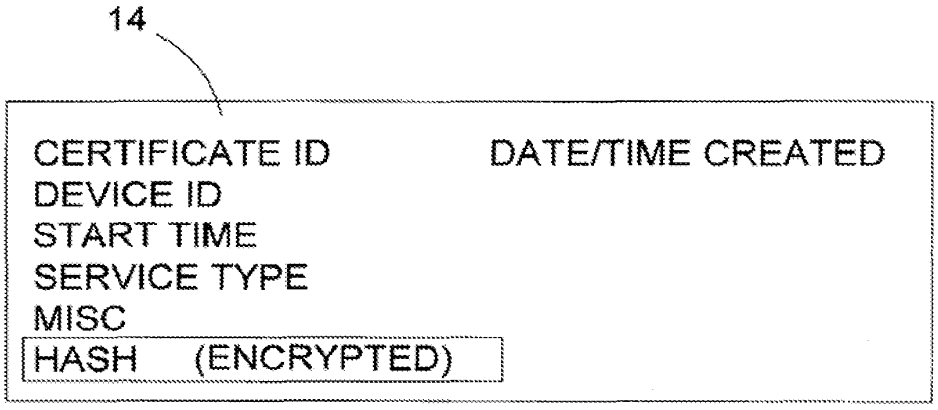

14
CERTIFICATE ID
DATE/TIME CREATED
DEVICE ID
START TIME
SERVICE TYPE
MISC
HASH (ENCRYPTED)

FIG. 2

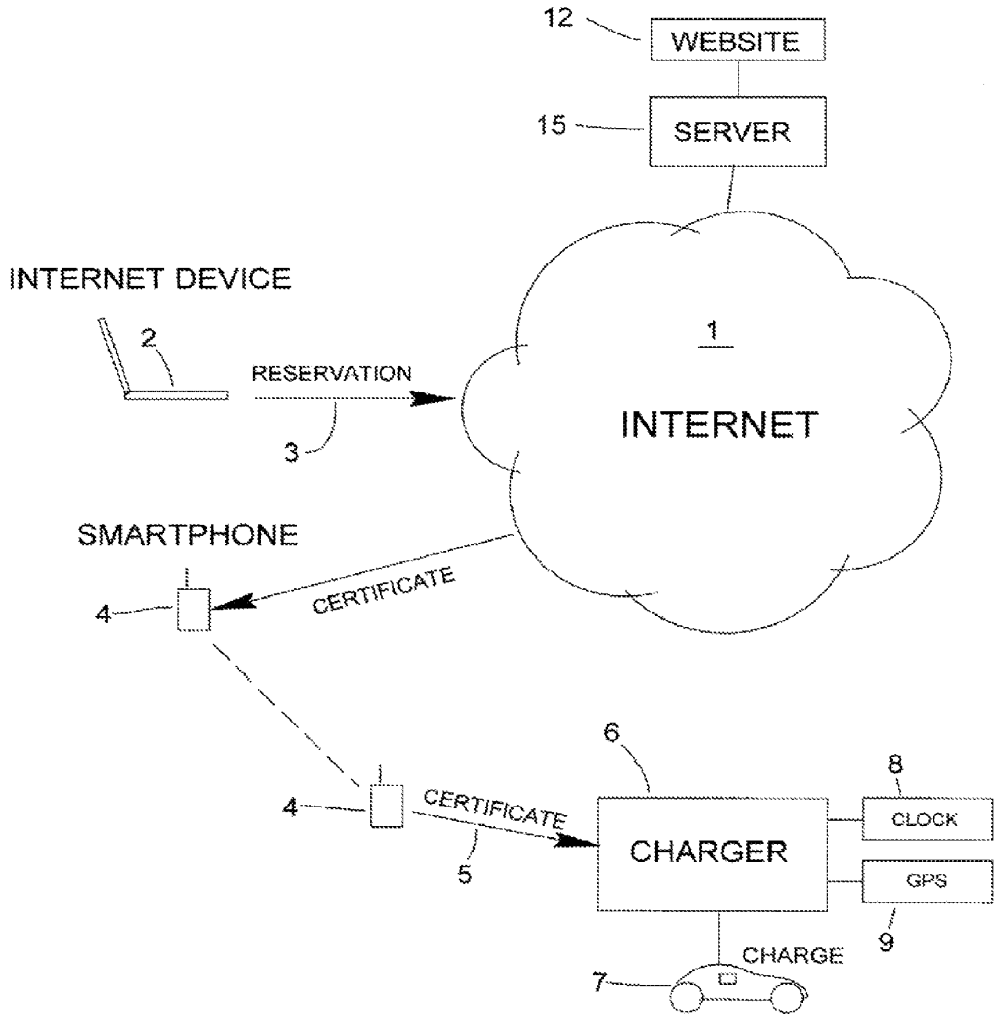

12
WEBSITE
15
SERVER
INTERNET DEVICE
2
RESERVATION
3
1
INTERNET
SMARTPHONE
4
CERTIFICATE
6
8
4
CERTIFICATE
CHARGER
CLOCK
GPS
5
9
CHARGE
7

FIG. 3

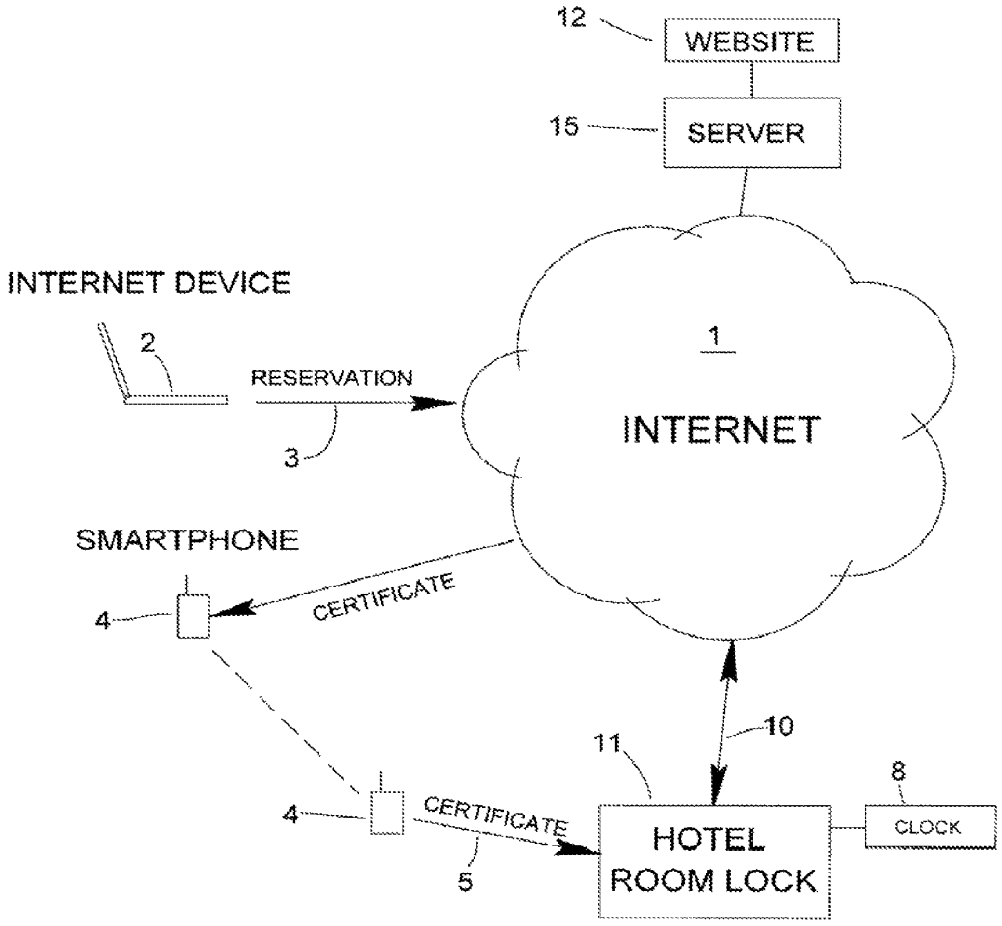

12
WEBSITE
15
SERVER
INTERNET DEVICE
2
RESERVATION
3
1
INTERNET
SMARTPHONE
4
CERTIFICATE
10
11
8
4
CERTIFICATE
5
HOTEL
ROOM LOCK
CLOCK

FIG. 4

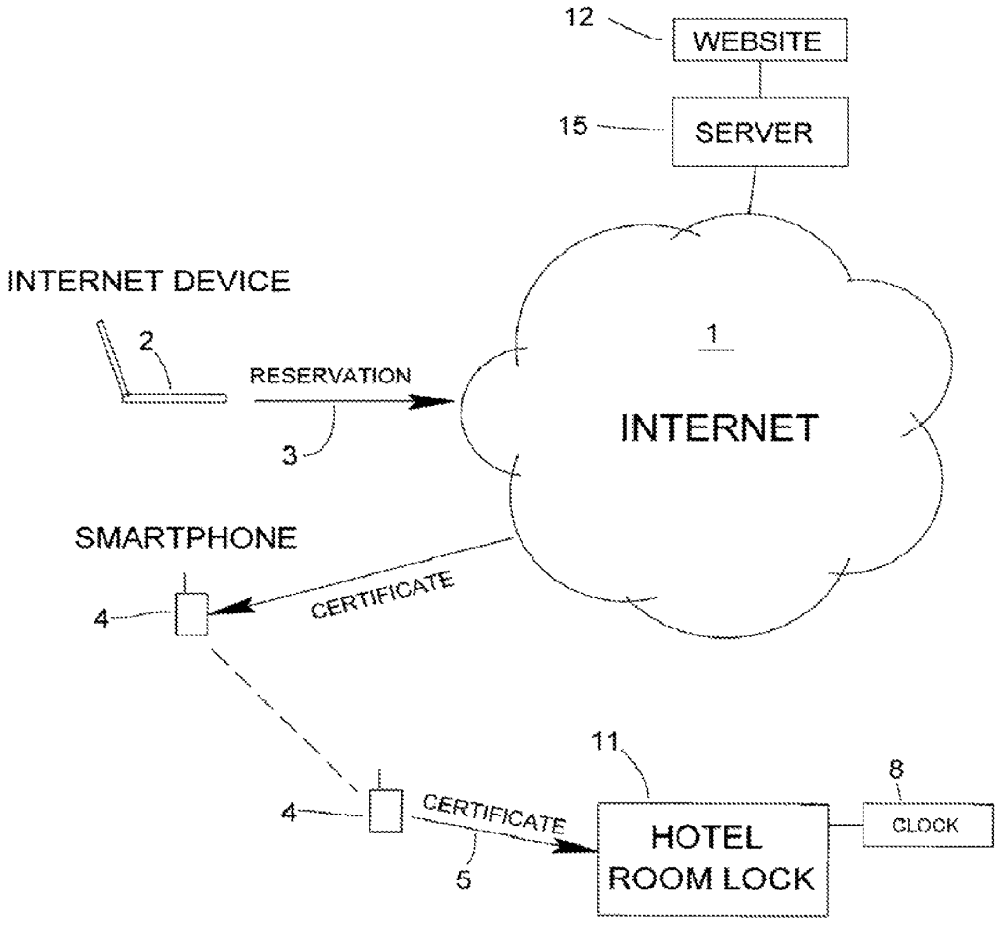

12
WEBSITE
15
SERVER
INTERNET DEVICE
2
RESERVATION
3
1
INTERNET
SMARTPHONE
4
CERTIFICATE
11
8
4
CERTIFICATE
5
HOTEL
ROOM LOCK
CLOCK

FIG. 5

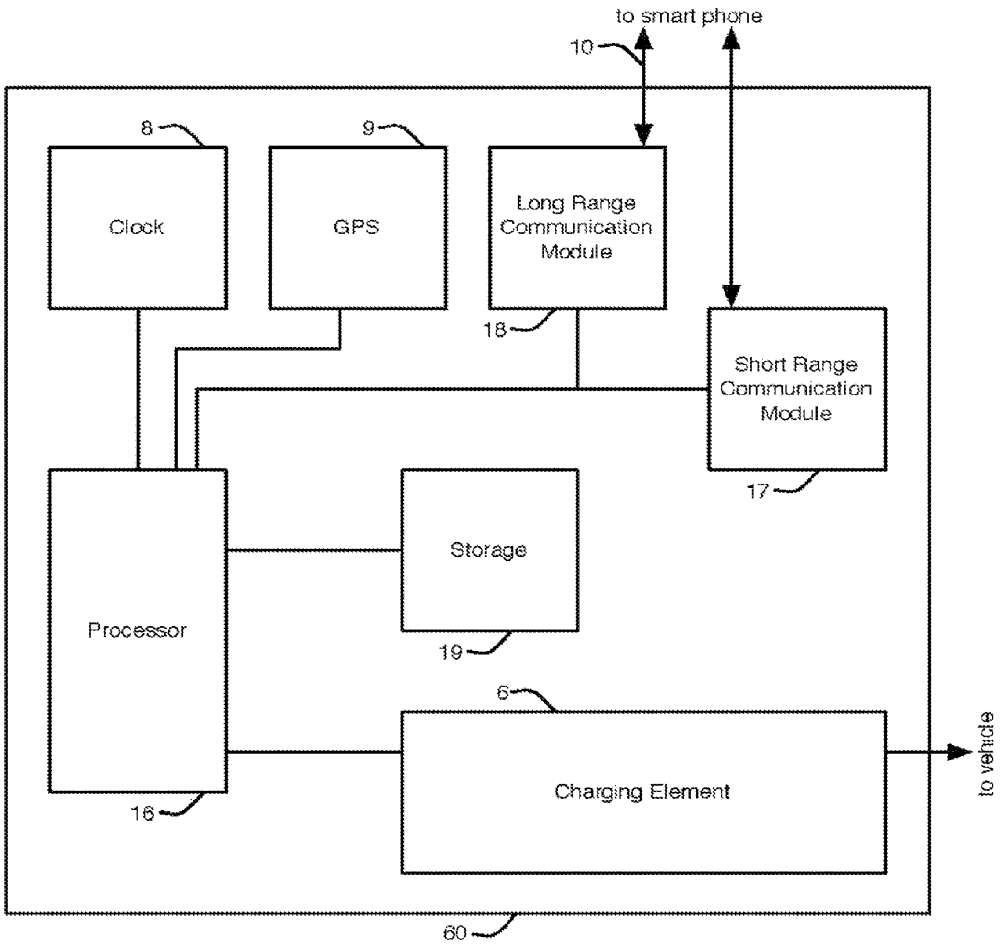

to smart phone
10
8
9
Clock
GPS
Long Range Communication Module
18
Short Range Communication Module
17
Storage
19
Processor
16
6
Charging Element
to vehicle
60

FIG. 6

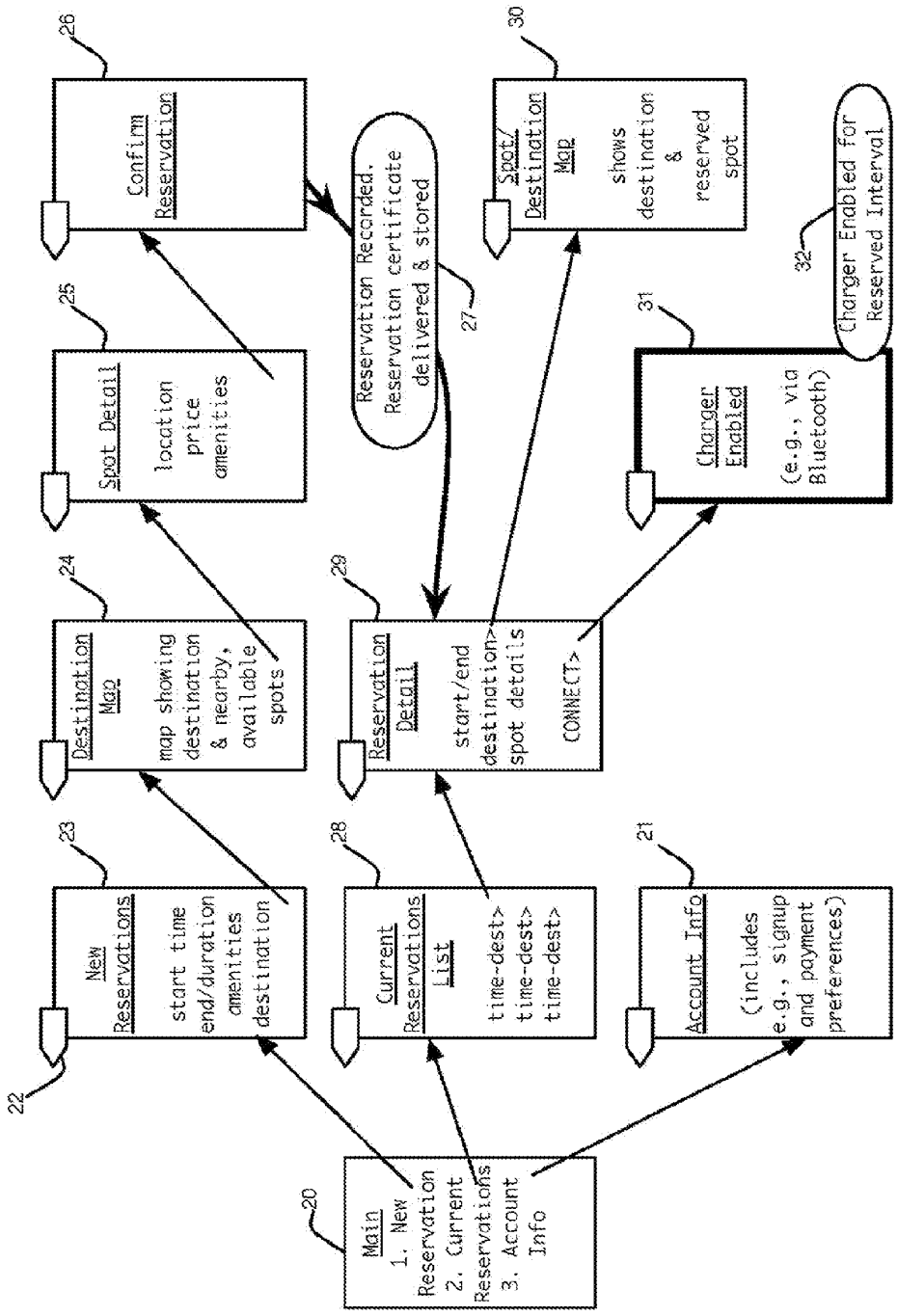

Main
1. New Reservation
2. Current Reservations
3. Account Info
20
New Reservations
start time
end/duration
amenities
destination
22
23
Current Reservations List
time-dest>
time-dest.>
time-dest>
28
Account Info
(includes e.g., signup and payment preferences)
21
Destination Map
map showing destination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

FIG. 7

ACCESS CONTROL SYSTEM AND METHOD FOR USE BY AN ACCESS DEVICE

CROSS-REFERENCE TO RELATED APPLICATION

This application is a continuation of U.S. patent application Ser. No. 13/582,467, filed Sep. 4, 2012, now U.S. Pat. No. 8,996,876, which is a national stage application of PCT Application No. PCT/US11/26781, filed Mar. 2, 2011, which claims the benefit of U.S. Provisional Patent Application No. 61/309,813, filed Mar. 2, 2010. All of the above mentioned applications are incorporated by reference herein in their entireties.

INTRODUCTION

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

As the smart phone approaches the charger or access device, a wireless connection is made (e.g., via Bluetooth™, Zigbee™, 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 inopportunely 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.)

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.

Funds transfer for the access service can be made by the website at the time of reservation from a user's account, from a money transfer service like PAYPAL™ or by receiving funds from a credit card similar to any other e-transaction. In addition, if the charger or access device is web-enabled, the device itself can report back that the charging took place or the access was allowed. Since the digital token or certificate has a reserved charging time, the certificate will 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

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

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

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

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

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

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

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

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

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

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.

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.

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.

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 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).

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.

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.

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.

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

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;

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

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

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

For security, in some embodiments, the first portion of the certificate can be hashed, and the hash encrypted using the public key of the charger. Upon receipt by the charger, the hash is decrypted using the private key of the charger, and the hash result compared with the charger's internal hash calculation. If the two match, then nobody has edited the reservation and the certificate may be trusted as authentic. This is safe unless someone cracks the key of the charger. In that case, only one charger **6** is affected. An alternative embodiment may use a signed hash or checksum. Here, the hash is computed as above, then encrypted with a private key held by a trusted authority such as the website.

Upon receipt, anyone, including the smart phone and the charger, can use the trusted authority's public key to decrypt the hash and compare that to the hash they run. This method is safe unless someone cracks the private key of the website. In still another embodiment, a Signed-then-Encrypted Hash/Checksum is used. Here the signed hash is encrypted so that only the charger can read it. This way, the private keys of both the charger **6** and the website server **15** need to be compromised, and then only that charger is threatened.

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.

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.

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.

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.

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.

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.

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**.

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.

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

The New Reservations **23** screen accepts a start-time, an end-time (or duration), and a destination.

Required amenities can be selected, including for the present invention, available charging for an EV (which may further include a selection for Level 1 or Level 2 charging, for instance). The destination may be an actual parking location, but more commonly (and as illustrated herein) it is the patron's destination for which nearby parking is sought.

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.

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.

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.

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).

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.

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.

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.

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.

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.

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.

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 device for use in an access control system, the access device comprising:

a processor (**16**) having control of a door lock (**11**); and

a communication module (**17**) connected to the processor, the processor able to receive a reservation certificate (**5**) presented by a portable terminal (**4**) through the communication module;

wherein the processor activates the door lock when a current reservation certificate has been presented.

2. The access device of claim **1** wherein the processor activates the door lock for up to a predetermined duration.

3. The access device of claim **2** wherein the predetermined duration is all day.

4. The access device of claim **1** wherein the reservation certificate comprise data representative of a duration and the processor activates the door lock for up to the duration.

5. The access device of claim **1** wherein the processor has access to the current time, the reservation certificate comprises data representative of an interval of the reservation, and the processor activates the door lock during the interval.

6. The access device of claim **5** wherein the interval is specified by a start time and one of an end time and a duration.

7. The access device of claim **1** further comprising:

a memory to which the processor has access, the memory containing a public key for a server authorized to issue the reservation certificate;

wherein at least a portion of the reservation certificate is encrypted by the server using a private key and the processor verifies that the reservation certificate is genuine by decrypting the portion with the public key.

8. The access device of claim 1 further comprising:

a memory to which the processor has access, the memory containing a symmetric key;

wherein at least a portion of the reservation certificate is encrypted by a server using the symmetric key and the processor verifies that the reservation certificate is genuine by decrypting the portion with the symmetric key.

9. The access device of claim 1 wherein the processor verifies that the reservation certificate is genuine.

10. The access device of claim 1 further comprising:

an identification to which the processor has access, the identification corresponding to one of the access device and the door lock, wherein the processor determines that the reservation certificate comprises data representative of the identification.

11. The access device of claim 1 further comprising:

a memory to which the processor has access, the memory containing a private key of the access device;

wherein at least a portion of the reservation certificate is encrypted by a server using a corresponding public key for the access device and the processor decrypts the portion with the private key.

12. The access device of claim 1 wherein the processor has access to a server through the communication module and the processor reports to the server that door lock was activated on the basis of the reservation certificate.

13. A method for use by an access device in an access control system, the method comprising:

a) accepting, by a processor through a communication module, a reservation certificate presented with a portable terminal;

b) determining, by the processor, that the reservation certificate is current; and

c) activating, by the processor on the basis of the reservation certificate being current, a door lock.

14. The method of claim 13 wherein the certificate is current for up to a predetermined duration.

15. The method of claim 14 wherein the predetermined duration is all day.

16. The method of claim 13 wherein the reservation certificate comprises data representative of a duration and the certificate is current for up to the duration.

17. The method of claim 13 wherein the processor has access to the current time and the reservation certificate comprises data representative of an interval of the reservation, and the certificate is current for up to the interval.

18. The method of claim 17 wherein the interval is specified by a start time and one of an end time and a duration.

19. The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a private key for which the corresponding public key is stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the public key, and the c) activating is on the further basis of the reservation certificate being genuine.

20. The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a symmetric key stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the symmetric key, and the c) activating is on the further basis of the reservation certificate being genuine.

21. The method of claim 13 wherein the b) determining by the processor is further that the reservation certificate is genuine, and the c) activating is on the further basis of the reservation certificate being genuine.

22. The method of claim 13 wherein the processor has access to an identification, the identification corresponding to one of the access device and the door lock, wherein the b) determining by the processor is further that the reservation certificate comprises data representative of the identification, and the c) activating is on the further basis of the reservation certificate comprising data representative of the identification.

23. The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a public key for which the corresponding private key is stored in a memory accessible to the processor, the method further comprising the step of:

d) decrypting the portion, by the processor, with the private key.

24. The method of claim 13 wherein the processor has access to a server through the communication module, the method further comprising the step of:

d) reporting to the server that the door lock was activated on the basis of the reservation certificate.

* * * * *

APPENDIX B

US 20030208386A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2003/0208386 A1**

Brondrup (43) **Pub. Date: Nov. 6, 2003**

(54) **WIRELESS RESERVATION, CHECK-IN, ACCESS CONTROL, CHECK-OUT AND PAYMENT**

(76) Inventor: **Rayner Brondrup**, Asker (NO)

Correspondence Address:
NIXON & VANDERHYE, PC
1100 N GLEBE ROAD
8TH FLOOR
ARLINGTON, VA 22201-4714 (US)

(21) Appl. No.: **09/788,402**

(22) Filed: **Feb. 21, 2001**

(30) **Foreign Application Priority Data**

Feb. 25, 2000 (NO) 2000 0491

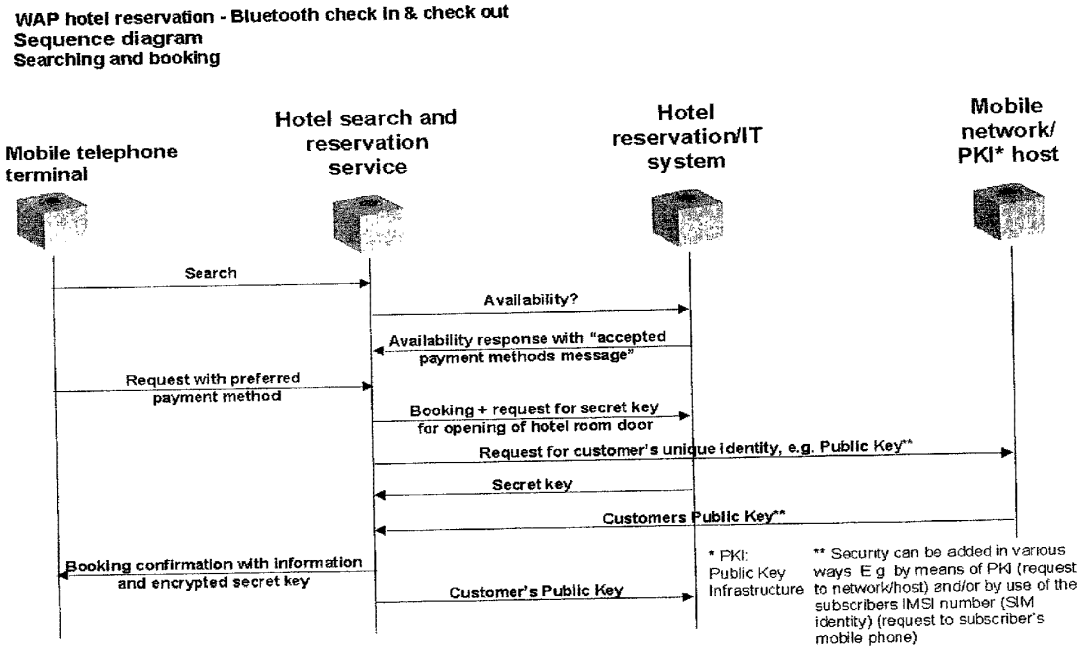
Publication Classification

(51) **Int. Cl.**[7] **G06F 17/60**

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

(57) **ABSTRACT**

A system and method for, by means of a mobile terminal, wireless hotel search and selection, reservation/booking, check-in, room access control, check-out and payment services for hotel customers is disclosed. The mobile terminal **(1)** comprises a mobile telephone and processing unit **(23)**, operating with wireless applications, for wireless communication **(2)** with a hotel search and reservation server **(12)** and a reservation/IT system **(7)** of a selected hotel, and a short-range wireless device **(25)** for wireless communication **(10)** with wireless devices **(9,16)** of door locks **(32)** and user locating arrangements, respectively. By means of the wireless application of the mobile terminal **(1)**, the user reserves a hotel room. A hotel room key token is transferred from the reservation/IT system **(7)** to the wireless device **(35)** of the mobile terminal, and hence to the wireless door lock **(9,32)**. When the terminal **(1)** and the wireless door lock **(9,31)** are in-range, the hotel room key token is transferred from mobile terminal **(1)** to the wireless door lock **(9,32)**, the door is unlocked and check-in is registered. On departure, exit or expiration of the reservation period, the system provides wireless check-out and electronic bill settlement.



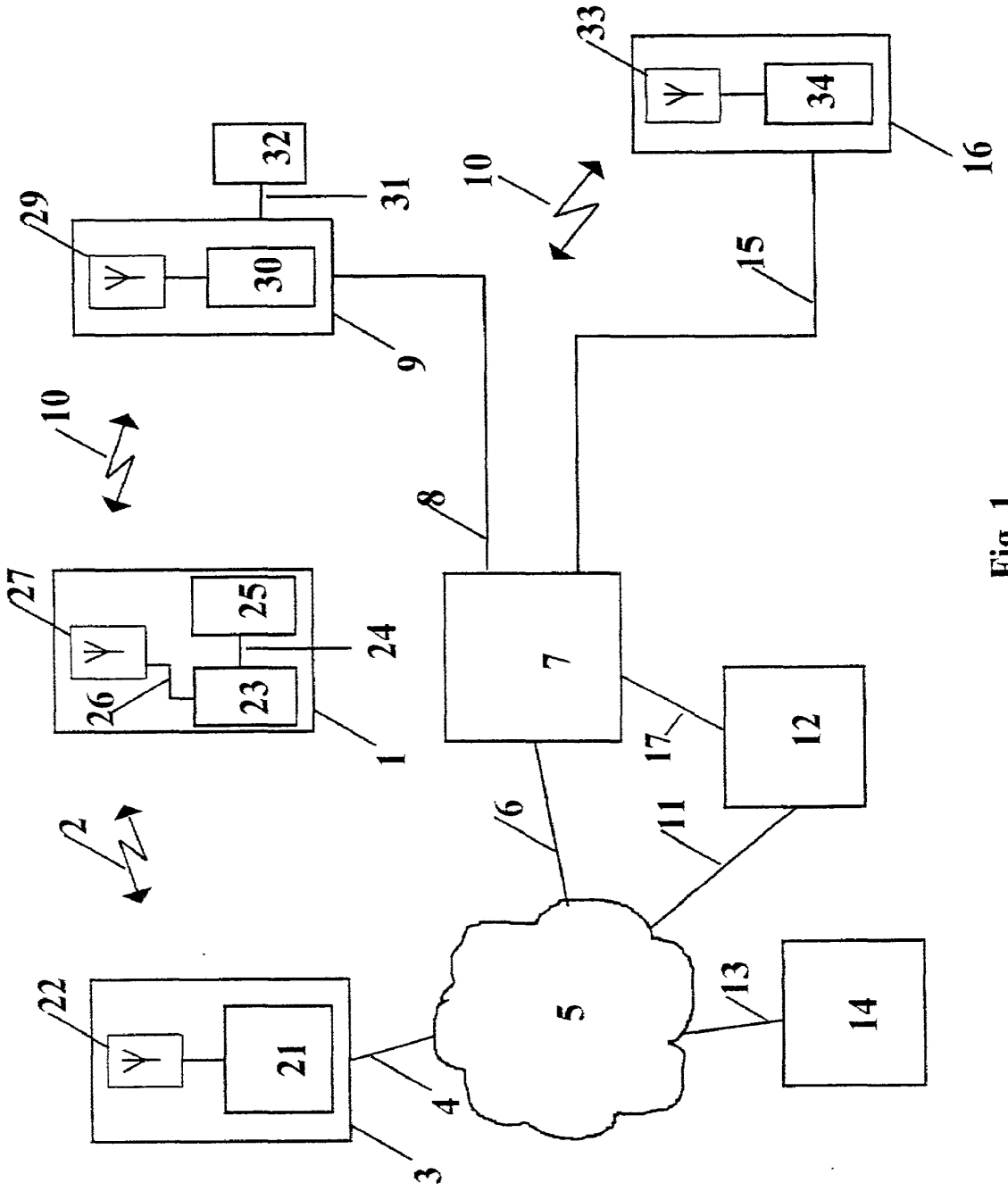

33
34
16
32
31
10
29
30
15
9
10
8
27
25
24
7
26
23
1
12
17
2
6
11
22
21
5
13
14
4
3

Fig. 1

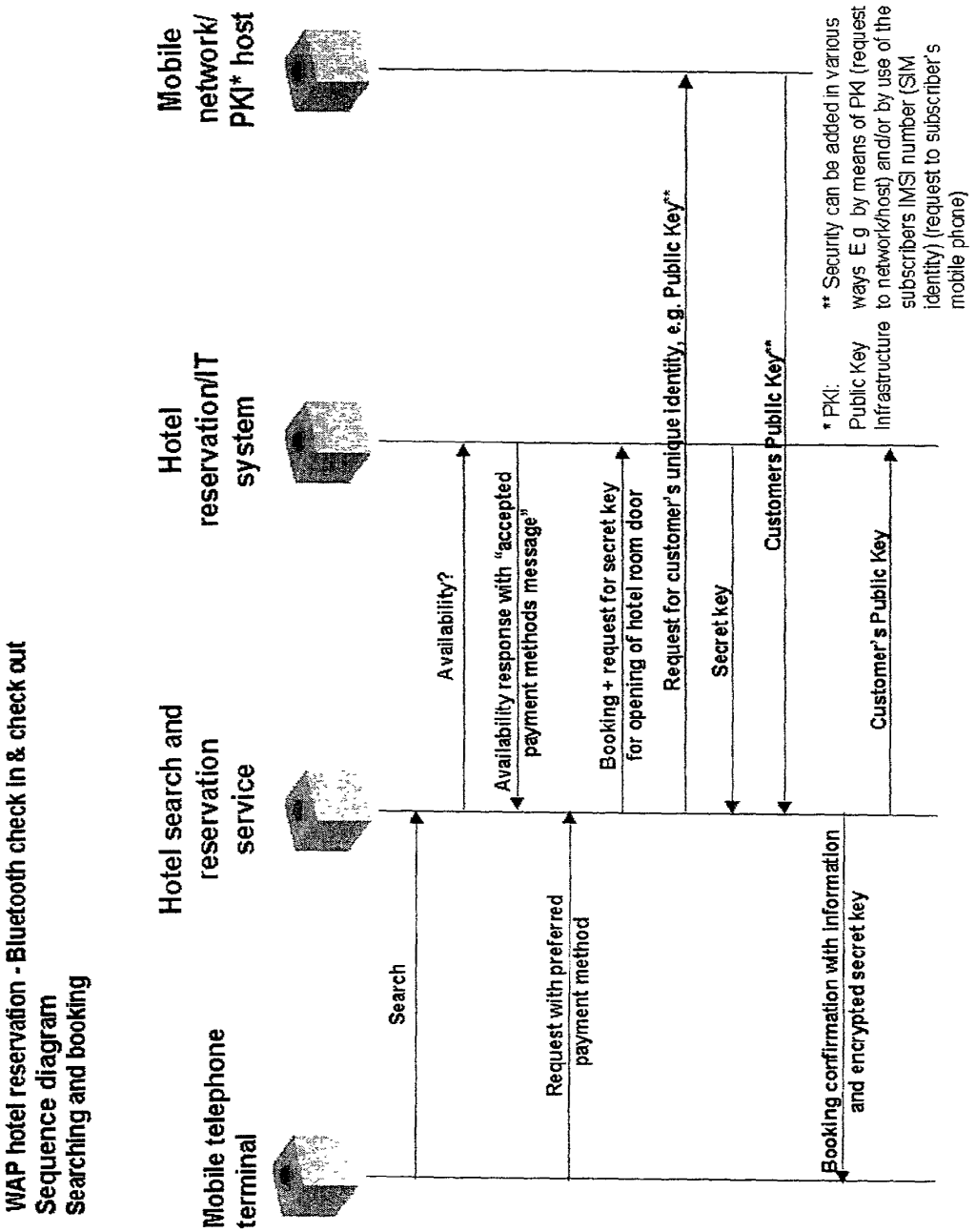

WAP hotel reservation - Bluetooth check in & check out
Sequence diagram
Searching and booking
Mobile telephone terminal
Hotel search and reservation service
Hotel reservation/IT system
Mobile network/ PKI* host
Search
Availability?
Availability response with "accepted payment methods message"
Request with preferred payment method
Booking + request for secret key for opening of hotel room door
Request for customer's unique identity, e.g. Public Key**
Secret key
Customers Public Key**
Customer's Public Key
Booking confirmation with information and encrypted secret key
* PKI: Public Key Infrastructure
** Security can be added in various ways E g by means of PKI (request to network/host) and/or by use of the subscribers IMSI number (SIM identity) (request to subscriber's mobile phone)

Fig. 2

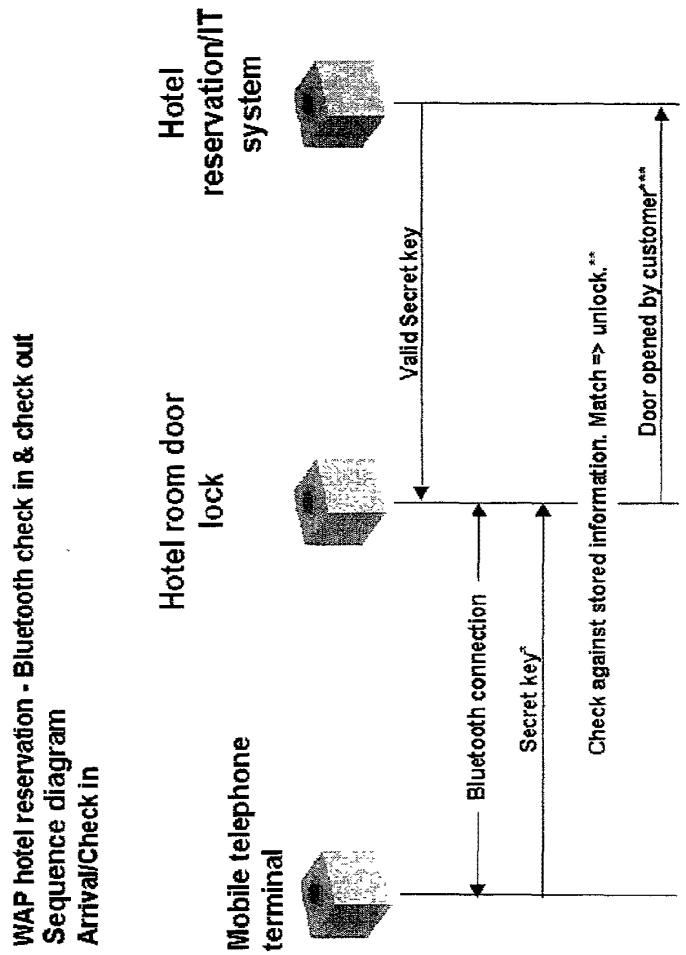

WAP hotel reservation - Bluetooth check in & check out
Sequence diagram
Arrival/Check in
Mobile telephone terminal
Hotel room door lock
Hotel reservation/IT system
Bluetooth connection
Secret key*
Check against stored information. Match => unlock.**
Valid Secret key
Door opened by customer***
* If PKI has been used as a means of security the secret key is embedded in a Private Key from the mobile phone
** The checking may be done in the lock or by checking against the hotel IT system
*** The first time during each stay that the door is opened, this initiates a check in registration in the hotel IT system

Fig. 3

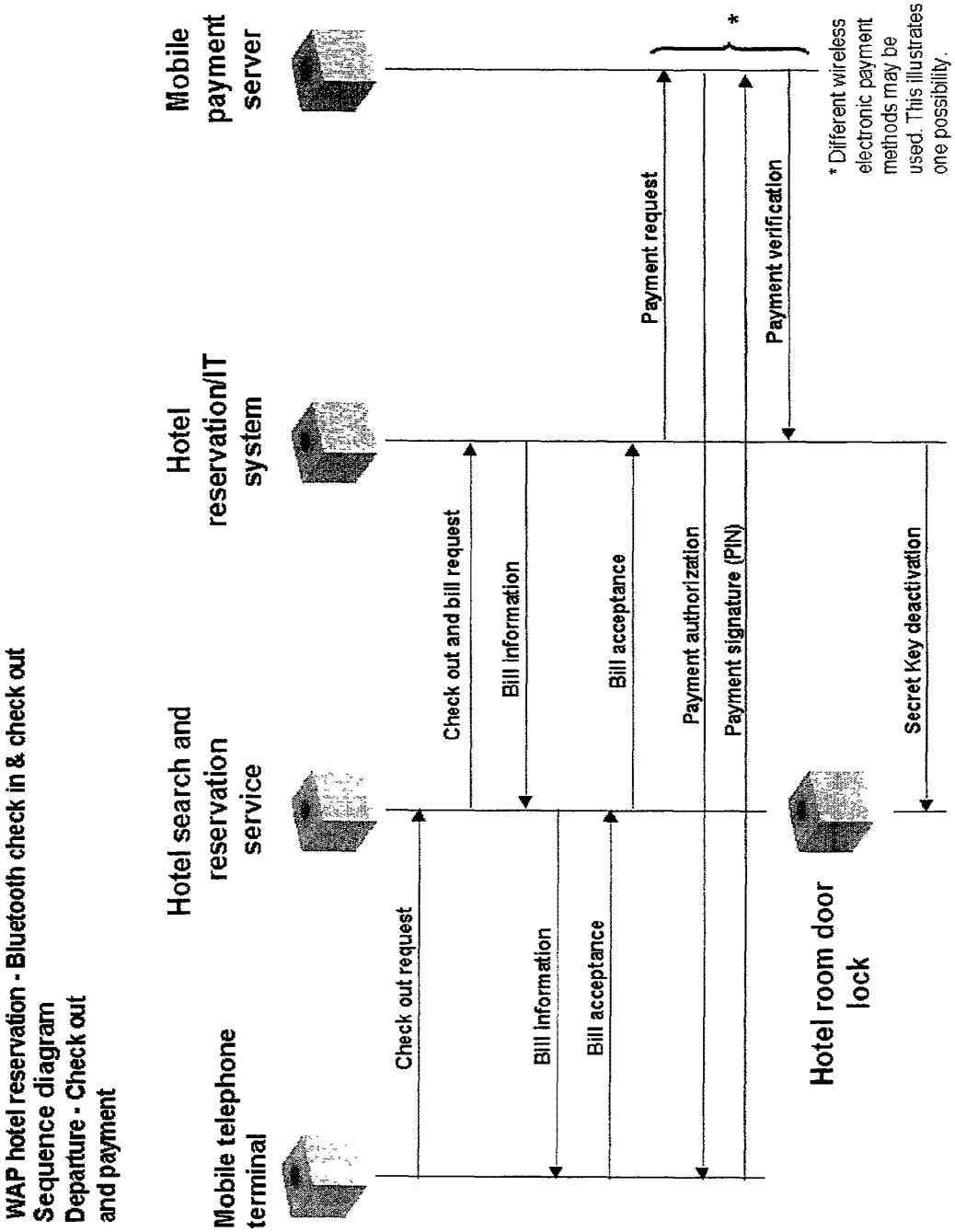

WAP hotel reservation - Bluetooth check in & check out
Sequence diagram
Departure - Check out
and payment
Mobile telephone terminal
Hotel search and reservation service
Hotel reservation/IT system
Mobile payment server
Hotel room door lock
Check out request
Bill information
Bill acceptance
Check out and bill request
Bill information
Bill acceptance
Payment authorization
Payment signature (PIN)
Payment request
Payment verification
Secret Key deactivation
*
* Different wireless electronic payment methods may be used. This illustrates one possibility.

Fig. 4

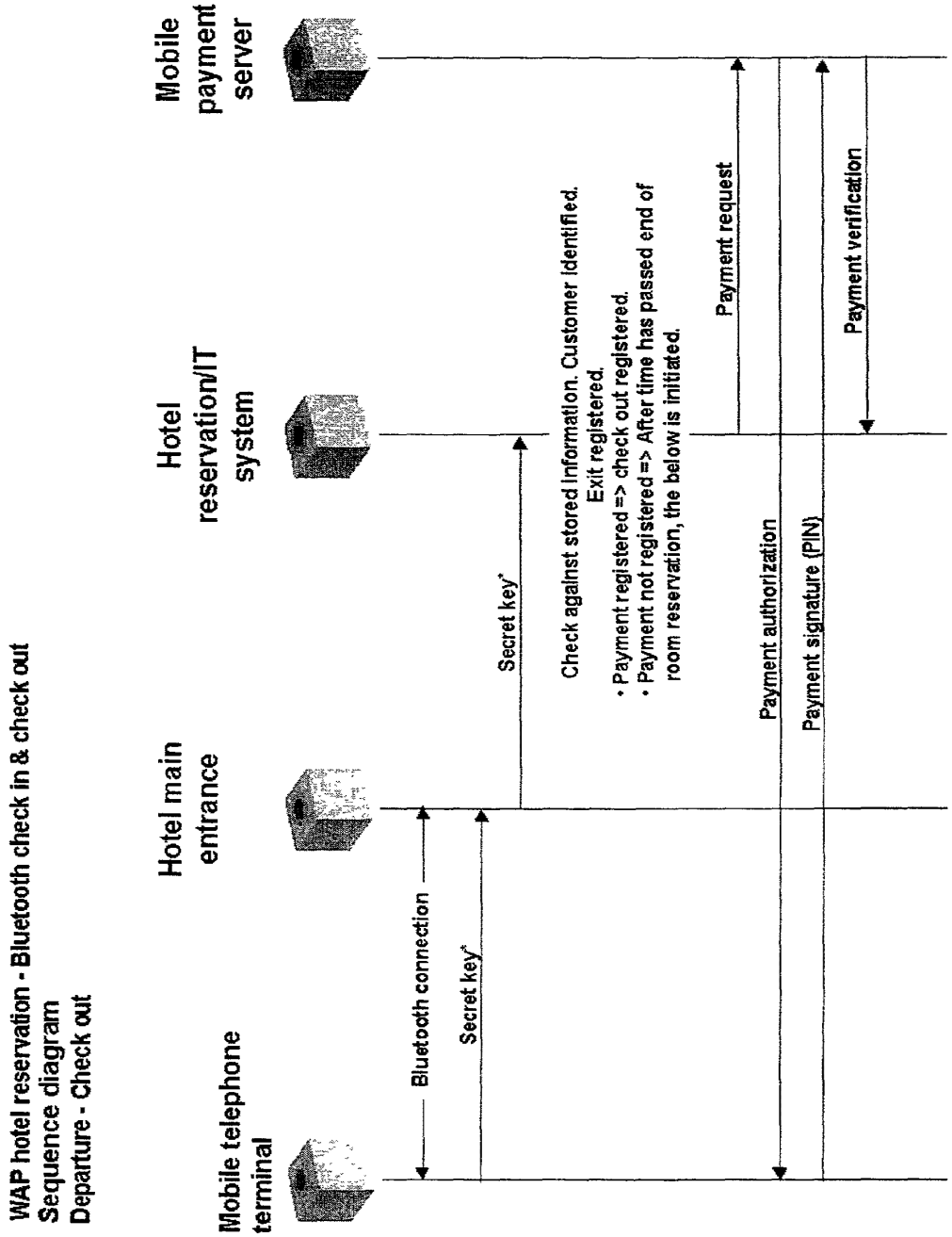

WAP hotel reservation - Bluetooth check in & check out
Sequence diagram
Departure - Check out
Mobile telephone terminal
Hotel main entrance
Hotel reservation/IT system
Mobile payment server
Bluetooth connection
Secret key'
Secret key'
Check against stored information. Customer identified.
Exit registered.
• Payment registered => check out registered.
• Payment not registered => After time has passed end of room reservation, the below is initiated.
Payment request
Payment authorization
Payment signature (PIN)
Payment verification

Fig. 5

WAP hotel reservation - Bluetooth check-in and check-out
Check-in and door lock activation
Hotel
reservation/IT
system
Hotel lock activated with the travelers
Bluetooth/terminal identity automatically at the
appropriate time in accordance with booking
Hotel
Upon arrival the traveler walks straight to
the appointed room as confirmed through
the WAP reservation service. The door
recognizes the travelers Bluetooth/terminal
identity and opens automatically as the
traveler approaches the door. This also
registers the check in in the hotel IT system.

Fig. 6

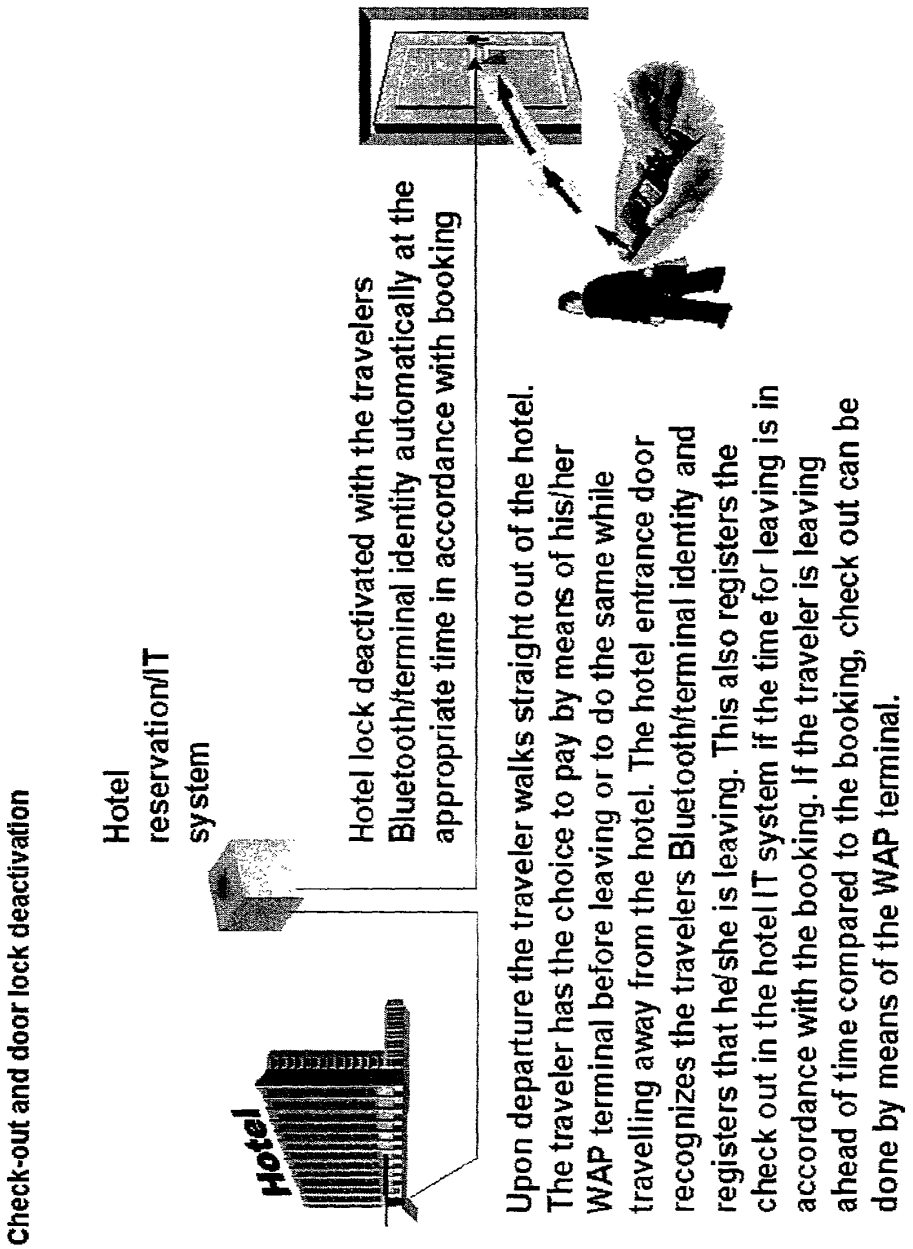

Check-out and door lock deactivation
Hotel
reservation/IT
system
Hotel lock deactivated with the travelers Bluetooth/terminal identity automatically at the appropriate time in accordance with booking
Hotel
Upon departure the traveler walks straight out of the hotel. The traveler has the choice to pay by means of his/her WAP terminal before leaving or to do the same while travelling away from the hotel. The hotel entrance door recognizes the travelers Bluetooth/terminal identity and registers that he/she is leaving. This also registers the check out in the hotel IT system if the time for leaving is in accordance with the booking. If the traveler is leaving ahead of time compared to the booking, check out can be done by means of the WAP terminal.

Fig. 7

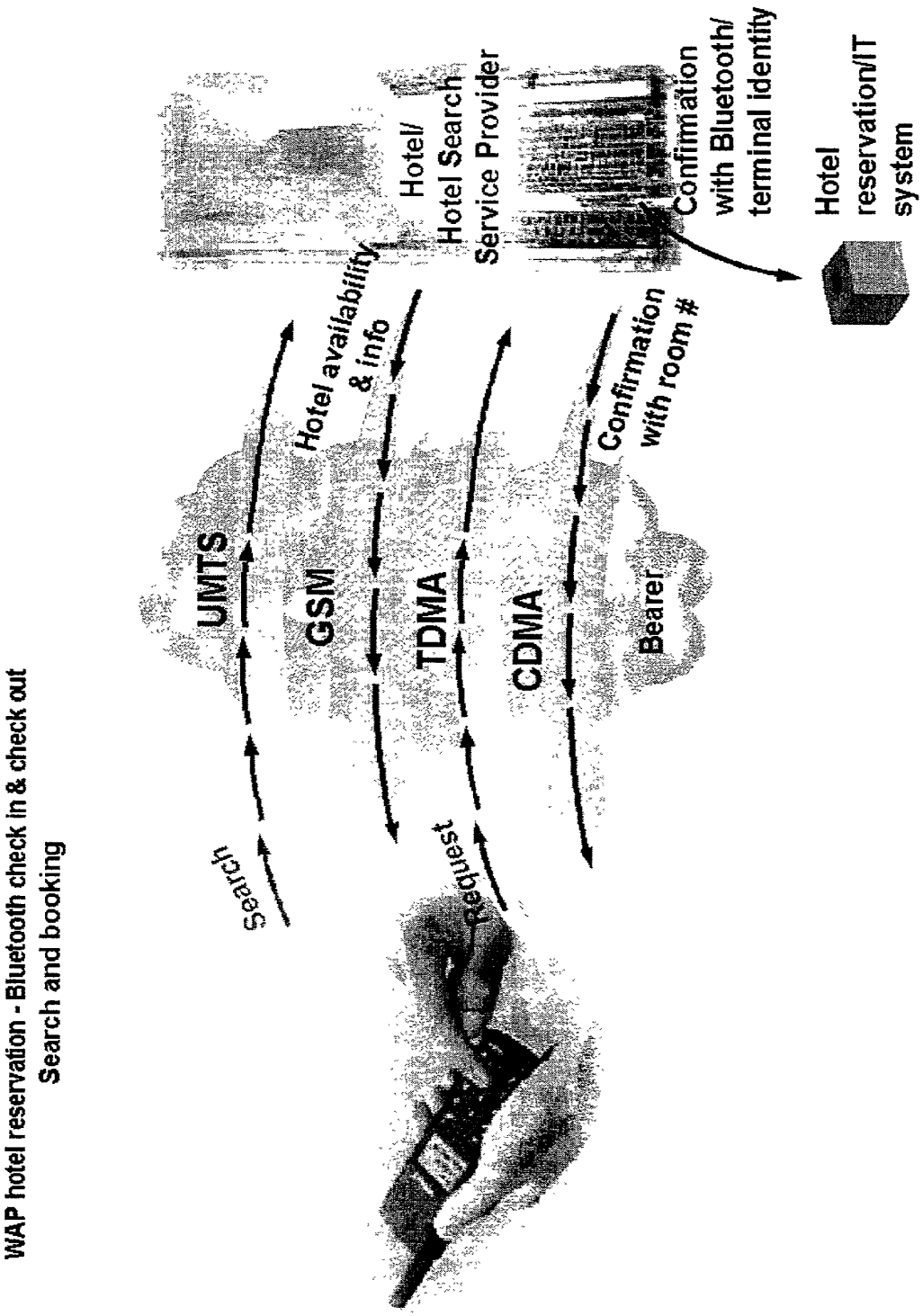

WAP hotel reservation - Bluetooth check in & check out
Search and booking
Search
Request
UMTS
GSM
TDMA
CDMA
Bearer
Hotel availability & info
Confirmation with room #
Hotel/ Hotel Search Service Provider
Confimation with Bluetooth/ terminal identity
Hotel reservation/IT system

Fig. 8

WIRELESS RESERVATION, CHECK-IN, ACCESS CONTROL, CHECK-OUT AND PAYMENT

FIELD OF THE INVENTION.

[0001] The present invention relates to the field of provision of wireless services for reservation, check-in, access control, check-out and payment, preferably for hotel customers by means of wireless application programs employing standard protocols operating on wireless user terminals provided with a wireless long or medium range communications and processing unit, such as a mobile telephone, and wireless short range device, such as a device complying with the Bluetooth industry standard.

[0002] The Problem Areas.

[0003] The invention addresses the following problem areas:

[0004] The problem of a traveller on the move to find a suitable hotel, particularly in foreign cities.

[0005] The problem of a traveller on the move who has to rely on the opening hours of travel agencies for finding hotels.

[0006] The problem of a traveller on the move of sitting in long and costly telephone 'waiting lines' with travel agencies to make hotel reservations.

[0007] Hotels difficulties in reaching the customers directly when they are looking for hotels in given areas.

[0008] Hotels challenge in building loyalties with frequent travellers.

[0009] Problems related to long check-in and/or check-out lines in many hotels for guest check-in, check-out and bill settlement.

[0010] Problems related to operation of locks requiring manual operations.

[0011] Known Solutions and Problems with These.

[0012] When wanting to book a hotel room, travellers often find themselves in long travel agency telephone 'waiting lines'. In addition, once a connection has been established, the communication with the travel agency agent introduces a distortion between the hotels' information and the traveller, e.g. in the understanding of hotel standard, quality, service level, etc. This occasionally makes the finding of a suitable hotel room slow, and unsafe as to whether the traveller is really getting what he/she requests. In addition the traveller is dependent on the travel agency's opening hours for the reservation/booking of hotel rooms in foreign cities.

[0013] For the hotel this also makes loyalty building and marketing to the end customer more difficult, since the travel agency, with it's agreements with different hotels, is the interface of traveller.

[0014] Norwegian patent publication no. NO 179888 to Ohrn discloses a system and method suitable for remote services searching, making reservations, ordering and confirming of orders, but does not provide for wireless registration, hotel check-in, room access control, hotel check-out and payment.

[0015] Another problem is the hotel check-in and the key for the hotel room door lock. The opening of a traditional hotel room door lock requires that the customer has been checked in through the reception desk, at which there is at times a long queue waiting for check in, very often to the business travellers annoyance and irritation. Existing hotel room door locks that can be electronically programmed from the hotel reception desk to accept only the key given to the customer. To operate the door locks, the locks require that the user inserts some form of physical key.

[0016] U.S. Pat. No. 5,614,703 to Martin et. al. discloses a system and for hotel check-in and check-out without the need for a desk clerk, wherein guest registration etc. is done by reading a card by means of a card reader, such as a magnetic credit card reader, located at the reserved hotel room.

[0017] Yet another problem is hotel check-out and payment. When leaving the hotel, the traveller often has to wait in a long check out line to settle the bill—while at times risking to be late for an important meeting or even to miss a flight.

[0018] On-line reservation/booking by means of Internet requires an Internet connection which may be a problem for the traveller when the traveller does not carry along a computer or a similar device which is capable of accessing the Internet. However, if the traveller should happen to have such a device, the start up of the device is still needed, and if the connection between the device and the Internet is made by means of a mobile telephone, a rather slow connection through a mobile phone will typically result in long connection times and, consequently, expensive phone bills. To alleviate this problem, hotel reservation/booking applications based on the Wireless Application Protocol (WAP) are also currently being developed and tested in various locations. However, to the knowledge of the applicant, none of these combine all of the following elements or services:

[0019] Search for a hotel that matches the user's preferences

[0020] Provision of a selection if several choices exist

[0021] Payment integrated with the reservation/booking

[0022] Provision of a reference number (booking token) that both serves as a receipt for accepted payment and as a key parameter in the communication protocol for door lock opening.

OBJECTS OF THE INVENTION

[0023] It is an object of the invention to provide a system and a method that alleviates a number of the above mentioned problems and limitations of the prior art systems, and which also integrate functions of previously separate systems to provide wireless hotel search, reservation/booking, check-in, room access control, check-out and payment services for hotel customers.

BRIEF DISCLOSURE OF THE INVENTION

[0024] In one aspect of the present invention, the invention provides a system providing wireless hotel search and selection, reservation/booking, check-in, room access con-

trol, check-out, and payment services for hotel customers by combining a wireless application for hotel search and reservation/booking services, a aireless application for check-out and payment services, and wireless hardware and applications for hotel locks. Systems according to the invention can include a plurality of mobile terminals, each mobile terminal having a short range wireless device and a long or medium range wireless communications and processing unit, at least one hotel search and reservation/booking serve means, and a plurality of hotel reservation/information technology (IT) systems to the communication network means and communication network means allowing these to communicate, wherein each such hotel reservation/IT system is in communication with an associated plurality of corresponding wireless devices associated with locks such as electrically operable door locks. The door lock wireless devices are short range devices capable of communicating with compatible wireless devices of in-range mobile terminals. Preferably, the wireless devices of the mobile terminals and the wireless door locks are devices complying with the Bluetooth industry standard. Systems according to the invention further include electronic payment server means capable of communicating with other elements of the system by means of said communication network means.

[0025] Optionally, systems according to the invention can also include additional short range wireless devices associated with and communicating with the hotel reservation/IT system for providing communication with nearby compatible and appropriately adapted mobile terminals. Such additional devices can be installed at the entrances and/or exits of a hotel employing a system according to the invention

[0026] In another aspect of the present invention, the invention provides a method providing wireless hotel search and selection, reservation/booking, check-in, room access control, check-out and/or payment services for hotel customers by means of a system combining wireless application for search and reservation/booking services, a wireless application for check-out and payment services, and wireless hardware and applications for hotel door locks. A method according to the invention can include the steps of a user by means of a properly adapted wireless mobile terminal connecting to a hotel search and reservation/booking server, searching for, finding and selecting a suitable hotel, sending a reservation/booking request and optionally information on a preferred method of payment to a connected hotel reservation/IT system and thereby making a reservation, receiving by the wireless long or medium wireless communications and processing unit of the mobile terminal a reservation/booking request confirmation including a key token, transferring the key token from the communications and processing unit to the wireless device of the mobile terminal, transmitting from the hotel reservation/IT system the key token to a wireless device associated with a door lock of the reserved hotel room, and, upon arrival at the hotel of the user carrying the mobile terminal, wirelessly, by means of the wireless device of the mobile terminal, transmitting the key token to nearby wireless devices associated with electrically operated door locks whereby, on receiving the appropriate key token, the arrival of the user is registered in the hotel reservation/IT system, and the door lock wireless device of the reserved room unlocks the door. Further, a method according to the invention includes, for user check-out from the hotel, the additional steps of a user, by means of the mobile terminal, connecting to a hotel search and reservation/booking server, and, while connected to the hotel search and reservation/booking server, communicating to the hotel reservation/IT system a check-out request, receiving therefrom bill information, sending thereto a bill acceptance, receiving from a payment server a payment authorisation request, sending thereto a payment authorisation response, and by the hotel reservation/IT system, upon receiving receiving a payment verification, sending a key token deactivation message to the door lock associated wireless device of the reserved room. Further, the method can include steps of encryption, whereby the key token is encrypted to become an encrypted secret key.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] **FIG. 1** is a simplified block diagram of an example of a system for wireless hotel search, reservation/booking, check-in, room access control, check-out and payment services according to the invention;

[0028] **FIG. 2** is a sequence diagram illustrating an example of steps of wireless hotel search, reservation/booking and key token transfer of an example of a method according to the invention;

[0029] **FIG. 3** is a sequence diagram illustrating an example of steps of wireless hotel door unlocking and guest registration of an example of a method according to the invention;

[0030] **FIG. 4** is a sequence diagram illustrating an example of steps of wireless hotel check-out, billing, payment and key deactivation of an example of a method according to the invention;

[0031] **FIG. 5** is a sequence diagram illustrating an example of steps of wireless hotel departure registration, check-out, billing and payment of an example of a method according to the invention;

[0032] **FIG. 6** illustrates an example of a hotel guest arrival scenario with wireless and automatic hotel door lock activation and guest check-in registration employing the invention;

[0033] **FIG. 7** illustrates an example of a hotel guest departure scenario for wireless and automatic hotel door lock deactivation and automatic or manual guest check-out registration employing the invention; and

[0034] **FIG. 8** illustrates examples of possible bearers in a wireless system according to the invention.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0035] In the following, with reference to the accompanying drawings, the invention will be explained by way of example.

[0036] In **FIG. 1** is shown a simplified block diagram of an exemplary system embodying the system of invention. The exemplary system includes a plurality of portable wireless mobile terminals **1** capable of wireless communication **2** with a plurality of base stations **3** which have connections **4** to a communication network **5**. Each mobile terminal **1** of the system in this example includes a typical mobile telephone and processing unit **23** provided with appropriate wireless application programs and with a con-

nection **26** to an antenna system **27**. The mobile wireless terminal **1** of the example also includes a short range wireless device **25** with a built-in antenna (not shown) and with a connection **24** to the mobile telephone and processing unit **23**. The telecommunication network **5** has connections **6** to a plurality of hotel reservation/IT systems **7** and connections **11** to at least one hotel search and reservation server **12**. Optionally, one or more hotel search and reservation server **12** ca n have direct links **17** to or be integrated with hotel reservation/IT system **7** of the system. Each hotel reservation/IT system **7** has a plurality of connections **8** to a plurality of short range wireless devices **9**, wherein each wireless device **9** is provided with a connection **31** to an associated door lock **32** which can be operated by the associated wireless device **9**. Optionally, the hotel reservation/IT system **7** can have connections **15** to wireless devices **16** located preferably at entrances/exits of the hotel. For wireless payment services, the system includes at least one payment server **14** with a connection **13** to the telecommunication network **5**. The wireless devices **25** can communicate with in-range wireless devices **9** and **16** by means of wireless connections **10**. For simplicity, in **FIG. 1**, only one unit or device is shown for each element, however, a typical system may equally well comprise a plurality of such units or devices.

[0037] With reference to **FIG. 2**, in one aspect of an embodiment of a method of the invention, the invention provides for wireless hotel reservation/booking by a user. The search for hotels and the possibility to book rooms in accordance with requirements of a user is provided through a WAP interface. The hotel reservation/booking of this example is performed mainly in two stages:

[0038] i. the user searches for a hotel to find one that matches the required criteria;

[0039] ii. the user makes a reservation/booking request in which the actual reservation/booking is performed.

[0040] In the first stage (i), the hotel search of the example is performed by a per se known search engine, intelligent agent or other available means which has access to one or several hotel reservation/booking systems. The user criteria for selecting a hotel can be parameters like location price, features of the hotel etc. The user interface presented to the user on the mobile terminal can be implemented suitably by any suitable application means, e.g known application means such as WAP (WML/WML Script), typical Web applications (HTML/Java Script) or Java Application/Applet. The server side of the application can be built using by means of standard Web application models or other suitable means. In the second stage (ii) of the hotel reservation/booking, the hotel reservation/booking is performed through a wireless application that communicates with the reservation/booking system of the chosen hotel using standard mechanisms according to any suitable application means, such as Wireless Mark-up Language (WML) forms or the ones described above. The user or a user controlled application on the mobile terminal inputs the necessary data needed to perform the reservation/booking and a receipt confirming the reservation/booking is received from the reservation/booking system.

[0041] Also with reference to **FIG. 2**, in another aspect of an embodiment of a method of the invention, the reservation/booking receipt from the hotel reservation system contains a key token such as e.g. a reference number which can be directly used for obtaining access to the reserved room upon arrival at the hotel.

[0042] Optionally, as shown in **FIG. 2**, security can added to the above, e.g. through the use of PKI (Public Key Infrastructure).

[0043] Now, with reference to **FIG. 3**, in a further aspect of an embodiment of a method of the invention, the invention provides for wireless operation of hotel room door locks. After successful reservation, the wireless door lock system of the reserved room receives information about the valid key token, or a secret key, from the hotel reservation/IT system. By means of the short range wireless device in the mobile wireless terminal, the key token is transmitted to nearby wireless devices associated with electrically operable door locks. On receiving the appropriate key token from the wireless device in the mobile wireless terminal, the door lock wireless device of the reserved room can notify the associated hotel reservation/IT system of the arrival of the user for check-in, and unlocks the door. The user is notified of the event, and is given the opportunity to control the door lock by means of a suitable user interface on the mobile wireless terminal. A situation of use of the method explained above is also illustrated in **FIG. 6**.

[0044] The communication protocol between the mobile terminal and the wireless door lock system is performed over a Bluetooth, Infrared or other suitable bearer. To achieve optimal security, this information shouldcould be protected in the user's terminal by means of a PIN code, fingerprint or other local authentication methods.

[0045] The protocol as described can be implemented in several ways; as a generic protocol that uses the Bluetooth data transport directly for information exchange, or it may be implemented using e.g. WAP as a transport mechanism.

[0046] Conventional electrically operated hotel room door locks employed by a system according to the invention may be equipped with Bluetooth chips and functionality. Together with WAP mobile phones equipped with wireless Bluetooth compliant devices, this makes possible mechanisms which may provide new value added services as described below. Such mechanisms may work in the following way:

[0047] Now, with reference to **FIG. 4**, in yet another aspect of an embodiment of a method of the invention, the invention provides for wireless user check-out from the hotel and wireless hotel bill payment. By means of the properly adapted mobile wireless terminal, connection is made to the hotel search and reservation/booking server. While connected to the hotel search and reservation/booking server, a check-out request is communicated to the hotel reservation/IT system by means of a communications network. The hotel reservation/IT system responds by sending back bill information, and the user responds by sending a bill acceptance or rejection message. On receiving the acceptance of the user, the hotel reservation/IT system sends a payment request to the payment server which in turn sends a payment authorisation request to the user. The user then responds to the payment server by sending a payment authorisation message back to the payment server. In turn, the payment sends a payment verification message to the

hotel reservation/IT system verifying that the bill has been paid electronically. Upon receiving the appropriate messages, the hotel reservation/IT system can send a key token deactivation message to the door lock associated wireless device of the reserved room.

[0048] A wireless application for service can be used for checking out of hotels and settling the hotel bill. In this way the customer will not need to wait in a check-out line at the check-out counter of the hotel before leaving the hotel. This application can be implemented as a standard "electronic commerce" type application which may additionally use information collected directly from a wireless Bluetooth-enabled door lock. From his/her application on the mobile terminal the user can initiate the proper check-out mechanism, such as e.g. if additional charges shall be incurred for late check-out. The application can use standard available secrecy and privacy mechanisms such as Secure Socket Layer (SSL), Secure Electronic Transfer (SET) or similar to protect the payment information.

[0049] Now, with reference to **FIG. 5**, in yet another aspect of an embodiment of a method of the invention, the invention provides for wireless user check-out from the hotel and electronic hotel bill payment. In contrast to what was explained above with reference to **FIG. 4**, the additional aspect of the hotel check-out and electronic hotel bill payment illustrated in **FIG. 5** is the triggering of automatic check-out or generation of a payment request from the hotel reservation/IT system to the payment server after exit registration or expiration of the reservation period. If the payment is registered on or prior to the registration of exit, then the check-out is registered. If the reservation period expires and the payment is not registered on or prior to the expiration of the reservation period, then the automatic generation of the payment request can be triggered. A situation of use of the method explained above with reference to **FIGS. 4 and 5** is also illustrated in **FIG. 7**.

[0050] With reference to **FIG. 8**, examples of bearers such as the standardised UMTS, GSM, TDMA and/or CDMA which can be employed by the Wireless application for mobile terminals and associated mobile networks in a system according to the invention is shown.

[0051] Other Useful Aspects of the Invention.

[0052] Using a wireless application reservation service for flight tickets combined with the use of the Bluetooth technology, the customer will not need a flight ticket, and the Bluetooth phone could even be the 'boarding pass' letting the traveller through the boarding gate of an airport. The same principle can be used in cinemas, mueseums, concerts and other such venues requiring a pass for entering.

[0053] Adding the use of automatic mobile localising applications will enable features as 'show me the nearest hotel (corresponding to my preferences)'. It will also enable services like supplying a digital map of how, and by what means of transportation, to get to the hotel from where the traveller is—together with the room confirmation.

[0054] By using wireless devices complying with the Bluetooth technology industry standard in conjunction with house door locks, the door may e.g. be locked at all occasions, except for when someone living in the house, and whose identity in accordance with the Subscriber Identity Module (SIM) of the mobile wireless terminal has been programmed into the lock, is approaching—then the door lock unlocks automatically. For the user, there will be no need to pick up keys when carrying shopping bags or small children—the user can just walk right in, or out. Combined with a motorised door opener, a secure hands-free door opening system can be provided, to the advantage of people in general and in particular for disabled persons. In addition, such wireless locks could also be opened using Bluetooth 'keys', traditional keys and/or special Bluetooth 'key' devices with built in Bluetooth technology.

[0055] In intelligent homes the unlocking and locking of the entrance door could also be combined with an alarm, with a function telling the residensee about unlocked windows or terrace doors, or even with a function that will automatically lock all windows and terrace doors when the last residensee holding a Bluetooth equipped phone or 'key' is leaving the house.

[0056] Car door locks can be equipped with wireless locks according to the invention. With wireless locks employing Bluetooth technology, the mobile phone may also function as a starter key—with Bluetooth connection; all that's needed is to push a button on the terminal to start the engine. Without the Bluetooth connection there will be no possibility to start. Thus, this also provides increased car theft protection.

[0057] The invention, and in particular the wireless hotel search and reservation/booking, makes it possible for hotels and hotel chains to get closer to the customer and to easier build loyalties with the customers. For the travellers it means a considerable improvement in ease of finding a suitable hotel—also when visiting a city for the first time, or e.g. when the favourite hotel is fully booked.

[0058] For the hotels this is a possibility to provide value added services, and for building customer loyalty—the customer will have his/her favourite hotel or hotel chain WAP reservation address programmed into the mobile phone, knowing that upon arrival, after making a reservation through the WAP hotel room reservation service, all he/she needs to do is to walk right up to the room that's been prepared for his/her arrival. The service also opens the door for the hotel(s) to keep track of the customer's preferences and customer profile, thus making it possible for the hotel(s) to tailor services for loyal customers.

[0059] A system according to the invention can be set to terminate the function of the Bluetooth phone as a key for the hotel room door lock after the customer exits the room after payment, after the customer leaves the hotel after payment, or after a certain time of the departure day, depending on the hotel wishes. For travellers in hurry, it will even be possible to settle the bill after the departure from the hotel, by use of the WAP check out and payment service. The service may have built in functions that prevent customers from escaping from hotel bills. If the customer has not actively settled the bill the WAP check out and payment service may prompt the customer to do so after a certain hour of the check out day. If the customer has still not settled the bill after a certain, pre-set time, the bill will be automatically settled through the chosen electronic payment method.

[0060] Advantages

[0061] With the WAP hotel room reservation service the customer can be able to choose the hotel corresponding the

best to his/her requirements. The WAP hotel room reservation service may, upon or in conjunction with confirmation of the reservation, send a message to the phone, including the hotel room number. Thus, even before the arrival at the hotel, the customer may know which room he/she has been assigned, and is then able go directly to the room without having to make a check-in at the reception desk of the hotel.

[0062] When the traveller approaches the hotel room, the hotel room door lock senses, by means of the wireless Bluetooth technology, the WAP and Bluetooth enabled mobile terminal, and when a security code is implemented, the latter provided either through the WAP reservation service and stored in the mobile terminal, or from the customers unique SIM card identity, and registered with the hotel, compares it with a security code automatically programmed into the lock through the WAP hotel room reservation service, and opens the door. When unlocking the door in this way for the first time at each stay, the check-in at the hotel may be automatically registered by the hotel reservation/IT system. In this way, the customer's mobile terminal functions as a wireless unique electronic key to his/her room until checking out, and at that time the WAP check-out and payment service may be used.

[0063] When the customer is leaving the hotel he/she can settle the bill by means of a WAP check-out and payment service provided by the system. The service will make it possible for the customer to check the bill before leaving, and to approve payment of it. The payment can be done through any electronic payment method chosen in the service implementation (if more than one method is available, the customer preferably chooses the preferred method of payment at the time of reservation of the hotel).

[0064] Using this invention, a WAP and Bluetooth equipped mobile terminal, and the associated WAP services, the customer experiences an immense increase in ease and flexibility of hotel reservation and in ease of finding hotels and rooms that correspond to personal and corporate requirements. In addition the customer avoids both check in and check out queues. The customer will thus enjoy increased flexibility and ease of use when staying at hotels providing this service.

1. A system providing wireless hotel search and selection, and, for the selected hotel, room reservation/booking, check-in, room access control, check-out and payment services for hotel customers by combining wireless applications for hotel search and reservation/booking services, a wireless applications for check-out and payment services, and wireless hardware and applications for hotel door locks,

characterised in that the system comprises a plurality of appropriately adapted mobile terminals (1), each such mobile terminal including a short range wireless device (25) and a long or medium range mobile telephone and processing unit (23) operating with wireless application programs, network communication means (5), hotel search and reservation/booking server means (12), and a plurality of hotel reservation/It systems (7), wherein said mobile terminals (1), server means (12) and reservation/It systems (7) communicate by said communication network means (5), and wherein each hotel reservation/It system (7) is in communication (8) with a plurality of associated short range wireless door lock devices (9,32) capable of communicating with in-range wireless devices (25) of said mobile terminals (1).

2. The system of claim 1, characterised in that the system further comprises at least one electronic payment server (14) communicating by said communication network means (5) with one or more of said teminals (1), server means (12) and/or reservation/IT systems (7).

3. The system of claim 1 or 2, characterised in that the system further comprises additional corresponding wireless devices (16) in communication (15) with the hotel reservation/IT system (7) for providing communication with nearby ones of said appropriately adapted mobile wireless terminal (1).

4. The system of any one of the previous claims, characterised in that one or more wireless application programs of the mobile terminal are implemeted by application means selected from a group including WAP (WML/WML Script), typical Web applications (HTML/Java Script) and Java Application/Applet

5. A method providing wireless hotel search and selection, reservation/booking, check-in, room access control, check-out and/or payment services for hotel customers by means of a system combining Wireless application for search and reservation/booking service applications, a Wireless application for check-out and payment service application, and wireless hardware and applications for hotel door locks,

characterised in that the method includes the steps of a user connecting, by means of a appropriately adapted mobile terminal including a short range wireless device and a long or medium range mobile telephone and processing unit operating with wireless application programs, to a hotel search and reservation/booking server, searching for, finding and selecting a suitable hotel, sending a reservation/booking request and, optionally, information on a preferred method of payment to a connected hotel reservation/IT system, receiving by the mobile terminal a reservation/booking request confirmation including a key token, transferring the key token from the mobile telephone and processing unit to the wireless device of the mobile terminal, transmitting from the hotel reservation/IT system the key token to a wireless device of a wireless door of the reserved hotel room, and, upon arrival at the hotel of the user carrying the mobile terminal, transmitting wirelessly, by means of the wireless device of the mobile terminal, the key token to nearby wireless devices of wireless door locks, whereby, on receiving the appropriate key token, the arrival of the user is registered in the hotel reservation/IT system and the wireless door lock of the reserved room unlocks the door.

6. The method of claim 5, characterised in that the method further includes steps of encryption, whereby the key token to become a secret encrypted key.

7. The method of claim 5 or 6, characterised in that the method further includes, for user check-out from the hotel and bill settlement, the additional steps of a user, by means of wireless applications of the mobile terminal, connecting to a hotel search and reservation/booking server, and, while connected to the hotel search and reservation/booking server, communicating to the hotel reservation/IT system a check-out request, receiving therefrom bill information, sending thereto a bill acceptance, receiving from a payment server a payment authorisation request, sending thereto a

payment authorisation response, and by the hotel reservation/IT system, upon receiving receiving a payment verification, sending a key token deactivation message to the wireless door lock of the respective reserved room.

8. The method of claim 5 or **6**, characterised in that the method further includes, for user check-out from the hotel and bill settlement by means of triggering of automatic check-out or generation of a payment request from the hotel reservation/IT system to the payment server after exit registration or expiration of the reservation period, the additional steps of registrating the exit from the hotel of a user by means of the wireless device of the mobile terminal and an additional wireless device located at the hotel exit, wherein, if user payment is registered on or prior to the registration of exit, the check-out is registered, or, if the reservation period expires and user payment is not registered on or prior to the expiration of the reservation period, the hotel reservation/IT system automatically generates a payment request to a payment server is, whereupon the user receives from a payment server a payment authorisation request, sends thereto a payment authorisation response, and wherein the hotel reservation/IT system, upon receiving a payment verification from the payment server, sends a key token deactivation message to the wireless door lock of the respective reserved room.

9. The method of any one of claims **5-8**, characterised in that any short range wireless devices are compliant with the Bluetooth industry standard

10. The system of any one of claims **1-3**, characterised in that short range wireless devices **(25,16)** associated with mobile terminals **(1)** and wirelessly operable door locks **(32)** are compliant with the Bluetooth industry standard.

* * * * *

APPENDIX C

PTO/SB/59 (09-16)
Approved for use through 11/30/2021. OMB 0651-0064
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 displays a valid OMB control number.

REQUEST FOR SUPPLEMENTAL EXAMINATION TRANSMITTAL FORM

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

Attorney Docket No.: LBT0010-CON-SE

Date:

1. ☑ This is a request for supplemental examination pursuant to 37 CFR 1.610 of patent number 9,373,205 issued June 21, 2016. 37 CFR 1.610(b)(1).

2. ☑ Supplemental examination of claim(s) 1-24 is requested. 37 CFR 1.610(b)(4).

3. ☑ a. The name(s) of the patent owner(s) (**not** the patent practitioner(s)) is (are):

URBAN INTEL, INC.

☑ b. A submission by the patent owner(s) in compliance with 37 CFR 3.73(c), which establishes that the patent owner(s) has (have) the entirety of the ownership in the patent for which supplemental examination is requested, is included. 37 CFR 1.610(b)(9).

4. ☐ a. A check in the amount of $_____ is enclosed to cover the fee for processing and treating a request for supplemental examination, the fee for reexamination ordered under 35 USC 257, and the fee for processing and treating each non-patent document over 20 sheets in length (37 CFR 1.20(k)(1 - 3));

☑ b. The Director is hereby authorized to charge all applicable fees as set forth in 37 CFR 1.20(k)(1 - 3) to Deposit Account No. 504075; or

☐ c. Payment by credit card. Form PTO-2038 is attached. 37 CFR 1.610(a).

5. ☑ Any refund should be made by ☐ check or ☑ credit to Deposit Account No 504075. 37 CFR 1.26(c). If payment is made by credit card, refund must be to the credit card account.

6. ☑ A copy of the patent for which supplemental examination is requested, and a copy of any disclaimer or certificate issued for the patent are included. 37 CFR 1.610(b)(6).

7. ☐ CD-ROM or CD-R in duplicate, Computer Program (Appendix) or large table
   ☐ Landscape Table on CD

8. ☐ Nucleotide and/or Amino Acid Sequence Submission
   If applicable, items a. – c. are required.
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM (2 copies) or CD-R (2 copies); or
      ii. ☐ paper
   c. ☐ Statements verifying the identity of above copies

9. ☑ A list of no more than 12 items of information submitted as part of this request is provided in Part B of this form. Where appropriate, the list must meet the requirements of 37 CFR 1.98(b). 37 CFR 1.605(a), 1.610(b)(2).

This collection of information is required by 37 CFR 1.610. 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 0.3 hours 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.

PTO/SB/59 (09-16)
Approved for use through 11/30/2021. OMB 0651-0064
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 displays a valid OMB control number.

10. ☑ A legible copy of each item of information listed in Part B of this form, and an English language translation of all necessary and pertinent parts of each non-English language item of information are included.

Copies of items of information that form part of the discussion within the body of the request (see 37 CFR 1.605(b)), and copies of U.S. patents and patent application publications, are not required. 37 CFR 1.610(b)(7).

11. ☐ A summary of the relevant portions of each non-patent document that is over 50 pages in length (other than the request) is included. The summary includes the required citations to the particular pages containing the relevant portions. 37 CFR 1.610(b)(8).

12. ☑ A separate, detailed explanation of the relevance and manner of applying each item of information to each claim of the patent for which supplemental examination is requested, is included. 37 CFR 1.610(b)(5).

13. ☑ The below list includes all prior or concurrent post-patent Office proceedings (*ex parte* or *inter partes* reexamination, reissue, supplemental examination, post grant review, or *inter partes* review) involving the patent for which supplemental examination is being requested. 37 CFR 1.610(b)(3). An identifying number may be, e.g., a control no. or reissue application no. Any prior or concurrent post-patent Office proceedings not listed below are listed on a separate paper accompanying the request.

Type of Proceeding	Identifying Number	Filing Date
None		
None		
None		
None		

☐ See accompanying paper for a list of additional prior or concurrent post-patent Office proceedings involving the patent for which supplemental examination is requested. The paper should be a separate sheet titled "List of Prior or Concurrent Post-Patent Office Proceedings" and must provide the type, identifying number, and filing date of the post-patent Office proceeding.

14. Correspondence Address: Please recognize, or change, the correspondence address for the file of the patent for which supplemental examination is requested and for the supplemental examination proceeding to be:

☑ The address associated with Customer Number: 67050 OR

☐ Firm or Individual Name

Address

City	State	Zip

Country

Telephone	Email

15. **WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

/Kelly L. Kasha/	August 4, 2021
Authorized Signature	Date
Kelly L. Kasha	47,743
Typed/Printed Name	Registration No.

PTO/SB/59 (09-16)
Approved for use through 11/30/2021 OMB 0651-0064
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 displays a valid OMB control number.

(Also referred to as FORM PTO-XXXX)

REQUEST FOR SUPPLEMENTAL EXAMINATION TRANSMITTAL FORM
PART B – LIST OF ITEMS OF INFORMATION – Page 1

Patent number for which supplemental examination is requested 9,373,205 Issue Date June 21, 2016

All items of information (no more than 12) submitted herewith as part of this request for supplemental examination of the above-identified patent are included in the following list:

U. S. PATENT DOCUMENTS

Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	US- 20030208386	11-06-2003	Brondrup (Attachment B)	[0022], [0041] [0043], Fig. 3
	US-			
	US-			
	US-			
	US-			
	US-			
	US-			
	US-			
	US-			
	US-			
	US-			
	US-			

FOREIGN PATENT DOCUMENTS

Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[2]

[1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/59 (09-16)
Approved for use through 11/30/2021. OMB 0651-0064
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 displays a valid OMB control number.

(Also referred to as FORM PTO-XXXX)

REQUEST FOR SUPPLEMENTAL EXAMINATION TRANSMITTAL FORM
PART B – LIST OF ITEMS OF INFORMATION – Page 2

Patent number for which supplemental examination is requested _____ Issue Date _____

All items of information (no more than 12) submitted herewith as part of this request for supplemental examination of the above- identified patent are included in the following list:

OTHER DOCUMENTS

Cite No.[1]	Document Information (include, where appropriate, name of the author, title of the article, book, magazine, journal, serial, symposium, catalog, etc., publication date, page(s), volume-issue number(s), publisher, city and/or country where published. If a court document, identify the specific court, the designation (case citation or numeric designation), the title of the document, and the date submitted in court. If a declaration, include the type (e.g., 37 CFR 1.132 or 1.131), name of declarant, and the date of declaration. If an invoice or sales receipt, include the date issued and the name of the issuer (e.g., the name of the corporation or other place of business). If a discussion within the body of the request, include the pages of the request on which the discussion appears, and a description of the discussion (e.g., "discussion in request of why the claims are patentable under 35 U.S.C. 101, pages 7-11.") For all other materials, include, where appropriate, the title, author, date, and any descriptive information that would describe the document.)	T[2]

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

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.

Litigation Search Report CRU 3999

Reexamination Control No. 96/000,367

To:	CARLSON	**From:**	MANUEL SALDANA
Location:	REM04A39	**Location:**	REM04C71
Art Unit:	3992	**Phone:**	571-272-7740
Date:	04 August 2021	**E-mail:**	MANUEL.SALDANA@USPTO.GOV

Search Notes

NO LITIGATION FOUND FOR US PAT. 9,373,205

1. Performed a KeyCite Search in Westlaw, which retrieves all history on the patent including any litigation.
2. Performed a search on the patent in Lexis CourtLink for any open dockets or closed cases.
3. Performed a search in Lexis in the Federal Courts and Administrative Materials databases for any cases found.
4. Performed a search in Lexis in the IP Journal and Periodicals database for any articles on the patent.
5. Performed a search in Lexis in the news databases for any articles about the patent or any articles about litigation on this patent.

Paper No. 20210804

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

Bib Data Sheet

CONFIRMATION NO. 7090

SERIAL NUMBER	FILING OR 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
96/000,367	08/04/2021 RULE	713	3992	LBT0010-CON-SE

AIA (First Inventor to File): YES

INVENTORS

9373205, Residence Not Provided;
URBAN INTEL, INC., SEATTLE, WA;
PATENT OWNER, Residence Not Provided;

APPLICANTS

9373205, Residence Not Provided;
URBAN INTEL, INC., SEATTLE, WA;
PATENT OWNER, Residence Not Provided;

**** CONTINUING DATA **************************

This application is a SER 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/US2011/026781 03/02/2011
which claims benefit of 61/309,813 03/02/2010

**** FOREIGN APPLICATIONS *********************

Foreign Priority claimed	☐ yes ☐ no	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119 (a-d) conditions met	☐ yes ☐ no ☐ Met after Allowance				
Verified and Acknowledged	Examiner's Signature Initials				

ADDRESS
67050

TITLE

Access Control System and Method for Use by an Access Device

☐ All Fees

☐ 1.16 Fees (Filing)

FILING FEE RECEIVED 0.00	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:	❑ 1.17 Fees (Processing Ext. of time) ❑ 1.18 Fees (Issue) ❑ Other _____ ❑ Credit

Patent Assignment Abstract of Title

Total Assignments: 3

Application #: 14603434 **Filing Dt:** 01/23/2015 **Patent #:** 9373205 **Issue Dt:** 06/21/2016
PCT #: NONE **Intl Reg #:** **Publication #:** US20150134968 **Pub Dt:** 05/14/2015
Inventors: Chris Outwater, William Gibbens Redmann
Title: Access Control System and Method for Use by an Access Device

Assignment: 1

Reel/Frame: 034801 / 0482 **Received:** 01/23/2015 **Recorded:** 01/23/2015 **Mailed:** 01/26/2015 **Pages:** 10
Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).
Assignors: OUTWATER, CHRIS **Exec Dt:** 10/29/2014
REDMANN, WILLIAM GIBBENS **Exec Dt:** 01/21/2015
Assignee: LIBERTY PLUGINS, INC.
1482 EAST VALLEY ROAD, SUITE 329
SANTA BARBARA, CALIFORNIA 93108
Correspondent: JOHN KASHA
14532 DUFIEF MILL ROAD
KASHA LAW LLC
NORTH POTOMAC, MD 20878

Assignment: 2

Reel/Frame: 048942 / 0162 **Received:** 04/19/2019 **Recorded:** 04/19/2019 **Mailed:** 04/22/2019 **Pages:** 4
Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).
Assignor: LIBERTY PLUGINS, INC **Exec Dt:** 04/19/2019
Assignee: URBAN INTEL, INC.
6527 SEWARD PARK AVE S.
C/O EDWARD GOMEZ
SEATTLE, WASHINGTON 98118
Correspondent: CLIFFORD H KRAFT
320 ROBIN HILL DR.
NAPERVILLE, IL 60540

Assignment: 3

Reel/Frame: 055881 / 0376 **Received:** 03/31/2021 **Recorded:** 03/31/2021 **Mailed:** 04/12/2021 **Pages:** 6
Conveyance: CORRECTIVE ASSIGNMENT TO CORRECT THE CONVEYING NAME AND RECEIVING NAME PREVIOUSLY RECORDED AT REEL: 48942 FRAME: 162. ASSIGNOR(S) HEREBY CONFIRMS THE ASSIGNMENT.
Assignor: LIBERTY PLUGINS, INC. **Exec Dt:** 04/19/2019
Assignee: URBAN INTEL, INC.
6527 SEWARD PARK AVE S.
C/O EDWARD GOMEZ
SEATTLE, WASHINGTON 98118
Correspondent: KELLY L. KASHA
14532 DUFIEF MILL RD
KASHA LAW LLC
NORTH POTOMAC, MD 20878

Search Results as of: 07/27/2021 08:44 AM

If you have any comments or questions concerning the data displayed, contact PRD / Assignments at 571-272-3350. v.2.6
Web interface last modified: Jun 26, 2017 v.2.6

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

Patent Owner's Name and Address:

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

OC000000127503169

Patent Number: 9373205 Control Number: 96/000,367 Date Mailed: 08/06/2021

NOTICE OF SUPPLEMENTAL EXAMINATION REQUEST FILING DATE

The patent owner is hereby notified that the filing date of the request for supplemental examination is 08/04/2021, the date that a request meeting all of the applicable requirements of 37 CFR §§ 1.605, 1.610, and 1.615 was received by the Office.

A supplemental examination certificate will issue within three months from the filing date of the request for supplemental examination. See 37 CFR 1.625.

This notice is being sent to the official correspondence address of record which, in a supplemental examination proceeding, is the official correspondence address of record in the patent file. See 37 CFR 1.33.

/RBELL/

Central Reexamination Unit
(571) 272-1549, FAX NO. (571)273-9900

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.
96/000,367	08/04/2021	9373205	LBT0010-CON-SE	7090

67050 7590 08/16/2021

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

EXAMINER
CARLSON, JEFFREY D

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
08/16/2021	PAPER

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.

(12) SUPPLEMENTAL EXAMINATION CERTIFICATE

United States Patent (10) **Number: US 9,373,205 F1**
Outwater et al. (45) **Certificate Issued: Aug. 16, 2021**

Control No.: 96/000,367 **Filing Date: Aug. 4, 2021**

Primary Examiner: Jeffrey D. Carlson

A substantial new question of patentability affecting at least one claim of the patent is raised in the request for supplemental examination. See the Reasons for Substantial New Question of Patentability Determination in the file of this proceeding.Accordingly, ex parte re-examination will be ordered pursuant to 35 U.S.C 257.

(56) Items of Information

U.S. PATENT DOCUMENTS

2003/0208386 A1	11/2003	Brondrup

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.
96/000,367	08/04/2021	9373205	LBT0010-CON-SE	7090

67050 7590 08/16/2021

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

EXAMINER	
CARLSON, JEFFREY D	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
08/16/2021	PAPER

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.

REASONS FOR SUBSTANTIAL NEW QUESTION OF PATENTABILITY DETERMINATION

Notice of Pre-AIA or AIA Status

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

I. Request for Supplemental Examination

On 8/4/2021, Patent Owner filed a Corrected Request For Supplemental Examination of claims 1–24 (all claims) of US Patent 9,373,205 ("the patent"). On 8/6/2021, the Office mailed a Notice of Supplemental Examination Request Filing Date indicating that the request was granted a filing date of 8/4/2021.

II. Pertinent Prosecution History

On 1/23/2015, applicant filed claims 1–24 in application 14/603,434. Claims 1–24 were pending.

On 11/13/2015, an office action included a double patenting rejection for claims 1–24 in view of US Patent 8,996,876.

On 12/14/2015, applicant filed a response including a Terminal Disclaimer. No claims were amended. Claims 1–24 were pending.

On 2/22/2016, an office action allowed the case with claims 1–24 being

allowable.

On 1/21/2016 the case issued as US Patent 9,373,205 with the following independent claims:

1. An access device for use in an access control system, the access device comprising:

a processor (16) having control of a door lock (11); and

a communication module (17) connected to the processor, the processor able to receive a reservation certificate (5) presented by a portable terminal (4) through the communication module;

wherein the processor activates the door lock when a current reservation certificate has been presented.

13. A method for use by an access device in an access control system, the method comprising:

a) accepting, by a processor through a communication module, a reservation certificate presented with a portable terminal;

b) determining, by the processor, that the reservation certificate is current; and

c) activating, by the processor on the basis of the reservation certificate being current, a door lock.

III. Items of Information

Supplemental examination has been requested based on the items of information that are listed below:

Item #	Document	Inventor / Doc ID	Publication Date
1	US 2003/0208386	Brondrup	11/6/2003

Each of these items of information qualifies as prior art against the patent. In addition, none of these items were cited in the original prosecution for the patent.

IV. Analyzing Items of Information For Substantial New Question(s) of Patentability

Item 1 – Brondrup, presented in the request for supplemental examination, raises a substantial new question of patentability (SNQ) affecting claims 1–24.

Brondrup discloses "[w]ireless reservation, check-in, access control, check-out and payment" techniques [Brondrup at TITLE].

Brondrup in particular teaches:

"the steps of a user by means of a properly adapted wireless mobile terminal connecting to a hotel search and reservation/booking server . . . sending a reservation/booking request . . . and thereby making a reservation, receiving by the . . . mobile terminal a reservation/booking request confirmation including a key token . . . transmitting from the hotel reservation/IT system the key token to a wireless device associated with a door lock of the reserved hotel room, and, upon arrival at the hotel of the user carrying the mobile terminal, wirelessly, by means of the wireless device of the mobile terminal, transmitting the key token to nearby wireless devices associated with electrically operated door locks whereby, on

receiving the appropriate key token, the arrival of the user is registered in the hotel reservation/IT system, and the door lock wireless device of the reserved room unlocks the door" (Brondrup ¶ 0026).

"Hotel lock activated with the travelers Bluetooth/terminal identity automatically at the appropriate time in accordance with booking" (Brondrup Fig. 6).

"the invention includes, for user check-out from the hotel, the additional steps of a user, by means of the mobile terminal, connecting to a hotel search and reservation/booking server, and, while connected to the hotel search and reservation/booking server, communicating to the hotel reservation/IT system a check-out request . . . and by the hotel reservation/IT system, upon receiving [sic] a payment verification, sending a key token deactivation message to the door lock associated wireless device of the reserved room" (Brondrup ¶ 0026).

"The mobile terminal (1) comprises a mobile telephone and processing unit" (Brondrup at ABSTRACT).

Brondrup therefore teaches:

- creating a hotel room reservation,
- receiving a key token at the user's phone,
- sending the key token from the IT system to the reserved room's wireless door lock,
- a user approaching the reserved room's door,
- transmitting the key token from the phone to the reserved room's door lock
- verifying the key token as an appropriate key token
- registering the user in the IT system as having arrived
- the door lock wireless device of the reserved room unlocking the door
- upon check-out, sending a key token deactivation message to the door lock

These teachings are relevant to the limitations deemed missing from the

cited art during the prosecution of the patent namely those found in exemplary claim 13:

a) accepting, by a processor through a communication module, a reservation certificate presented with a portable terminal;

b) determining, by the processor, that the reservation certificate is current; and

c) activating, by the processor on the basis of the reservation certificate being current, a door lock.

Brondrup further teaches that the door lock is "activated" by transmitting the particular token key to the particular door lock in accordance with the booking and that upon check-out the particular door lock is "deactivated" via a key token deactivation message to the door lock. This therefore results in the door lock possessing an activated key token which represents a "current" reservation. Successfully matching a user-presented key token with a stored, active key token represents a determination that the reservation is current and the user is allowed entry accordingly.

For these reasons, the request for supplemental examination and the teachings of Brondrup establish that there is a substantial likelihood that a reasonable examiner would consider the teachings important in deciding the patentability of claims 1–24.

V. Conclusion

For the reasons above, item 1 (Brondrup) raises an SNQ for the requested claims. Therefore, at least one substantial new question of patentability (SNQ) affecting at least one claim of US Patent 9,373,205 is raised by the present request for supplemental examination. Accordingly, *ex parte* reexamination of the patent will be ordered pursuant to 35 USC § 257.

/JEFFREY D CARLSON/
Primary Examiner, Art Unit 3992

Conferees:

/J.W/
Primary Examiner, Art Unit 3992

/M.F/
Supervisory Patent Reexamination Specialist, Art Unit 3992

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.
96/000,367	08/04/2021	9373205	LBT0010-CON-SE	7090

67050 7590 08/18/2021

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

EXAMINER
CARLSON, JEFFREY D

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
08/18/2021	PAPER

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.

Ex Parte Reexamination Ordered Pursuant to 35 U.S.C. 257	**Control No.** 96/000,367	**Patent Under Reexamination** 9373205	
	Examiner Carlson	**Art Unit** 3992	**AIA (FITF) Status** No

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

The supplemental examination proceeding filed on 08/04/2021, concluded with the issuance of the supplemental examination certificate on 16 August 2021. The certificate indicated that one or more items of information submitted as part of the request for supplemental examination raises a substantial new question of patentability. See the Reasons for Substantial New Question of Patentability Determination in the file of this proceeding.

Accordingly, *ex parte* reexamination of claim(s) 1-24 of U.S. Patent No. 9,373,205 is ordered. See 35 U.S.C. 257(b) and 37 CFR 1.625(b). This *ex parte* reexamination proceeding is hereby initiated by the mailing of this order. *Ex parte* reexamination under 35 U.S.C. 257 will be conducted in accordance with 37 CFR 1.530 through 1.570, which govern *ex parte* reexamination, subject to the exceptions enumerated in 37 CFR 1.625(d), and, in addition, to the exception that a patent owner's statement, including any amendment, under 37 CFR 1.530(a)-(c) may not be filed. For this reason, no amendment in an *ex parte* reexamination proceeding ordered under 35 U.S.C. 257 may be filed until after the mailing of a first Office action on the merits.

This reexamination proceeding has been assigned to the art unit listed above. All future correspondence should be directed to the assigned art unit and should be identified by the control number listed above, which is identical to the control number assigned to the now-concluded supplemental examination proceeding.

/MICHAEL FUELLING/ Supervisory Patent Examiner, Art Unit 3992	/JDC/	/SGR/

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.
96/000,367	08/04/2021	9373205	LBT0010-CON-SE	7090

67050 7590 10/18/2021

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

EXAMINER	
CARLSON, JEFFREY D	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
10/18/2021	PAPER

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.

Office Action in Ex Parte Reexamination	**Control No.** 96/000,367	**Patent Under Reexamination** 9373205	
	Examiner JEFFREY D CARLSON	**Art Unit** 3992	**AIA (FITF) Status** No

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

a. ☐ Responsive to the communication(s) filed on _____.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

b. ☐ This action is made FINAL.

c. ☑ A statement under 37 CFR 1.530 has not been received from the patent owner.

A shortened statutory period for response to this action is set to expire 2 month(s) from the mailing date of this letter. Failure to respond within the period for response will result in termination of the proceeding and issuance of an *ex parte* reexamination certificate in accordance with this action. 37 CFR 1.550(d). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).** If the period for response specified above is less than thirty (30) days, a response within the statutory minimum of thirty (30) days will be considered timely.

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. ☑ Notice of References Cited by Examiner, PTO-892.
2. ☐ Information Disclosure Statement, PTO/SB/08.
3. ☐ Interview Summary, PTO-474.
4. ☐ _____.

Part II SUMMARY OF ACTION

1a. ☑ Claims 1-24 are subject to reexamination.
1b. ☐ Claims _____ are not subject to reexamination.
2. ☐ Claims _____ have been canceled in the present reexamination proceeding.
3. ☐ Claims _____ are patentable and/or confirmed.
4. ☑ Claims 1-24 are rejected.
5. ☐ Claims _____ are objected to.
6. ☐ The drawings, filed on _____ are acceptable.
7. ☐ The proposed drawing correction, filed on _____ has been (7a) ☐ approved (7b) ☐ disapproved.
8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the certified copies have
   1 ☐ been received.
   2 ☐ not been received.
   3 ☐ been filed in Application No. _____.
   4 ☐ been filed in reexamination Control No. _____.
   5 ☐ been received by the International Bureau in PCT application No. _____.
   * See the attached detailed Office action for a list of the certified copies not received.
9. ☐ Since the proceeding appears to be in condition for issuance of an *ex parte* reexamination certificate except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte* Quayle, 1935 C.D. 11, 453 O.G. 213.
10. ☐ Other: _____

cc: Requester (if third party requester)

EX PARTE REEXAMINATION OFFICE ACTION

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

This is a reexamination of US Patent 9,373,205. The *Ex Parte* Reexamination Order mailed 8/18/2021 indicated that a substantial new question of patentability affecting patented claims 1–24 (all claims) of the patent was raised by the request. Accordingly, claims 1–24 are pending in this reexamination.

No claim amendments have been filed.

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1–12 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

- Claim 1 is confusing in claim scope. It is an apparatus (device) claim setting forth structure, yet the claim includes what appear to be method steps (processor activates when a current reservation certificate is presented).

This step appears to represent a method of using the system rather than the structure (e.g. the processor configured to activate . . .) of the device itself.

- See MPEP 2173.05(p)(II), *In re Katz* Interactive Call Processing Patent Litigation, 639 F.3d 1303, 1318, 97 USPQ2d 1737, 1748-49 (Fed. Cir. 2011) and *IPXL Holdings v. Amazon.com, Inc.*, 430 F.3d 1377, 1384, 77 USPQ2d 1140, 1145 (Fed. Cir. 2005).

- Claims 2–12 are similarly confusing in claim scope for their apparent method steps. They likewise fail to set forth the structure present which is responsible for the carrying out the alleged method steps.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1–4, 9, 12–16, 21 and 24 are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by US 2003/0208386 (Brondrup).

1. An access device for use in an access control system, the access device comprising:

"Wireless reservation, check-in, access control, check-out and payment" (Brondrup at TITLE).

"wireless devices (9,16) of door locks (32)" (Brondrup at ABSTRACT).

a processor (16) having control of a door lock (11); and a communication module (17) connected to the processor,

"Each hotel reservation/IT system 7 has a plurality of connections 8 to a plurality of short range wireless devices 9, wherein each wireless device 9 is provided with a connection 31 to an associated door lock 32 which can be operated by the associated wireless device 9" (Brondrup ¶ 0036).

"hotel reservation/It system (7) is in communication (8) with a plurality of associated short range wireless door lock devices (9,32) capable of communicating with in-range wireless devices (25) of said mobile terminals (1)" (Brondrup claim 1).

the processor able to receive a reservation certificate (5) presented by a portable terminal (4) through the communication module;

"upon arrival at the hotel of the user carrying the mobile terminal, wirelessly, by means of the wireless device of the mobile terminal, transmitting the key token to nearby wireless devices associated with electrically operated door locks . . ." (Brondrup ¶ 0026).

wherein the processor activates the door lock when a current reservation certificate has been presented.

". . . whereby, on receiving the appropriate key token, the arrival of the user is registered in the hotel reservation/IT system, and the door lock wireless device of the reserved room unlocks the door" (Brondrup ¶ 0026).

"When the terminal (1) and the wireless door lock (9,31) are in-range, the hotel room key token is transferred from mobile terminal (1) to the wireless door lock (9,32), the door is unlocked and check-in is registered" (Brondrup at ABSTRACT).

Brondrup therefore certainly provides for this "wherein" activity/capability – the door can be opened when a current reservation is presented. Brondrup further

teaches that the door lock is activated by transmitting the particular token key to the particular door lock in accordance with the booking for check-in and that upon check-out the particular door lock is deactivated via a key token deactivation message to the door lock. This therefore results in the door lock possessing an activated key token which represents a current reservation. In as much as pertinent given the current claim scope, successfully matching a user-presented key token with a stored, active key token represents a determination that the reservation is current, that the user has checked-in and authorizes activation of the door lock so that the reservation user may unlock the door for entry as needed during the reservation duration.

"Hotel lock activated with the travelers Bluetooth/terminal identity automatically at the appropriate time in accordance with booking" (Brondrup Fig. 6).

"the invention includes, for user check-out from the hotel, the additional steps of a user, by means of the mobile terminal, connecting to a hotel search and reservation/booking server, and, while connected to the hotel search and reservation/booking server, communicating to the hotel reservation/IT system a check-out request . . . and by the hotel reservation/IT system, upon receiving [sic] a payment verification, sending a key token deactivation message to the door lock associated wireless device of the reserved room" (Brondrup ¶ 0026).

2. The access device of claim 1 wherein the processor activates the door lock for up to a predetermined duration.

See claim 1 – the reservation user is authorized and the lock is activated for unlocking the reserved room's door lock for the duration of her reservation.

3. The access device of claim 2 wherein the predetermined duration is all day.

See claim 1 – the reservation user is authorized and the lock is activated for unlocking the reserved room's door lock for the duration of her reservation, regardless of the duration, but inclusive of stays of one day / all day. The Brondrup disclosure is capable of activating the reserved room's door for a stay of one day / all day.

4. The access device of claim 1 wherein the reservation certificate comprise data representative of a duration and the processor activates the door lock for up to the duration.

"Provision of a reference number (booking token) that both serves as a receipt for accepted payment and as a key parameter in the communication protocol for door lock opening" (Brondrup ¶ 0022).

"the reservation/booking receipt from the hotel reservation system contains a key token such as e.g. a reference number which can be directly used for obtaining access to the reserved room upon arrival at the hotel" (Brondrup ¶ 0041).

"When the traveller approaches the hotel room, the hotel room door lock senses, by means of the wireless Bluetooth technology, the WAP and Bluetooth enabled mobile terminal, and when a security code is implemented, the latter provided either through the WAP reservation service and stored in the mobile terminal, or from the customers unique SIM card identity, and registered with the hotel, compares it with a security code automatically programmed into the lock through the WAP hotel room reservation service, and opens the door. When unlocking the door in this way for the first time at each stay, the check-in at the hotel may be automatically registered by the hotel reservation/IT system. In this way, the customer's mobile terminal functions as a wireless unique electronic key to his/her room until checking out" (Brondrup ¶ 0062).

Brondrup teaches communication of a reservation certificate (key token)

from the mobile device to the door lock and if the reservation certificate (key token) matches the active reservation key token stored at the door lock, then the door is unlocked. This key token is associated with the reservation for that (and only that) room and for the predetermined duration starting from the check-in date. The reservation key token is fairly described as comprising data representing a duration because the reservation it is tied to includes a duration of the reservation. Further, the key token will serve to open the specified door for only the specified reservation duration.

9. The access device of claim 1 wherein the processor verifies that the reservation certificate is genuine.

Brondrup teaches security features for the reservation token such that it is protected via encryption:

"the method can include steps of encryption, whereby the key token is encrypted to become an encrypted secret key" (Brondrup ¶ 0026).

Brondrup's encryption is necessarily followed by decryption in order to use the reservation token. Decrypting provides verification that the certificate is genuine, per the claim language of claim 7.

12. The access device of claim 1 wherein the processor has access to a server through the communication module and the processor reports to the server that door lock was activated on the basis of the reservation certificate.

"On receiving the appropriate key token from the wireless device in the mobile wireless terminal, the door lock wireless device of the reserved room can notify the associated hotel reservation/IT system of the arrival of the user for check-in, and unlocks the door" (Brondrup ¶ 0043).

13. A method for use by an access device in an access control system, the method comprising:

"Wireless reservation, check-in, access control, check-out and payment" (Brondrup at TITLE).

"A system and method for, by means of a mobile terminal, wireless hotel search and selection, reservation/booking, check-in, room access control, check-out and payment services for hotel customers is disclosed" (Brondrup at ABSTRACT).

"wireless devices (9,16) of door locks (32)" (Brondrup at ABSTRACT).

a) accepting, by a processor through a communication module, a reservation certificate presented with a portable terminal;

"Each hotel reservation/IT system 7 has a plurality of connections 8 to a plurality of short range wireless devices 9, wherein each wireless device 9 is provided with a connection 31 to an associated door lock 32 which can be operated by the associated wireless device 9" (Brondrup ¶ 0036).

"hotel reservation/It system (7) is in communication (8) with a plurality of associated short range wireless door lock devices (9,32) capable of communicating with in-range wireless devices (25) of said mobile terminals (1)" (Brondrup claim 1).

"upon arrival at the hotel of the user carrying the mobile terminal, wirelessly, by means of the wireless device of the mobile terminal, transmitting the key token to nearby wireless devices associated with electrically operated door locks . . ." (Brondrup ¶ 0026).

b) determining, by the processor, that the reservation certificate is current; and c) activating, by the processor on the basis of the reservation certificate being current, a door lock.

". . . whereby, on receiving the appropriate key token, the arrival of the user is registered in the hotel reservation/IT system, and the door lock wireless device of the reserved room unlocks the door" (Brondrup ¶ 0026).

"When the terminal (1) and the wireless door lock (9,31) are in-range, the hotel room key token is transferred from mobile terminal (1) to the wireless door lock (9,32), the door is unlocked and check-in is registered" (Brondrup at ABSTRACT).

Brondrup therefore certainly provides for this "wherein" activity/capability – the door can be opened when a current reservation is presented. Brondrup further teaches that the door lock is activated by transmitting the particular token key to the particular door lock in accordance with the booking for check-in and that upon check-out the particular door lock is deactivated via a key token deactivation message to the door lock. This therefore results in the door lock possessing an activated key token which represents a current reservation. In as much as pertinent given the current claim scope, successfully matching a user-presented key token with a stored, active key token represents a determination that the reservation is current, that the user has checked-in and authorizes activation of the door lock so that the reservation user may unlock the door for entry as needed during the reservation duration.

"Hotel lock activated with the travelers Bluetooth/terminal identity automatically at the appropriate time in accordance with booking" (Brondrup Fig. 6).

"the invention includes, for user check-out from the hotel, the additional steps of a user, by means of the mobile terminal, connecting to a hotel search and reservation/booking server, and, while connected to the hotel search and

reservation/booking server, communicating to the hotel reservation/IT system a check-out request . . . and by the hotel reservation/IT system, upon receiving [sic] a payment verification, sending a key token deactivation message to the door lock associated wireless device of the reserved room" (Brondrup ¶ 0026).

14. The method of claim 13 wherein the certificate is current for up to a predetermined duration.

See claim 13 – the reservation user is authorized and the lock is activated for unlocking the reserved room's door lock for the duration of her current reservation.

15. The method of claim 14 wherein the predetermined duration is all day.

See claim 13 – the reservation user is authorized and the lock is activated for unlocking the reserved room's door lock for the duration of her reservation, regardless of the duration, but inclusive of stays of one day / all day. The Brondrup disclosure covers activating the reserved room's door for a stay of one day / all day.

16. The method of claim 13 wherein the reservation certificate comprises data representative of a duration and the certificate is current for up to the duration.

"Provision of a reference number (booking token) that both serves as a receipt for accepted payment and as a key parameter in the communication protocol for door lock opening" (Brondrup ¶ 0022).

"the reservation/booking receipt from the hotel reservation system contains a key token such as e.g. a reference number which can be directly used for obtaining access to the reserved room upon arrival at the hotel" (Brondrup ¶ 0041).

"When the traveller approaches the hotel room, the hotel room door lock senses, by means of the wireless Bluetooth technology, the WAP and Bluetooth enabled mobile terminal, and when a security code is implemented, the latter provided either through the WAP reservation service and stored in the mobile terminal, or from the customers unique SIM card identity, and registered with the hotel, compares it with a security code automatically programmed into the lock through the WAP hotel room reservation service, and opens the door. When unlocking the door in this way for the first time at each stay, the check-in at the hotel may be automatically registered by the hotel reservation/IT system. In this way, the customer's mobile terminal functions as a wireless unique electronic key to his/her room until checking out" (Brondrup ¶ 0062).

Brondrup teaches communication of a reservation certificate (key token) from the mobile device to the door lock and if the reservation certificate (key token) matches the active reservation key token stored at the door lock, then the door is unlocked. This key token is associated with the reservation for that (and only that) room and for the predetermined duration starting from the check-in date. The reservation key token is fairly described as comprising data representing a duration because the reservation it is tied to includes a duration of the reservation. Further, the key token will serve to open the specified door for only the specified reservation duration.

21. The method of claim 13 wherein the b) determining by the processor is further that the reservation certificate is genuine, and the c) activating is on the further basis of the reservation certificate being genuine.

Brondrup teaches security features for the reservation token such that it is protected via encryption:

"the method can include steps of encryption, whereby the key token is encrypted to become an encrypted secret key" (Brondrup ¶ 0026).

Brondrup's encryption is necessarily followed by decryption in order to use the reservation token. Decrypting provides verification that the certificate is genuine, per the claim language of claim 19.

24. The method of claim 13 wherein the processor has access to a server through the communication module, the method further comprising the step of: d) reporting to the server that the door lock was activated on the basis of the reservation certificate.

"On receiving the appropriate key token from the wireless device in the mobile wireless terminal, the door lock wireless device of the reserved room can notify the associated hotel reservation/IT system of the arrival of the user for check-in, and unlocks the door" (Brondrup ¶ 0043).

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

> Patentability shall not be negatived by the manner in which the invention was made.

Claims 5, 6, 17 and 18 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Brondrup in view of WO 2005017840.

5. The access device of claim 1 wherein the processor has access to the current time, the reservation certificate comprises data representative of an interval of the reservation, and the processor activates the door lock during the interval.

Similar to that stated above for claim 4, Brondrup's reservation certificate (key token) is interpreted as comprising data representing a reservation interval because the reservation it is tied to defines an interval according to the start time/date and ending time/date of the reservation. Brondrup does not appear to teach the door lock processor having access to the current time.

WO 2005017840 also teaches electronically accessible locks at a hotel. A mobile phone stores the appropriate electronic key which can be transmitted to the room's door lock in order to open the hotel room. WO 2005017840 teaches that the electronic key can be provided with a period of validity or an expiry date in order to limit access to the room to the appropriate time interval. WO 2005017840 also teaches that the lock itself checks the expiration/validity period before allowing access.

"Another application example arises in the case of a hotel stay in which the hotel guest is to be given the opportunity for a limited period of time to be able to lock or unlock the hotel room door" (WO 2005017840 p. 032).

"the mobile control device transmits an electronic key to electronic lock in order to access the locking state thereof" (WO 2005017840 at ABSTRACT).

"The electronic lock 20 can, for example, represent the lock of a hotel room door for which a hotel guest is granted the locking authorization for the duration of his stay" (WO 2005017840 p. 036).

"The expiry of the period of validity or the reaching of the expiry time is advantageously checked by the electronic lock assigned to the transferred key in order to rule out manipulation of the other electronic control unit" (WO 2005017840 p. 031).

It would have been obvious to one of ordinary skill at the time of the invention to have communicated from the phone to the lock of Brondrup reservation data that included interval/duration validity data and to have enabled the locks of Brondrup to determine whether the user's reservation at that moment is current/active/valid by accessing a date/time clock. Doing so provides a predictable manner of determining a valid reservation by comparing the reservation interval with the current date/time and allows access only for a currently valid reservation. This represents an obvious alternative for determining valid reservation status at the time of requesting access. One of ordinary skill would recognize that the lock would require access to the current time (and day) in order to "check" the expiry of the validity period.

6. The access device of claim 5 wherein the interval is specified by a start time and one of an end time and a duration.

Given the obviousness laid out for claim 5, one of ordinary skill would have recognized either of 1) start time and end time or 2) start time and duration as two obvious and essentially equivalent and alternative ways to define, determine and discriminate the validity period of a user's hotel reservation for a door opening request.

17. The method of claim 13 wherein the processor has access to the current time and the reservation certificate comprises data representative of an interval of the reservation, and the certificate is current for up to the interval.

Similar to that stated above for claim 4, Brondrup's reservation certificate (key token) is interpreted as comprising data representing a reservation interval because the reservation it is tied to defines an interval according to the start time/date and ending time/date of the reservation. Brondrup does not appear to teach the door lock processor having access to the current time.

WO 2005017840 also teaches electronically accessible locks at a hotel. A mobile phone stores the appropriate electronic key which can be transmitted to the room's door lock in order to open the hotel room. WO 2005017840 teaches that the electronic key can be provided with a period of validity or an expiry date in order to limit access to the room to the appropriate time interval. WO 2005017840 also teaches that the lock itself checks the expiration/validity period before allowing access.

"Another application example arises in the case of a hotel stay in which the hotel guest is to be given the opportunity for a limited period of time to be able to lock or unlock the hotel room door" (WO 2005017840 p. 032).

"the mobile control device transmits an electronic key to electronic lock in order to access the locking state thereof" (WO 2005017840 at ABSTRACT).

"The electronic lock 20 can, for example, represent the lock of a hotel room door for which a hotel guest is granted the locking authorization for the duration of his stay" (WO 2005017840 p. 036).

"The expiry of the period of validity or the reaching of the expiry time is advantageously checked by the electronic lock assigned to the transferred key in order to rule out manipulation of the other electronic control unit" (WO 2005017840 p. 031).

It would have been obvious to one of ordinary skill at the time of the invention to have communicated from the phone to the lock of Brondrup reservation data that included interval/duration validity data and to have enabled the locks of Brondrup to determine whether the user's reservation at that moment is current/active/valid by accessing a date/time clock. Doing so provides a predictable manner of determining a valid reservation by comparing the reservation interval with the current date/time and allows access only for a currently valid reservation. This represents an obvious alternative for determining valid reservation status at the time of requesting access. One of ordinary skill would recognize that the lock would require access to the current time (and day) in order to "check" the expiry of the validity period.

18. The method of claim 17 wherein the interval is specified by a start time and one of an end time and a duration.

Given the obviousness laid out for claim 17, one of ordinary skill would have recognized either of 1) start time and end time or 2) start time and duration as two obvious and essentially equivalent and alternative ways to define, determine and discriminate the validity period of a user's hotel reservation for a door opening request.

Claims 7, 8, 10, 11, 19, 20, 22 and 23 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Brondrup in view of Business Data Communications[1] (Stallings).

7. The access device of claim 1 further comprising: a memory to which the processor has access, the memory containing a public key for a server authorized to issue the reservation certificate; wherein at least a portion of the reservation certificate is encrypted by the server using a private key and the processor verifies that the reservation certificate is genuine by decrypting the portion with the public key.

Brondrup teaches security features for the reservation token such that it is protected via encryption:

"the method can include steps of encryption, whereby the key token is encrypted to become an encrypted secret key" (Brondrup ¶ 0026).

Brondrup does not however describe the types of encryption employed.

[1] Stallings, et al, "Business Data Communications", second edition, Prentice Hall, 1994, pp. 583–613.

Stallings however teaches various encryption and decryption techniques in order to protect certain information and prevent unauthorized access or use of the information. In particular Stallings teaches symmetric encryption where the sender possesses a private key used to encrypt information and the recipient also has a copy of such a private key used to decrypt the information. Stallings also teaches public key (asymmetric) encryption where a public key and a private key are used for the encryption and decryption:

"Alice has a message (plaintext) she wants to send to Bob. She does not want anyone else to know what's in the message so she transforms it into an unintelligible form (ciphertext). The specific form of the ciphertext is determined by Alice's key. Alice then sends the ciphertext to Bob, who performs an inverse process, using his key to recover the plaintext. Traditionally, Alice and Bob's keys had to be the same. In the last 15 years, more general systems have been developed that allow the keys to be different. The traditional schemes are called, variously, secret key, single-key, or symmetric encryption systems. The new systems are called public-key, or asymmetric encryption, systems. Figure 14-3 illustrates both approaches" (Stallings p. 584).

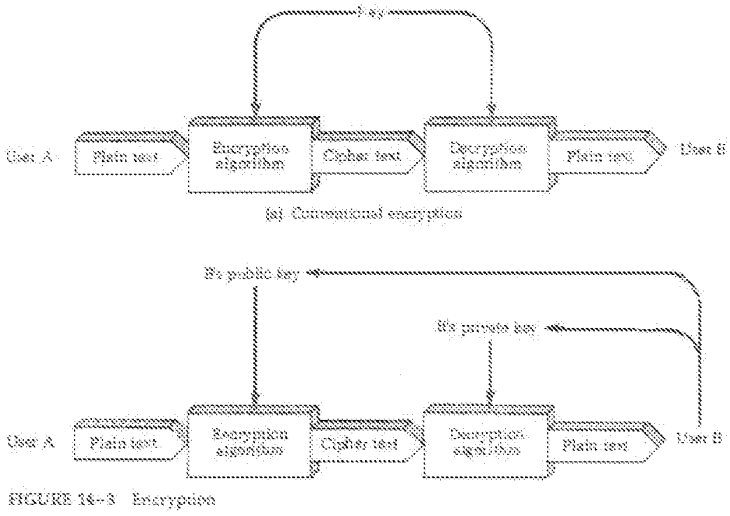


FIGURE 14-3 Encryption

[Stallings p. 585].

"For single-key encryption schemes, the keys used for encryption and decryption are the same. This is not a necessary condition. Instead, it is possible to develop an algorithm that uses one key for encryption and a companion but different key for decryption. Furthermore, it is possible to develop algorithms such that knowledge of the encryption algorithm plus the encryption key is not sufficient to determine the decryption key. Thus, the following technique will work:

1. Each end system in a network generates a pair of keys to be used for encryption and decryption of messages that it will receive.

2. Each system publishes its encryption key by placing it in a public register or file. This is the public key. The companion key is kept private.

3. If A wishes to send a message to B, it encrypts the message using B's public key.

4. When B receives the message, it decrypts it by using B's private key.

No other recipient can decrypt the message because only B knows B's private key" (Stallings p.597).

It would have been obvious to one of ordinary skill at the time of the invention to have employed any well-known encryption techniques with that of the end points of Brondrup, including symmetric, private key or asymmetric encryption using public and private keys as described by Stallings. Doing so would provide encryption security, as desired by Brondrup. Decrypting provides verification that the certificate is genuine, per the claim language.

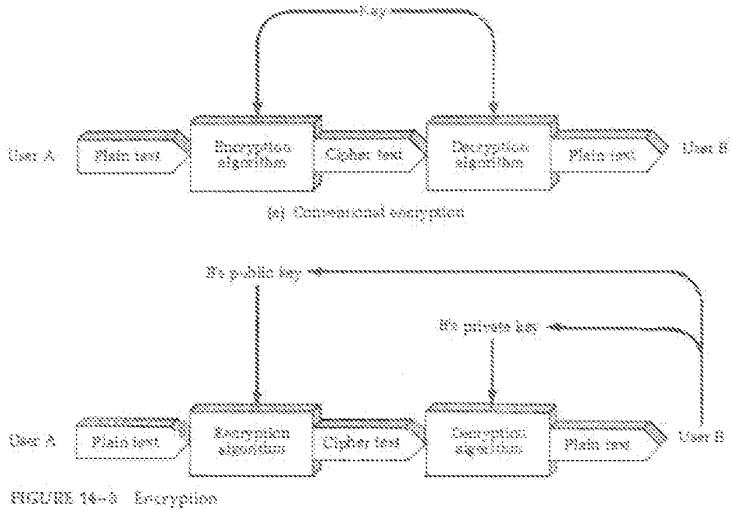
8. The access device of claim 1 further comprising: a memory to which the processor has access, the memory containing a symmetric key; wherein at least a portion of the reservation certificate is encrypted by a server using the symmetric key and the processor verifies that the reservation certificate is genuine by decrypting the portion with the symmetric key.

Brondrup teaches security features for the reservation token such that it is protected via encryption:

"the method can include steps of encryption, whereby the key token is encrypted to become an encrypted secret key" (Brondrup ¶ 0026).

Brondrup does not however describe the types of encryption employed. Stallings however teaches various encryption and decryption techniques in order to protect certain information and prevent unauthorized access or use of the information. In particular Stallings teaches symmetric encryption where the sender possesses a private key used to encrypt information and the recipient also has a copy of such a private key used to decrypt the information. Stallings also teaches public key (asymmetric) encryption where a public key and a private key are used for the encryption and decryption:

"Alice has a message (plaintext) she wants to send to Bob. She does not want anyone else to know what's in the message so she transforms it into an unintelligible form (ciphertext). The specific form of the ciphertext is determined by Alice's key. Alice then sends the ciphertext to Bob, who performs an inverse process, using his key to recover the plaintext. Traditionally, Alice and Bob's keys had to be the same. In the last 15 years, more general systems have been developed that allow the keys to be different. The traditional schemes are called, variously, secret key, single-key, or symmetric encryption systems. The new systems are called public-key, or asymmetric encryption, systems. Figure 14-3 illustrates both approaches" (Stallings p. 584).



[Stallings p. 585].

"For single-key encryption schemes, the keys used for encryption and decryption are the same. This is not a necessary condition. Instead, it is possible to develop an algorithm that uses one key for encryption and a companion but different key for decryption. Furthermore, it is possible to develop algorithms such that knowledge of the encryption algorithm plus the encryption key is not sufficient to determine the decryption key. Thus, the following technique will work:

1. Each end system in a network generates a pair of keys to be used for encryption and decryption of messages that it will receive.

2. Each system publishes its encryption key by placing it in a public register or file. This is the public key. The companion key is kept private.

3. If A wishes to send a message to B, it encrypts the message using B's public key.

4. When B receives the message, it decrypts it by using B's private key.

No other recipient can decrypt the message because only B knows B's private key" (Stallings p.597).

It would have been obvious to one of ordinary skill at the time of the invention to have employed any well-known encryption technique with that of Brondrup, including symmetric, private key or asymmetric encryption using public

and private keys as described by Stallings. Doing so would provide encryption security, as desired by Brondrup. Decrypting provides verification that the certificate is genuine, per the claim language.

10. The access device of claim 1 further comprising: an identification to which the processor has access, the identification corresponding to one of the access device and the door lock, wherein the processor determines that the reservation certificate comprises data representative of the identification.

Brondrup does not appear to teach this determination of identification information for which the lock device has access. Stallings however also teaches the known concepts of authentication and digital signatures used in combination with encryption security in order to provide further assurance of information integrity and to determine the actual sources.

"The data to be sent, together with a secret key, are used to generate a message authentication code. The data plus code are transmitted to the intended recipient. The recipient performs the same calculation on the data, using the same secret key, to generate a new message authentication code. The received code is compared to the calculated code (Figure 14-15). If we assume that only the receiver and the sender know the identity of the secret key, and if the received code matches the calculated code, then 1. The receiver is assured that the message has not been altered . . . 2. The receiver is assured that the message is from the alleged sender" (Stallings p. 607–608).

"The recipient, upon receiving the message, uses the sender's public key to recover the digest. The recipient then applies the hash function to the message to get a second digest. If this digest agrees with one recovered\ with the public key, the receiver can be assured (1) that the message is correct, and (2) that it was sent by the person corresponding to the public key" (Stallings p. 610).

It would have been obvious to one of ordinary skill at the time of the invention to have employed the foregoing techniques in order to provide further assurance of information integrity and to determine the actual sources of the information exchange.

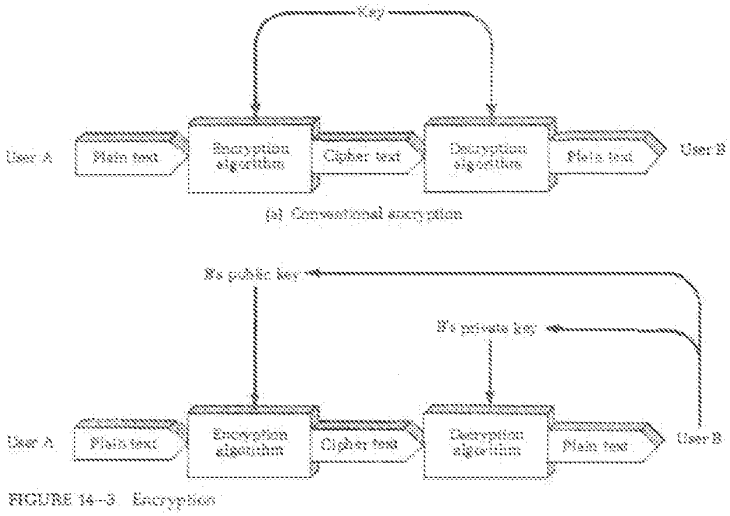
11. The access device of claim 1 further comprising: a memory to which the processor has access, the memory containing a private key of the access device; wherein at least a portion of the reservation certificate is encrypted by a server using a corresponding public key for the access device and the processor decrypts the portion with the private key.

Brondrup teaches security features for the reservation token such that it is protected via encryption:

"the method can include steps of encryption, whereby the key token is encrypted to become an encrypted secret key" (Brondrup ¶ 0026).

Brondrup does not however describe the types of encryption employed. Stallings however teaches various encryption and decryption techniques in order to protect certain information and prevent unauthorized access or use of the information. In particular Stallings teaches symmetric encryption where the sender possesses a private key used to encrypt information and the recipient also has a copy of such a private key used to decrypt the information. Stallings also teaches public key (asymmetric) encryption where a public key and a private key are used for the encryption and decryption:

"Alice has a message (plaintext) she wants to send to Bob. She does not want anyone else to know what's in the message so she transforms it into an unintelligible form (ciphertext). The specific form of the ciphertext is determined by Alice's key. Alice then sends the ciphertext to Bob, who performs an inverse process, using his key to recover the plaintext. Traditionally, Alice and Bob's keys had to be the same. In the last 15 years, more general systems have been developed that allow the keys to be different. The traditional schemes are called, variously, secret key, single-key, or symmetric encryption systems. The new systems are called public-key, or asymmetric encryption, systems. Figure 14-3 illustrates both approaches" (Stallings p. 584).



[Stallings p. 585].

"For single-key encryption schemes, the keys used for encryption and decryption are the same. This is not a necessary condition. Instead, it is possible to develop an algorithm that uses one key for encryption and a companion but different key for decryption. Furthermore, it is possible to develop algorithms such that knowledge of the encryption algorithm plus the encryption key is not sufficient to determine the decryption key. Thus, the following technique will work:

1. Each end system in a network generates a pair of keys to be used for encryption and decryption of messages that it will receive.

2. Each system publishes its encryption key by placing it in a public register or file. This is the public key. The companion key is kept private.

3. If A wishes to send a message to B, it encrypts the message using B's public key.

4. When B receives the message, it decrypts it by using B's private key.

No other recipient can decrypt the message because only B knows B's private key" (Stallings p.597).

It would have been obvious to one of ordinary skill at the time of the invention to have employed any well-known encryption technique with that of Brondrup, including symmetric, private key or asymmetric encryption using public and private keys as described by Stallings. Doing so would provide encryption security, as desired by Brondrup.

19. The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a private key for which the corresponding public key is stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the public key, and the c) activating is on the further basis of the reservation certificate being genuine.

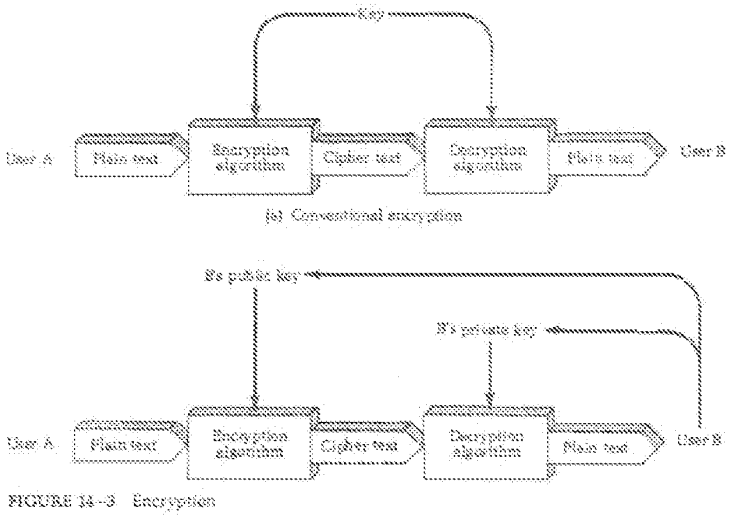
Brondrup teaches security features for the reservation token such that it is protected via encryption:

"the method can include steps of encryption, whereby the key token is encrypted to become an encrypted secret key" (Brondrup ¶ 0026).

Brondrup does not however describe the types of encryption employed. Stallings however teaches various encryption and decryption techniques in order to protect certain information and prevent unauthorized access or use of the

information. In particular Stallings teaches symmetric encryption where the sender possesses a private key used to encrypt information and the recipient also has a copy of such a private key used to decrypt the information. Stallings also teaches public key (asymmetric) encryption where a public key and a private key are used for the encryption and decryption:

"Alice has a message (plaintext) she wants to send to Bob. She does not want anyone else to know what's in the message so she transforms it into an unintelligible form (ciphertext). The specific form of the ciphertext is determined by Alice's key. Alice then sends the ciphertext to Bob, who performs an inverse process, using his key to recover the plaintext. Traditionally, Alice and Bob's keys had to be the same. In the last 15 years, more general systems have been developed that allow the keys to be different. The traditional schemes are called, variously, secret key, single-key, or symmetric encryption systems. The new systems are called public-key, or asymmetric encryption, systems. Figure 14-3 illustrates both approaches" (Stallings p. 584).



[Stallings p. 585].

"For single-key encryption schemes, the keys used for encryption and decryption are the same. This is not a necessary condition. Instead, it is possible to develop an algorithm that uses one key for encryption and a companion but different key for

decryption. Furthermore, it is possible to develop algorithms such that knowledge of the encryption algorithm plus the encryption key is not sufficient to determine the decryption key. Thus, the following technique will work:

1. Each end system in a network generates a pair of keys to be used for encryption and decryption of messages that it will receive.

2. Each system publishes its encryption key by placing it in a public register or file. This is the public key. The companion key is kept private.

3. If A wishes to send a message to B, it encrypts the message using B's public key.

4. When B receives the message, it decrypts it by using B's private key.

No other recipient can decrypt the message because only B knows B's private key" (Stallings p.597).

It would have been obvious to one of ordinary skill at the time of the invention to have employed any well-known encryption techniques with that of the end points of Brondrup, including symmetric, private key or asymmetric encryption using public and private keys as described by Stallings. Doing so would provide encryption security, as desired by Brondrup. Decrypting provides verification that the certificate is genuine, per the claim language.

20. The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a symmetric key stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the symmetric key, and the c) activating is on the further basis of the reservation certificate being genuine.

Brondrup teaches security features for the reservation token such that it is

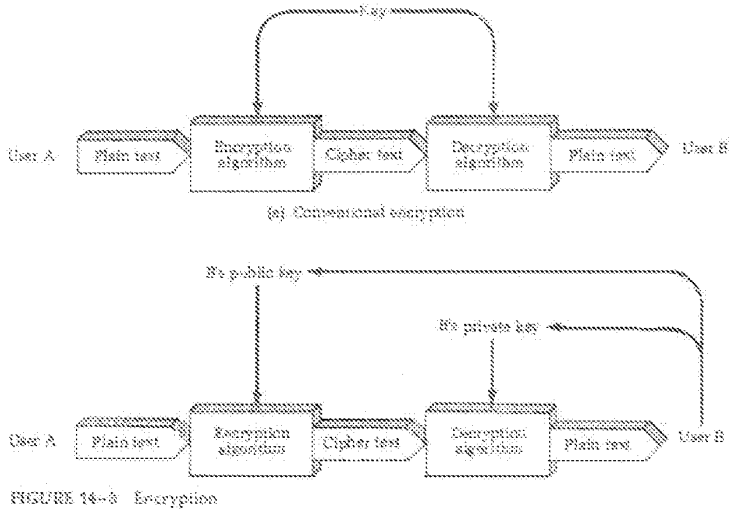
protected via encryption:

"the method can include steps of encryption, whereby the key token is encrypted to become an encrypted secret key" (Brondrup ¶ 0026).

Brondrup does not however describe the types of encryption employed.

Stallings however teaches various encryption and decryption techniques in order to protect certain information and prevent unauthorized access or use of the information. In particular Stallings teaches symmetric encryption where the sender possesses a private key used to encrypt information and the recipient also has a copy of such a private key used to decrypt the information. Stallings also teaches public key (asymmetric) encryption where a public key and a private key are used for the encryption and decryption:

"Alice has a message (plaintext) she wants to send to Bob. She does not want anyone else to know what's in the message so she transforms it into an unintelligible form (ciphertext). The specific form of the ciphertext is determined by Alice's key. Alice then sends the ciphertext to Bob, who performs an inverse process, using his key to recover the plaintext. Traditionally, Alice and Bob's keys had to be the same. In the last 15 years, more general systems have been developed that allow the keys to be different. The traditional schemes are called, variously, secret key, single-key, or symmetric encryption systems. The new systems are called public-key, or asymmetric encryption, systems. Figure 14-3 illustrates both approaches" (Stallings p. 584).



[Stallings p. 585].

"For single-key encryption schemes, the keys used for encryption and decryption are the same. This is not a necessary condition. Instead, it is possible to develop an algorithm that uses one key for encryption and a companion but different key for decryption. Furthermore, it is possible to develop algorithms such that knowledge of the encryption algorithm plus the encryption key is not sufficient to determine the decryption key. Thus, the following technique will work:

1. Each end system in a network generates a pair of keys to be used for encryption and decryption of messages that it will receive.

2. Each system publishes its encryption key by placing it in a public register or file. This is the public key. The companion key is kept private.

3. If A wishes to send a message to B, it encrypts the message using B's public key.

4. When B receives the message, it decrypts it by using B's private key.

No other recipient can decrypt the message because only B knows B's private key" (Stallings p.597).

It would have been obvious to one of ordinary skill at the time of the invention to have employed any well-known encryption techniques with that of the end points of Brondrup, including symmetric, private key or asymmetric

encryption using public and private keys as described by Stallings. Doing so would provide encryption security, as desired by Brondrup. Decrypting provides verification that the certificate is genuine, per the claim language.

22. The method of claim 13 wherein the processor has access to an identification, the identification corresponding to one of the access device and the door lock, wherein the b) determining by the processor is further that the reservation certificate comprises data representative of the identification, and the c) activating is on the further basis of the reservation certificate comprising data representative of the identification.

Brondrup does not appear to teach this determination of identification information for which the lock device has access. Stallings however also teaches the known concepts of authentication and digital signatures used in combination with encryption security in order to provide further assurance of information integrity and to determine the actual sources.

"The data to be sent, together with a secret key, are used to generate a message authentication code. The data plus code are transmitted to the intended recipient. The recipient performs the same calculation on the data, using the same secret key, to generate a new message authentication code. The received code is compared to the calculated code (Figure 14-15). If we assume that only the receiver and the sender know the identity of the secret key, and if the received code matches the calculated code, then 1. The receiver is assured that the message has not been altered . . . 2. The receiver is assured that the message is from the alleged sender" (Stallings p. 607–608).

"The recipient, upon receiving the message, uses the sender's public key to recover the digest. The recipient then applies the hash function to the message to get a second digest. If this digest agrees with one recovered\ with the public key, the

receiver can be assured (1) that the message is correct, and (2) that it was sent by the person corresponding to the public key" (Stallings p. 610).

It would have been obvious to one of ordinary skill at the time of the invention to have employed the foregoing techniques in order to provide further assurance of information integrity and to determine the actual sources of the information exchange.

23. The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a public key for which the corresponding private key is stored in a memory accessible to the processor, the method further comprising the step of: d) decrypting the portion, by the processor, with the private key.

Brondrup teaches security features for the reservation token such that it is protected via encryption:

"the method can include steps of encryption, whereby the key token is encrypted to become an encrypted secret key" (Brondrup ¶ 0026).

Brondrup does not however describe the types of encryption employed. Stallings however teaches various encryption and decryption techniques in order to protect certain information and prevent unauthorized access or use of the information. In particular Stallings teaches symmetric encryption where the sender possesses a private key used to encrypt information and the recipient also has a copy of such a private key used to decrypt the information. Stallings also teaches public key (asymmetric) encryption where a public key and a private key are used

for the encryption and decryption:

"Alice has a message (plaintext) she wants to send to Bob. She does not want anyone else to know what's in the message so she transforms it into an unintelligible form (ciphertext). The specific form of the ciphertext is determined by Alice's key. Alice then sends the ciphertext to Bob, who performs an inverse process, using his key to recover the plaintext. Traditionally, Alice and Bob's keys had to be the same. In the last 15 years, more general systems have been developed that allow the keys to be different. The traditional schemes are called, variously, secret key, single-key, or symmetric encryption systems. The new systems are called public-key, or asymmetric encryption, systems. Figure 14-3 illustrates both approaches" (Stallings p. 584).

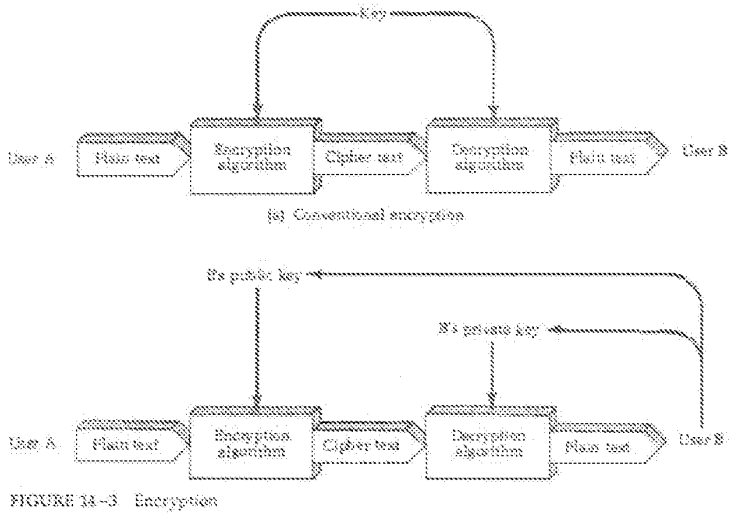


FIGURE 14-3 Encryption

[Stallings p. 585].

"For single-key encryption schemes, the keys used for encryption and decryption are the same. This is not a necessary condition. Instead, it is possible to develop an algorithm that uses one key for encryption and a companion but different key for decryption. Furthermore, it is possible to develop algorithms such that knowledge of the encryption algorithm plus the encryption key is not sufficient to determine the decryption key. Thus, the following technique will work:

1. Each end system in a network generates a pair of keys to be used for encryption and decryption of messages that it will receive.

2. Each system publishes its encryption key by placing it in a public register or file. This is the public key. The companion key is kept private.

3. If A wishes to send a message to B, it encrypts the message using B's public key.

4. When B receives the message, it decrypts it by using B's private key.

No other recipient can decrypt the message because only B knows B's private key" (Stallings p.597).

It would have been obvious to one of ordinary skill at the time of the invention to have employed any well-known encryption techniques with that of the end points of Brondrup, including symmetric, private key or asymmetric encryption using public and private keys as described by Stallings. Doing so would provide encryption security, as desired by Brondrup.

Conclusion

In order to ensure full consideration of any amendments, affidavits or declarations, or other documents as evidence of patentability, such documents must be submitted in response to this Office action. Submissions after the next Office action, which is intended to be a final action, will be governed by the requirements of 37 CFR 1.116, after final rejection and 37 CFR 41.33 after appeal, which will be strictly enforced.

Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant"

and not to parties in a reexamination proceeding. Additionally, 35 U.S.C. 305 requires that reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.550(a)). Extension of time in *ex parte* reexamination proceedings are provided for in 37 CFR 1.550(c).

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the Patent throughout the course of this reexamination proceeding. The third party requester (if any) is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

All correspondence relating to this ex parte reexamination proceeding should be directed:

By Mail to: Mail Stop *Ex Parte* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building

401 Dulany Street
Alexandria, VA 22314

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at:

https://efs.uspto.gov/efile/myportal/efs-registered

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Any inquiry concerning this communication should be directed to **the Central Reexamination Unit** at telephone number **517-272-7705.**

/JEFFREY D CARLSON/
Primary Examiner, Art Unit 3992

Conferees:
/SAMUEL G RIMELL/
Primary Examiner, Art Unit 3992
/M.F/
Supervisory Patent Examiner, Art Unit 3992

Notice of References Cited	Application/Control No. 96/000,367	Applicant(s)/Patent Under Reexamination 9373205	
	Examiner JEFFREY D CARLSON	Art Unit 3992	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-20030208386-A1	11-2003	Brondrup, Rayner	G07C9/00904	705/5
	B					
	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	WO-2005017840-A1	02-2005	WO	RANKL WOLFGANG	G07C9/00309
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Stallings, et al, "Business Data Communications", second edition, Prentice Hall, 1994, pp. 583–613. (Year: 1994)
	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.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	96/000,367	9373205
	Examiner	Art Unit
	JEFFREY D CARLSON	3992

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* 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
PE2E search - see attached	10/14/2021	jdc

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

/JEFFREY D CARLSON/ Primary Examiner, Art Unit 3992	

Reexamination	Application/Control No.	Applicant(s)/Patent Under Reexamination
	96/000,367	9373205
	Certificate Date	Certificate Number

Requester Correspondence Address: ☑ Patent Owner ☐ Third Party
KASHA LAW LLC 14532 Dufief Mill Road North Potomac, MD 20878

LITIGATION REVIEW ☑	jdc (examiner initials)	(date)
Case Name		Director Initials
1:18cv3627		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER
none	

/JEFFREY D CARLSON/ Primary Examiner, Art Unit 3992	

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
24. Februar 2005 (24.02.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/017840 A1

(51) Internationale Patentklassifikation[7]: G07C 9/00

(21) Internationales Aktenzeichen: PCT/EP2004/008815

(22) Internationales Anmeldedatum:
6. August 2004 (06.08.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 36 567.2 8. August 2003 (08.08.2003) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **RANKL, Wolfgang** [DE/DE]; Frauenalplweg 2b, 81825 München (DE).

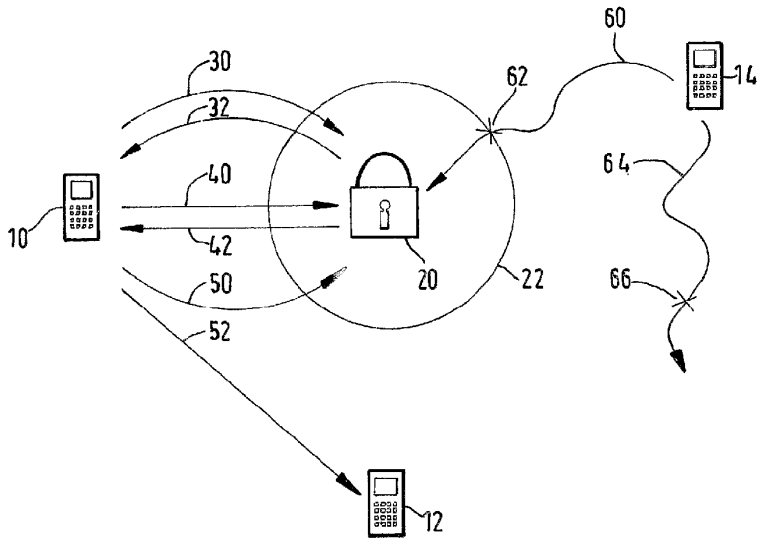
(74) Anwalt: **KLUNKER SCHMITT-NILSON HIRSCH**; Winzererstrasse 106, 80797 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: 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.

[Fortsetzung auf der nächsten Seite]

(54) **Title:** METHOD AND DEVICE FOR CONTACTLESSLY CONTROLLING THE LOCKING STATE OF AN ELECTRONIC LOCK

(54) **Bezeichnung:** VERFAHREN UND VORRICHTUNG ZUR KONTAKTLOSEN STEUERUNG DES SCHLIESSZUSTANDS EINES ELEKTRONISCHEN SCHLOSSES



(57) **Abstract:** The invention relates to a method for contactlessly controlling the locking state of an electronic lock with a mobile control device by a user, during which a bi-directional communications link is established between the mobile control device and the electronic lock. An authentication for verifying the identity and authenticity of the mobile control device and/or of the electronic lock is carried out via said communications link, and the mobile control device transmits an electronic key to electronic lock in order to access the locking state thereof.

[Fortsetzung auf der nächsten Seite]

WO 2005/017840 A1

WO 2005/017840 A1

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, 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).

Veröffentlicht:
— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur kontaktlosen Steuerung des Schliesszustands eines elektronischen Schlosses mit einer mobilen Steuereinrichtung durch einen Benutzer, bei dem zwischen der mobilen Steuereinrichtung und dem elektronischen Schloss eine bidirektionale Kommunikationsverbindung hergestellt wird, über die Kommunikationsverbindung eine Authentisierung zur Überprüfung der Identität und Auathentizität der mobilen Steuereinrichtung und/oder des elektronischen Schlosses durchgeführt wird, und die mobile Steuereinrichtung zum Zugriff auf den Schliesszustand des elektronischen Schlosses diesem einen elektronischen Schlüssel übermittelt.

Verfahren und Vorrichtung zur kontaktlosen Steuerung des Schließzustands eines elektronischen Schlosses

Die Erfindung betrifft ein Verfahren zur kontaktlosen Steuerung des Schließzustands eines elektronischen Schlosses. Die Erfindung betrifft ferner eine mobile Steuereinrichtung und eine Schlüssel-Schloss-Anordnung zur Durchführung eines derartigen Verfahrens.

Heutige Mobiltelefone haben neben den primären Funktionen wie Kommunikation und Datenspeicherung nur wenige Funktionalitäten, die sich im täglichen Leben einsetzen lassen. Aktuelle Erweiterungen, wie etwa MP3-Player, eine eingebaute Digitalkamera oder standortbezogene Dienste wie beispielsweise GPS (Global Positioning System) zeigen die Entwicklungstendenzen hin zu vielfältigeren Einsatzgebieten von Mobiltelefonen an.

Davon ausgehend liegt der Erfindung die Aufgabe zugrunde, dem Benutzer eines Mobiltelefons zusätzliche Anwendungsmöglichkeiten im Bereich des täglichen Lebens zu öffnen.

Diese Aufgabe wird durch das Verfahren zur kontaktlosen Steuerung des Schließzustands eines elektronischen Schlosses mit den Merkmalen des Hauptanspruchs gelöst. Eine mobile Steuereinrichtung und eine Schlüssel-Schloss-Anordnung zur Durchführung eines derartigen Verfahrens sind Gegenstand der nebengeordneten Ansprüche 20 und 22. Weiterbildungen der Erfindung sind Gegenstand der Unteransprüche.

Gemäß der Erfindung erfolgt die kontaktlose Steuerung durch einen Benutzer mit einer mobilen Steuereinrichtung. Zwischen der mobilen Steuerein-

richtung und dem elektronischen Schloss wird dabei eine bidirektionale Kommunikationsverbindung hergestellt und über die Kommunikationsverbindung eine Authentisierung zur Überprüfung der Identität und Authentizität der mobilen Steuereinrichtung und/oder des elektronischen Schlosses durchgeführt. Zum Zugriff auf den Schließzustand des elektronischen Schlosses übermittelt die mobile Steuereinrichtung diesem einen elektronischen Schlüssel.

Die Erfindung ermöglicht, der Funktionalität von mobilen Steuergeräten wie etwa Mobiltelefonen um die Funktion eines Schlüsselbretts für elektronische Schlösser zu erweitern. Das Mobiltelefon stellt gerade im Bereich Schlüssel-Schloss ein ideales Medium dar, da es in der Regel immer mitgeführt wird und durch ein enthaltenes Sicherheitsmodul auch eine deutlich höher Sicherheit als mit bisherigen Schlössern zu erreichen ist.

In einer vorteilhaften Ausgestaltung des erfindungsgemäßen Verfahrens wird die Kommunikationsverbindung in einem Mobilfunknetz wie GSM (Global System for Mobile communications) oder UMTS (Universal Mobile Telecommunication System), insbesondere mit einem paketorientierten Trägerdienst, wie beispielsweise GPRS (General Packet Radio Service) hergestellt. Nach einer weiteren vorteilhaften Ausgestaltung wird die Kommunikationsverbindung in einem in der mobilen Steuereinrichtung integrierten Nahbereichskanal wie der IrDA (Infrared Data Association) Schnittstelle, Bluetooth oder WLAN (Wireless Local Area Network) hergestellt.

Für die Kommunikationsverbindung können auch mehrere verschiedene Übertragungskanäle zur Verfügung stehen. Vor dem Aufbau einer Verbindung wird dann ein geeigneter Übertragungskanal für die Kommunikationsverbindung etwa durch automatisches Probieren oder durch Inanspruch-

nahme eines standortbezogenen Dienstes ausgewählt. Typischerweise wird der kostengünstigste der zur Verfügung stehenden Kanäle für den Aufbau der Kommunikationsverbindung gewählt. Es können jedoch auch andere Kriterien, etwa die Qualität oder die Sicherheit einer Verbindung als Auswahlkriterium herangezogen werden.

Vor dem Zugriff auf den Schließzustand des elektronischen Schlosses wird bevorzugt die Berechtigung des Benutzers durch Übergabe eines Geheimnisses, wie einer PIN-Nummer, oder durch Prüfung eines biometrischen Merkmals, wie etwa von Sprachmerkmalen des Benutzers geprüft. Durch die eindeutige Identifizierung des Benutzers wird das Risiko, das durch eine verloren gegangene oder gestohlene Steuereinheit entsteht, deutlich reduziert.

In einer bevorzugten Weiterbildung des Verfahrens kann die mobile Steuereinrichtung eine Mehrzahl elektronischer Schlüssel für verschiedene zugehörige elektronische Schlösser enthalten. Die Steuereinrichtung dient dann als elektronisches Schlüsselbrett, das eine Vielzahl elektronischer Schlüssel verwalten und einsetzen kann.

Die Mehrzahl elektronischer Schlüssel enthält nach einer zweckmäßigen Ausgestaltung der Erfindung sicherheitskritische und sicherheitsunkritische Schlüssel. Vor dem Zugriff auf den Schließzustand eines elektronischen Schlosses mit einem zugeordneten sicherheitskritischen Schlüssel wird die Berechtigung des Benutzers durch Übergabe eines Geheimnisses oder durch Prüfung eines biometrischen Merkmals geprüft. Es ist auch denkbar, verschieden aufwendige Sicherheitsmaßnahmen für den Einsatz sicherheitskritischer und -unkritischer Schlüssel vorzusehen oder eine Einteilung der Schlüssel in mehr als zwei Sicherheitskategorien vorzunehmen.

Mit Vorteil stellt die mobile Steuereinrichtung dem Benutzer aus der Mehrzahl elektronischer Schlüssel eine Teilmenge nutzbarer Schlüssel zum Öffnen und/oder Schließen der zugehörigen Schlösser zur Verfügung. Insbesondere kann die Auswahl der Teilmenge auf Grundlage der Ortskoordinaten der mobilen Steuereinrichtung und der elektronischen Schlösser erfolgen.

Beispielsweise können dem Benutzer nur solche Schlüssel angezeigt werden, deren zugehörige Schlösser sich innerhalb eines vorgewählten Umgebungsbereichs der mobilen Steuereinrichtung befinden. Dadurch werden zum einen unerwünschte Fehlbedienungen vermieden, wie etwa ein unbeabsichtigtes Öffnen des heimischen Haustürschlosses, während der Benutzer sich weit entfernt im Urlaub befindet. Zum anderen wird die Bedienung des mobilen Steuergeräts, gerade bei einer Vielzahl verfügbarer Schlüssel deutlich vereinfacht, da nur noch diejenigen Schlüssel angezeigt werden, deren Benutzung am momentanen Ort sinnvoll möglich ist. Andernfalls würde, gerade bei großflächigem Einsatz des Schlüssel-Schloss-Verfahrens die Benutzerfreundlichkeit durch eine große Anzahl von Auf- und Zusperrmöglichkeiten leiden.

Die mobile Steuereinrichtung kann einen elektronischen Schlüssel auch an eine andere mobile Steuereinrichtung übergeben. Dazu wird eine Authentisierung zur Überprüfung der Identität und Authentizität der anderen mobilen Steuereinrichtung und/oder des Benutzers der anderen mobilen Steuereinrichtung durchgeführt. Im Gutfall wird eine elektronische Kopie des Schlüssels der anderen mobilen Steuereinrichtung, vorzugsweise in elektronischer Form über eine Luftschnittstelle übergeben. Das elektronische Schlüsselbrett beinhaltet damit die Möglichkeit, Schließberechtigungen autorisiert weiterzugeben.

Der übergebene Schlüssel wird in einer zweckmäßigen Ausgestaltung mit einer Gültigkeitsdauer oder einem Verfallszeitpunkt versehen. Der Ablauf der Gültigkeitsdauer oder das Erreichen des Verfallszeitpunkts wird mit Vorteil durch das dem übergebenen Schlüssel zugeordnete elektronische Schloss geprüft, um Manipulationen der anderen elektronischen Steuereinheit auszuschließen. Bestimmte Schlüssel können von der Weitergabe ausgeschlossen werden, um das Risiko unbefugter Benutzung der Schlüssel zu minimieren. Ebenso kann vorgesehen sein, dass weitergegebene Schlüssel nicht erneut weitergegeben werden können.

Beispielsweise können Schlüssel innerhalb einer Familie, etwa an Kinder, autorisiert weitergegeben werden. Eine Weitergabe durch die Kinder an Dritte kann dabei ausgeschlossen werden. Ein anderes Anwendungsbeispiel ergibt sich bei einem Hotelaufenthalt, bei dem dem Hotelgast zeitlich befristet die Möglichkeit gegeben werden soll, die Hotelzimmertür oder eine Tiefgarage auf- oder absperren zu können.

Gemäß einer vorteilhaften Weiterbildung kann ein elektronischer Schlüssel vorgespannt werden, um das zugeordnete elektronische Schloss automatisch oder auf eine einfache Benutzerbestätigung hin zu öffnen, wenn die mobile Steuereinrichtung in einen vorbestimmten Umgebungsbereich des Schlosses gelangt. Dabei wird vor dem Vorspannen eines Schlüssels bevorzugt die Berechtigung des Benutzers durch Übergabe eines Geheimnisses oder durch Prüfung eines biometrischen Merkmals geprüft. Das Vorspannen eines Schlüssels wird zweckmäßig mit einer Gültigkeitsdauer oder einem Verfallszeitpunkt versehen, um zu verhindern, dass ein vorgespannter Schlüssel das zugeordnete elektronische Schloss unbeabsichtigt öffnet.

Nach einer weiteren zweckmäßigen Verfahrensmöglichkeit wird der Schließzustand des elektronischen Schlosses von der mobilen Steuereinrichtung über die Kommunikationsverbindung abgefragt. Ein vergesslicher Benutzer kann sich somit über eine Fernabfrage des versperrten Zustands eines elektronischen Schlosses versichern und sich den bisher oft erforderlichen, teilweise erheblichen Zeitaufwand zur nachträglichen Prüfung des Schließzustands ersparen.

In einer weiteren vorteilhaften Ausgestaltung kann über die Kommunikationsverbindung eine Ortsinformation des elektronischen Schlosses von der mobilen Steuereinrichtung abgefragt werden. Insbesondere können die Ortskoordinaten des Schlosses abgefragt werden und/oder die Information, ob sich das Schloss noch am Ort des letzten Verschließens befindet. Es versteht sich, dass diese Möglichkeit vor allem bei mobil angebrachten Schlössern, etwa an einem Kraftfahrzeug zum Einsatz kommt. Die Ortskoordinaten des Schlosses können von diesem beispielsweise über die von einem Mobilfunksystem gelieferten Ortsinformationen oder über GPS oder einen vergleichbaren Dienst ermittelt werden.

Die mobile Steuereinrichtung wird vorteilhaft durch ein Mobiltelefon oder eine mobile Recheneinheit, etwa einen so genannten digitalen Assistenten (PDA) mit Mobilfunkerweiterung gebildet.

Aus Sicherheitsgründen sind die Steuerungsfunktionen für das elektronische Schloss bevorzugt in einem Sicherheitsmodul, wie einem SIM (Subscriber Identity Module), einem USIM (Universal Subscriber Identity Module) oder einem R-UIM (Removeable User Identity Module) verwirklicht. Alternativ können sich die Steuerungsfunktionen auch als Programm auf der mobilen Steuereinrichtung befinden, beispielsweise als J2ME (Java 2 Micro Edition)-

Applet in einem JAVA-fähigen Mobiltelefon. In diesem Fall werden zweckmäßig zur Absicherung der Daten auf der Luftschnittstelle aus dem Chipkartenbereich bekannte Sicherheitsmechanismen wie beispielsweise Signatur- und Verschlüsselungsfunktionen der WIM (Wireless Application Protocol Identity Module) eingesetzt.

Die Authentisierung zur Überprüfung der Identität und Authentizität einer mobilen Steuereinrichtung und/oder eines Schlosses wird bevorzugt nach einem Challenge-Response-Verfahren durchgeführt. Dabei ist ein geheimer Schlüssel eines Kryptoalgorithmus das gemeinsame Geheimnis der mobilen Steuereinrichtung und des elektronischen Schlosses. Einer der Kommunikationspartner sendet dem anderen eine Zufallszahl, die diese mit dem Kryptoalgorithmus verschlüsselt und an den Fragesteller zurücksendet. Wendet der Fragesteller die Umkehrfunktion des Kryptoalgorithmus auf die erhaltene Zahl an und vergleicht das Ergebnis mit der ursprünglich gesendeten Zufallszahl, kann er bei Übereinstimmung darauf schließen, dass der andere Teilnehmer den geheimen Schlüssel kennt und somit authentisch ist. Je nach der nachfolgend vorgesehenen Funktion können dabei eine einseitige oder eine gegenseitige Authentisierung durchgeführt werden.

Die Erfindung enthält auch eine mobile Steuereinrichtung, die zur Durchführung des beschriebenen Verfahrens ausgelegt und eingerichtet ist. Insbesondere ist die mobile Steuereinrichtung durch ein Mobiltelefon oder eine mobile Recheneinheit mit Mobilfunkerweiterung gebildet.

Ferner umfasst die Erfindung eine Schlüssel-Schloss-Anordnung mit einer mobilen Steuereinrichtung und einem oder mehreren elektronischen Schlössern, die zur Durchführung des beschriebenen Verfahrens ausgelegt und eingerichtet sind. Auch dabei ist die mobile Steuereinrichtung mit Vorteil

durch ein Mobiltelefon oder eine mobile Recheneinheit mit Mobilfunkerweiterung gebildet.

Ein Ausführungsbeispiel sowie Vorteile der Erfindung werden nachfolgend anhand der Figur erläutert. Die einzige Figur zeigt in einer schematischen Darstellung mögliche Benutzungsfälle eines in einem Mobiltelefon integrierten elektronischen Schlüsselbretts nach einem Ausführungsbeispiel der Erfindung.

Die Mobiltelefone 10, 12 und 14 enthalten neben den herkömmlichen Funktionalitäten jeweils ein elektronisches Schlüsselbrett mit einer Mehrzahl elektronischer Schlüssel. Das elektronische Schloss 20 steht beispielhaft für die den Schlüsseln zugeordneten elektronischen Schlösser. Die nachfolgend beschriebenen Funktionen des Schlüsselbretts sind jeweils in einer sicheren Umgebung der Mobiltelefone 10, 12, 14, wie beispielsweise einem SIM, realisiert.

Zur Steuerung des Schließzustands des Schlosses 20 baut das Mobiltelefon 10 eine bidirektionale Kommunikationsverbindung zu dem elektronischen Schloss 20 auf, im Ausführungsbeispiel unter Verwendung des paketorientierten GPRS Datendienstes. Da die ausgetauschten Datenmengen sehr gering sind (nur wenige Bytes), sind die Kosten für die Kommunikation zwischen dem Mobiltelefon 10 und dem Schloss 20 vernachlässigbar.

Durch die bidirektionale Kommunikationsverbindung können ohne großen Aufwand übliche Authentisierungsverfahren, wie beispielsweise Challenge-Response zwischen dem Mobiltelefon 10 und dem Schloss 20 durchgeführt werden. Je nach nachfolgenden Funktionen werden eine einseitige oder eine gegenseitige Authentisierung eingesetzt.

Ein erster Benutzungsfall besteht in der Abfrage des Schließzustands des Schlosses 20. Das Mobiltelefon 10 sendet dazu eine entsprechende Anfrage 30 an das Schloss 20. Bei erfolgreicher Authentisierung des abfragenden Mobiltelefons 10 gibt das Schloss 20 eine Schließzustandsinformation 32 zurück, also die Information, ob das Schloss offen oder versperrt ist. Die Information wird dann auf dem Display des Mobiltelefons 10 für den Benutzer angezeigt.

In einem zweiten Benutzungsfall fragt das Mobiltelefon 10 über eine entsprechende Anfrage 40 den Aufenthaltsort des Schlosses 20 ab. Diese Abfrage kann insbesondere bei mobilen Schlössern, etwa dem Türschloss eines Kraftfahrzeugs sinnvoll eingesetzt werden. Das Schloss 20 kann als Antwort 42 die Ortskoordinaten des Schlosses zurückgeben, oder, falls gewünscht, lediglich die Information zurückgeben, ob sich das Schloss 20 noch am Ort des letzten Zusperrens befindet. Seine Ortskoordinaten ermittelt das Schloss 20 beispielsweise über die Ortsinformation des Mobilfunksystems oder über GPS.

Die Weitergabe der Schließberechtigung für das Schloss 20 an ein anderes Mobiltelefon 12 ist als dritter Benutzungsfall illustriert. Dazu wird nach vorheriger Identifizierung und/oder Authentisierung des anderen Mobiltelefons 12 eine elektronische Kopie des Schlüssels angefertigt und dem anderen Mobiltelefon 12 in elektronischer Form 52 über die Luftschnittstelle übertragen. Der kopierte Schlüssel wird mit einem Verfallsdatum versehen, das dem Schloss 20 vom ersten Mobiltelefon 10 mitgeteilt wird (Bezugszeichen 50). Bei einem Zugriffsversuch durch das andere Mobiltelefon 12 prüft das Schloss 20 dann zunächst, ob der kopierte Schlüssel 52 noch gültig ist.

Das elektronische Schloss 20 kann beispielsweise das Schloss einer Hotelzimmertür darstellen, für das einem Hotelgast für die Dauer seines Aufenthalts die Schließberechtigung übertragen wird.

Die drei geschilderten Benutzungsfälle erfordern beispielsweise bei einem GSM oder UMTS Netz jeweils eine kostenpflichtige Verbindung, da Daten übertragen werden müssen.

Das Vorspannen eines elektronischen Schlüssels für das Schloss 20 ist für ein weiteres Mobiltelefon 14 illustriert. Das Vorspannen des Schlüssels führt dazu, dass das zugeordnete Schloss 20 automatisch geöffnet wird, sobald das Mobiltelefon 14 durch eine räumliche Bewegung 60 in einen vorbestimmten Umgebungsbereich 22 des Schlosses 20 gelangt. Im Ausführungsbeispiel ist dies am Punkt 62 der Fall. Alternativ kann am Punkt 62 automatisch eine Öffnungsfrage wie "Schloss öffnen?" auf dem Display des Mobiltelefons 14 erscheinen und das Schloss 20 auf eine einfache Bestätigung hin geöffnet werden.

Der vorgespannte Zustand eines Schlüssels ist im Ausführungsbeispiel mit einer Gültigkeitsdauer versehen, nach deren Ablauf die Vorspannung des Schlüssels aufgehoben wird. Dies in beim Bewegungspfad 64 illustriert, der das Mobiltelefon 14 bis zum Ablauf der Gültigkeitsdauer nie in den Umgebungsbereich 22 des Schlosses 20 bringt. Bei Ablauf der Gültigkeitsdauer im Punkt 66 erlischt der Vorspannungszustand des Schlüssels, eine nachfolgendes Betreten des Umgebungsbereichs 22 bewirkt dann keine automatische Aktion.

Das Schlüsselbrett des Mobiltelefons 10 enthält typischerweise mehrere Schlüssel, deren Eigenschaften im Ausführungsbeispiel in Form einer Tabelle

in einem Speicher des Mobiltelefons 10 abgelegt sind. Die ersten beiden Einträge dieser Tabelle können etwa die in Tabelle 1 gezeigte Form und Inhalt haben.

Tabelle 1:

Schloss-ID	1234	9876
Verbindungsart	GSM	WLAN
Authentisierung gegenüber Schloss	MSISDN des Mobil-telefons	Challenge-Response, gegenseitig
Identifizierung des Benutzers	keine	Sprache
Ortsfunktion Schloss	stationär	mobil, Koordinaten werden beim Zuschließen gespeichert
Funktionen Schloss	Auf, Zu, Abfrage Schließzustand	Auf, Zu, Abfrage Schließzustand, Abtrage Schlossort
Weitergabe Schließberechtigung	erlaubt	nicht erlaubt

Patentansprüche

1. Verfahren zur kontaktlosen Steuerung des Schließzustands eines elektronischen Schlosses mit einer mobilen Steuereinrichtung durch einen Benutzer, bei dem zwischen der mobilen Steuereinrichtung und dem elektronischen Schloss eine bidirektionale Kommunikationsverbindung hergestellt wird, über die Kommunikationsverbindung eine Authentisierung zur Überprüfung der Identität und Authentizität der mobilen Steuereinrichtung und/oder des elektronischen Schlosses durchgeführt wird, und die mobile Steuereinrichtung zum Zugriff auf den Schließzustand des elektronischen Schlosses diesem einen elektronischen Schlüssel übermittelt.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** die Kommunikationsverbindung in einem Mobilfunknetz wie GSM oder UMTS, insbesondere mit einem paketorientierten Trägerdienst, wie beispielsweise GPRS hergestellt wird.

3. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** die Kommunikationsverbindung in einem in der mobilen Steuereinrichtung integrierten Nahbereichskanal wie der IrDA-Schnittstelle , Bluetooth oder WLAN hergestellt wird.

4. Verfahren nach wenigstens einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** für die Kommunikationsverbindung mehrere verschiedene Übertragungskanäle zur Verfügung stehen und vor dem Aufbau der Kommunikationsverbindung ein geeigneter Übertragungskanal für die Kommunikationsverbindung ausgewählt wird, insbesondere dass der geeig-

nete Übertragungskanal durch automatisches Probieren oder durch Inanspruchnahme eines standortbezogenen Dienstes ausgewählt wird.

5. Verfahren nach wenigstens einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, dass** vor dem Zugriff auf den Schließzustand des elektronischen Schlosses die Berechtigung des Benutzers durch Übergabe eines Geheimnisses, wie einer PIN-Nummer, oder durch Prüfung eines biometrischen Merkmals geprüft wird.

6. Verfahren nach wenigstens einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, dass** die mobile Steuereinrichtung eine Mehrzahl elektronischer Schlüssel für verschiedene zugehörige elektronische Schlösser enthalten kann.

7. Verfahren nach Anspruch 6, **dadurch gekennzeichnet, dass** die Mehrzahl elektronischer Schlüssel sicherheitskritische und sicherheitsunkritische Schlüssel umfasst, und vor dem Zugriff auf den Schließzustand des elektronischen Schlosses mit einem zugeordneten sicherheitskritischen Schlüssel die Berechtigung des Benutzers durch Übergabe eines Geheimnisses oder durch Prüfung eines biometrischen Merkmals geprüft wird.

8. Verfahren nach Anspruch 6 oder 7, **dadurch gekennzeichnet, dass** die mobile Steuereinrichtung dem Benutzer eine Teilmenge nutzbarer Schlüssel aus der Mehrzahl elektronischer Schlüssel zum Öffnen und/oder Schließen der zugehörigen Schlösser zur Verfügung stellt, insbesondere auf Grundlage der Ortskoordinaten der mobilen Steuereinrichtung und der elektronischen Schlösser.

9. Verfahren nach wenigstens einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet, dass** die mobile Steuereinrichtung einen elektronischen Schlüssel einer anderen mobilen Steuereinrichtung übergibt, indem eine Authentisierung zur Überprüfung der Identität und Authentizität der anderen mobilen Steuereinrichtung und/oder des Benutzers der anderen mobilen Steuereinrichtung durchgeführt wird, und im Gutfall eine elektronische Kopie des Schlüssels der anderen mobilen Steuereinrichtung übergeben wird, vorzugsweise in elektronischer Form über eine Luftschnittstelle.

10. Verfahren nach Anspruch 9, **dadurch gekennzeichnet, dass** der übergebene Schlüssel mit einer Gültigkeitsdauer oder einem Verfallszeitpunkt versehen wird.

11. Verfahren nach Anspruch 10, **dadurch gekennzeichnet, dass** der Ablauf der Gültigkeitsdauer oder das Erreichen des Verfallszeitpunkts durch das dem übergebenen Schlüssel zugeordnete elektronische Schloss geprüft wird.

12. Verfahren nach wenigstens einem der Ansprüche 1 bis 11, **dadurch gekennzeichnet, dass** ein elektronischer Schlüssel vorgespannt werden kann, um das zugeordnete elektronische Schloss automatisch oder auf eine einfache Benutzerbestätigung hin zu öffnen, wenn die mobile Steuereinrichtung in einen vorbestimmten Umgebungsbereich des Schlosses gelangt.

13. Verfahren nach Anspruch 12, **dadurch gekennzeichnet, dass** vor dem Vorspannen eines Schlüssels die Berechtigung des Benutzers durch Übergabe eines Geheimnisses oder durch Prüfung eines biometrischen Merkmals geprüft wird.

14. Verfahren nach Anspruch 12 oder 13, **dadurch gekennzeichnet, dass** das Vorspannen eines Schlüssels mit einer Gültigkeitsdauer oder einem Verfallszeitpunkt versehen wird.

15. Verfahren nach wenigstens einem der Ansprüche 1 bis 14, **dadurch gekennzeichnet, dass** der Schließzustand des elektronischen Schlosses von der mobilen Steuereinrichtung über die Kommunikationsverbindung abgefragt wird.

16. Verfahren nach wenigstens einem der Ansprüche 1 bis 15, **dadurch gekennzeichnet, dass** eine Ortsinformation des elektronischen Schlosses über die Kommunikationsverbindung von der mobilen Steuereinrichtung abgefragt wird, insbesondere die Ortskoordinaten des Schlosses und/oder die Information, ob sich das Schloss noch am Ort des letzten Verschließens befindet.

17. Verfahren nach wenigstens einem der Ansprüche 1 bis 16, **dadurch gekennzeichnet, dass** die mobile Steuereinrichtung durch ein Mobiltelefon oder eine mobile Recheneinheit mit Mobilfunkerweiterung gebildet wird.

18. Verfahren nach wenigstens einem der Ansprüche 1 bis 17, **dadurch gekennzeichnet, dass** die Steuerungsfunktionen für das elektronische Schloss in einem Sicherheitsmodul, wie einem SIM, einem USIM oder einem R-UIM verwirklicht sind.

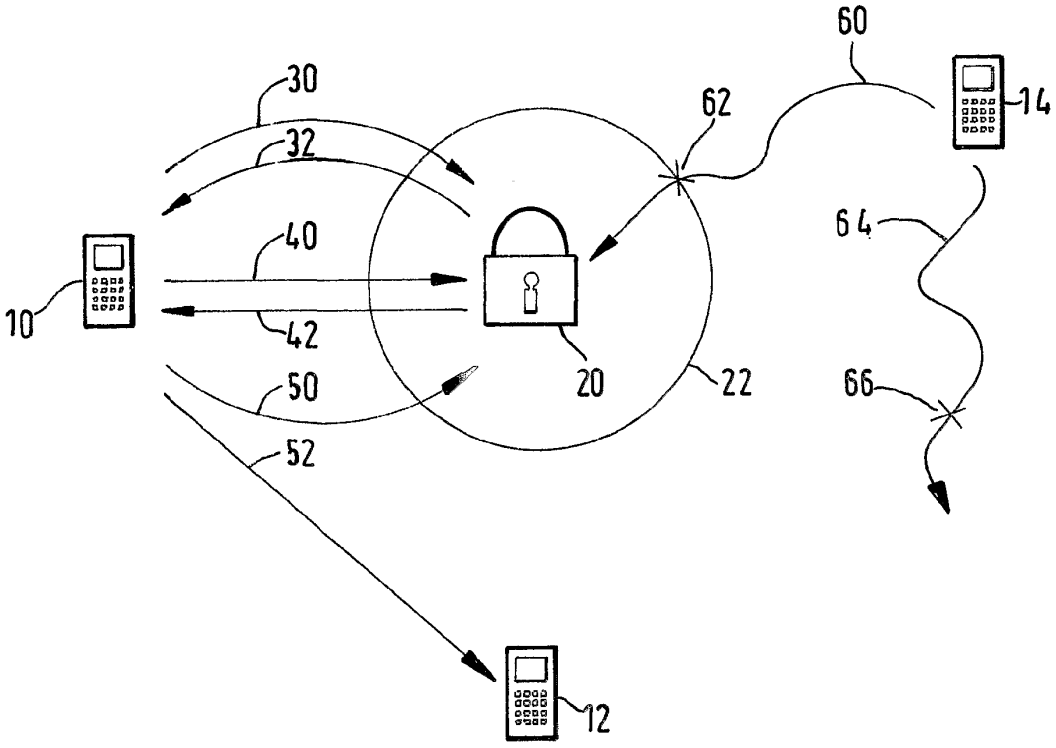
19. Verfahren nach wenigstens einem der Ansprüche 1 bis 18, **dadurch gekennzeichnet, dass** die Authentisierung nach einem Challenge-Response-Verfahren durchgeführt wird.

20. Mobile Steuereinrichtung (10, 12, 14) zur Durchführung des Verfahrens nach wenigstens einem der Ansprüche 1 bis 19.

21. Mobile Steuereinrichtung nach Anspruch 20, **dadurch gekennzeichnet, dass** die mobile Steuereinrichtung durch ein Mobiltelefon (10, 12, 14) oder eine mobile Recheneinheit mit Mobilfunkerweiterung gebildet ist.

22. Schlüssel-Schloss-Anordnung mit einer mobilen Steuereinrichtung (10, 12, 14) und einem oder mehreren elektronischen Schlössern (20) zur Durchführung des Verfahrens nach wenigstens einem der Ansprüche 1 bis 19.

23. Schlüssel-Schloss-Anordnung nach Anspruch 22, **dadurch gekennzeichnet, dass** die mobile Steuereinrichtung durch ein Mobiltelefon (10, 12, 14) oder eine mobile Recheneinheit mit Mobilfunkerweiterung gebildet ist.


60
30
62
14
32
64
40
10
42
20
22
50
66
52
12

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/008815

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C9/00

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)
IPC 7 G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 924 657 A (TRW INC) 23 June 1999 (1999-06-23) abstract; figures 1,4 paragraph '0016! - paragraph '0021! paragraph '0027! - paragraph '0031!	1-3,5, 17-23
X	WO 02/31778 A (NOKIA CORP ; NOKIA INC (US)) 18 April 2002 (2002-04-18) claims 1,2,8,11,12,15,1618,22,29 page 5, paragraph 2 - page 6, paragraph 1 page 7, paragraph 1 page 8, paragraph 1 - paragraph 3	1-3,5, 9-14, 17-23
X	WO 00/38119 A (GUENTZER PETER ; SIEMENS AG (DE)) 29 June 2000 (2000-06-29) abstract; claims	1-5,12, 13,17, 18,20-23

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 November 2004	06/12/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/008815

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 01/40605 A (NIELSEN ERNST LYKKE ; BORDING DATA AS (DK)) 7 June 2001 (2001-06-07) abstract; claims 1-10; figures 2a,2c,6a page 26, line 31 - page 27, line 9 page 42, line 18 - line 26	1-8,17, 18,20-23
X	WO 01/23694 A (TACTEL AB) 5 April 2001 (2001-04-05) abstract; figures 2-4	1-3,5, 12,13, 17-23
X	US 2003/117293 A1 (GHABRA RIAD ET AL) 26 June 2003 (2003-06-26) abstract; claims 1,6,7,11; figures	1,15,16
X	WO 01/86097 A (FRUM HANAN ; LEV IDI BINYAMIN (IL)) 15 November 2001 (2001-11-15) claims 1-3,9; figure 8 page 23, line 21 - page 27, line 19	1,2,15

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/008815

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0924657 A	23-06-1999	US 6038666 A	14-03-2000
		EP 0924657 A2	23-06-1999
		JP 3222111 B2	22-10-2001
		JP 11316818 A	16-11-1999
		US 6182221 B1	30-01-2001
WO 0231778 A	18-04-2002	FI 20002255 A	14-04-2002
		AU 9411501 A	22-04-2002
		EP 1325476 A1	09-07-2003
		WO 0231778 A1	18-04-2002
WO 0038119 A	29-06-2000	WO 0038119 A1	29-06-2000
WO 0140605 A	07-06-2001	AU 1513201 A	12-06-2001
		AU 1513301 A	12-06-2001
		CA 2392405 A1	07-06-2001
		CN 1413283 T	23-04-2003
		WO 0140605 A1	07-06-2001
		WO 0141075 A1	07-06-2001
		EP 1234084 A1	28-08-2002
		JP 2003515688 T	07-05-2003
		US 2002180582 A1	05-12-2002
WO 0123694 A	05-04-2001	AU 7697300 A	30-04-2001
		WO 0123694 A1	05-04-2001
US 2003117293 A1	26-06-2003	DE 10258760 A1	17-07-2003
		US 2003117267 A1	26-06-2003
WO 0186097 A	15-11-2001	AU 5661601 A	20-11-2001
		WO 0186097 A2	15-11-2001

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2004/008815

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07C9/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07C

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 924 657 A (TRW INC) 23. Juni 1999 (1999-06-23) Zusammenfassung; Abbildungen 1,4 Absatz '0016! - Absatz '0021! Absatz '0027! - Absatz '0031!	1-3,5, 17-23
X	WO 02/31778 A (NOKIA CORP ; NOKIA INC (US)) 18. April 2002 (2002-04-18) Ansprüche 1,2,8,11,12,15,1618,22,29 Seite 5, Absatz 2 - Seite 6, Absatz 1 Seite 7, Absatz 1 Seite 8, Absatz 1 - Absatz 3	1-3,5, 9-14, 17-23
X	WO 00/38119 A (GUENTZER PETER ; SIEMENS AG (DE)) 29. Juni 2000 (2000-06-29) Zusammenfassung; Ansprüche	1-5,12, 13,17, 18,20-23

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
26. November 2004	06/12/2004

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Buron, E

Formblatt PCT/ISA/210 (Blatt 2) (Januar 2004)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2004/008815

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 01/40605 A (NIELSEN ERNST LYKKE ; BORDING DATA AS (DK)) 7. Juni 2001 (2001-06-07) Zusammenfassung; Ansprüche 1-10; Abbildungen 2a,2c,6a Seite 26, Zeile 31 - Seite 27, Zeile 9 Seite 42, Zeile 18 - Zeile 26	1-8,17, 18,20-23
X	WO 01/23694 A (TACTEL AB) 5. April 2001 (2001-04-05) Zusammenfassung; Abbildungen 2-4	1-3,5, 12,13, 17-23
X	US 2003/117293 A1 (GHABRA RIAD ET AL) 26. Juni 2003 (2003-06-26) Zusammenfassung; Ansprüche 1,6,7,11; Abbildungen	1,15,16
X	WO 01/86097 A (FRUM HANAN ; LEV IDI BINYAMIN (IL)) 15. November 2001 (2001-11-15) Ansprüche 1-3,9; Abbildung 8 Seite 23, Zeile 21 - Seite 27, Zeile 19	1,2,15

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internat[illegible]es Aktenzeichen
PCT/EP2004/008815

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 0924657	A	23-06-1999	US	6038666 A	14-03-2000
			EP	0924657 A2	23-06-1999
			JP	3222111 B2	22-10-2001
			JP	11316818 A	16-11-1999
			US	6182221 B1	30-01-2001
WO 0231778	A	18-04-2002	FI	20002255 A	14-04-2002
			AU	9411501 A	22-04-2002
			EP	1325476 A1	09-07-2003
			WO	0231778 A1	18-04-2002
WO 0038119	A	29-06-2000	WO	0038119 A1	29-06-2000
WO 0140605	A	07-06-2001	AU	1513201 A	12-06-2001
			AU	1513301 A	12-06-2001
			CA	2392405 A1	07-06-2001
			CN	1413283 T	23-04-2003
			WO	0140605 A1	07-06-2001
			WO	0141075 A1	07-06-2001
			EP	1234084 A1	28-08-2002
			JP	2003515688 T	07-05-2003
			US	2002180582 A1	05-12-2002
WO 0123694	A	05-04-2001	AU	7697300 A	30-04-2001
			WO	0123694 A1	05-04-2001
US 2003117293	A1	26-06-2003	DE	10258760 A1	17-07-2003
			US	2003117267 A1	26-06-2003
WO 0186097	A	15-11-2001	AU	5661601 A	20-11-2001
			WO	0186097 A2	15-11-2001

DOCUMENT ID WO 2005017840 A1

DATE PUBLISHED 2005-02-24

INVENTOR INFORMATION

NAME	CITY	STATE	ZIP CODE	COUNTRY
RANKL WOLFGANG	N/A	N/A	N/A	DE

CPC CURRENT

TYPE	CPC	DATE
CPCI	G 07 C 9/00309	2013-01-01
CPCA	G 07 C 9/00563	2013-01-01
CPCA	G 07 C 2009/00793	2013-01-01
CPCA	G 07 C 2009/00388	2013-01-01
CPCA	G 07 C 2209/62	2013-01-01

KWIC Hits

APPLICATION FILING DATE

20[illegible]

Abstract

The invention relates to a method for contactlessly controlling the locking state of an electronic lock with a mobile control device by a user, during which a bi-directional communications link is established between the mobile control device and the electronic lock. An authentication for verifying the identity and authenticity of the mobile control device and/or of the electronic lock is carried out via said communications link, and the mobile control device transmits an electronic key to electronic lock in order to access the locking state thereof.

Description

<Desc / Clms Page number 1> The invention relates to a method for contactless control of the closed state of an el

Claims

1. Method for contactless control of the closed state of an electronic lock with a mobile control device by a user, in which a bidirectional communication connection is established between the mobile control device and the electronic lock, authentication via the communication connection for checking the identity and Authenticity of the mobile control device and / or the electronic lock is carried out, and the mobile control device transmits an electronic key to access the closed state of the electronic lock.

2. The method according to claim 1, characterized in that the communication connection is established in a mobile radio network such as GSM or UMTS, in particular with a packet-oriented carrier service such as GPRS.

3. The method according to claim 1, characterized in that the communication connection is established in a short-range channel integrated in the mobile control device, such as the IrDA interface, Bluetooth or WLAN.

4. The method according to at least one of claims 1 to 3, characterized in that a plurality of different transmission channels are available for the communication connection and a suitable transmission channel is selected for the communication connection before the communication connection is set up, in particular that the suitable <Desc / Clms Page number 13> nete transmission channel is selected by automatic testing or by using a location-based service.

5. The method according to at least one of claims 1 to 4, characterized in that prior to access to the closed state of the electronic lock, the authorization of the user by transferring a secret, such as a PIN number, or by checking one biometric feature is checked.

6. The method according to at least one of claims 1 to 5, characterized in that the mobile control device can contain a plurality of electronic keys for various associated electronic locks.

7. The method according to claim 6, characterized in that the plurality of electronic keys comprises security-critical and non-security-critical keys, and prior to access to the locked state of the electronic lock with an assigned security-critical key, the authorization of the user by transferring a secret or by checking a biometric feature is checked.

8. The method according to claim 6 or 7, characterized in that the mobile control device provides the user with a subset of usable keys from the plurality of electronic keys for opening and / or closing the associated locks, in particular on the basis of the location coordinates of the mobile control device and electronic locks. <Desc / Clms Page number 14>

9. The method according to at least one of claims 1 to 8, characterized in that the mobile control device transfers an electronic key to another mobile control device by authentication to check the identity and authenticity of the other mobile control device and / or the user of the other mobile control device is carried out, and in the best case an electronic copy of the key is handed over to the other mobile control device, preferably in electronic form via an air interface.

10. The method according to claim 9, characterized in that the transferred key is provided with a period of validity or an expiry time.

11. The method according to claim 10, characterized in that the expiry of the period of validity or the reaching of the expiry time is checked by the electronic lock assigned to the transferred key.

12. The method according to at least one of claims 1 to 11, characterized in that an electronic key can be biased to open the associated electronic lock automatically or upon simple user confirmation when the mobile control device is in a predetermined surrounding area of the lock arrives.

13. The method according to claim 12, characterized in that prior to the pretensioning of a key, the authorization of the user is checked by transferring a mistake or by checking a biometric feature. <Desc / Clms Page number 15>

027

14. The method according to claim 12 or 13, characterized in that the pretensioning of a key is provided with a period of validity or an expiry time.

15. The method according to at least one of claims 1 to 14, characterized in that the closed state of the electronic lock is queried by the mobile control device via the communication link.

16. The method according to at least one of claims 1 to 15, characterized in that location information of the electronic lock is queried via the communication link by the mobile control device, in particular the location coordinates of the lock and / or the information as to whether the lock is still at the location of the last closure.

17. The method according to at least one of claims 1 to 16, characterized in that the mobile control device is formed by a mobile phone or a mobile computing unit with a mobile radio extension.

18. The method according to at least one of claims 1 to 17, characterized in that the control functions for the electronic lock are implemented in a security module, such as a SIM, a USIM or an R-UIM.

19. The method according to at least one of claims 1 to 18, characterized in that the authentication is carried out according to a challenge-response method. <Desc / Clms Page number 16>

20. Mobile control device (10, 12, 14) for performing the method according to at least one of claims 1 to 19.

21. Mobile control device according to claim 20, characterized in that the mobile control device is formed by a mobile phone (10, 12, 14) or a mobile computing unit with a mobile radio extension.

22. Key and lock arrangement with a mobile control device (10, 12, 14) and one or more electronic locks (20) for carrying out the method according to at least one of claims 1 to 19.

23. The lock and key arrangement according to claim 22, characterized in that the mobile control device is formed by a mobile phone (10, 12, 14) or a mobile computing unit with a mobile radio extension.

Copyright ©2021 Clarivate Analytics. All rights reserved. Republication or redistribution of Clarivate Analytics content, including by framing or similar means, is prohibited without the prior written consent of Clarivate Analytics. Clarivate and its logo are trademarks of the Clarivate Analytics group.

<Desc / Clms Page number 1> The invention relates to a method for contactless control of the closed state of an electronic lock. The invention further relates to a mobile control device and a key and lock arrangement for carrying out such a method. In addition to the primary functions such as communication and data storage, today's mobile phones have only a few functionalities that can be used in everyday life. Current enhancements such as MP3 players, a built-in digital camera or location-based services such as GPS (Global Positioning System) show the trends towards more diverse areas of application for mobile phones. Proceeding from this, the object of the invention is to open up additional application possibilities in the field of daily life to the user of a mobile telephone. This object is achieved by the method for contactless control of the closing state of an electronic lock with the features of the main claim. A mobile control device and a key lock arrangement for carrying out such a method are the subject of the independent claims 20 and 22. Further developments of the invention are the subject of the dependent claims. According to the invention, the contactless control is carried out by a user with a mobile control device. Between the mobile tax <Desc / Clms Page number 2> direction and the electronic lock, a bidirectional communication link is established and authentication is carried out via the communication link to check the identity and authenticity of the mobile control device and / or the electronic lock. To access the closed state of the

electronic lock, the mobile control device transmits an electronic key to it. The invention makes it possible to expand the functionality of mobile control devices, such as mobile telephones, by the function of a key board for electronic locks. The mobile phone is an ideal medium, particularly in the area of the key lock, because it is usually always carried with you and, thanks to the security module it contains, you can achieve significantly higher security than with previous locks. In an advantageous embodiment of the method according to the invention, the communication connection is established in a mobile radio network such as GSM (Global System for Mobile communications) or UMTS (Universal Mobile Telecommunication System), in particular with a packet-oriented carrier service, such as GPRS (General Packet Radio Service). According to a further advantageous embodiment, the communication connection is established in a short-range channel integrated in the mobile control device, such as the IrDA (Infrared Data Association) interface, Bluetooth or WLAN (Wireless Local Area Network). Several different transmission channels can also be available for the communication connection. Before a connection is established, a suitable transmission channel for the communication connection is then established, for example by automatic testing or by using <Desc / Clms Page number 3> selected a location-based service. Typically, the cheapest of the available channels is chosen for the establishment of the communication connection. However, other

criteria, such as the quality or security of a connection, can also be used as a selection criterion. Before accessing the closed state of the electronic lock, the authorization of the user is preferably checked by transferring a secret, such as a PIN number, or by checking a biometric feature, such as voice features of the user. By uniquely identifying the user, the risk of a lost or stolen control unit is significantly reduced. In a preferred development of the method, the mobile control device can contain a plurality of electronic keys for various associated electronic locks. The control device then serves as an electronic key board, which can manage and use a large number of electronic keys. According to an expedient embodiment of the invention, the plurality of electronic keys contain security-critical and security-non-critical keys. Before accessing the locked state of an electronic lock with an assigned security-critical key, the user's authorization is checked by transferring a secret or by checking a biometric feature. It is also conceivable to provide various complex security measures for the use of security-critical and non-critical keys or to divide the keys into more than two security categories. <Desc / Clms Page number 4> The mobile control device advantageously provides the user with a subset of usable keys from the plurality of electronic keys for opening and / or closing the associated locks. In particular, the subset can be selected on the basis of the location coordinates of the mobile control device and the electronic locks. For example, only those keys can be displayed

to the user whose associated locks are located within a preselected surrounding area of the mobile control device. On the one hand, this prevents undesired operating errors, such as unintentional opening of the front door lock at home, while the user is far away on vacation. On the other hand, the operation of the mobile control device is significantly simplified, especially when there are a large number of available keys, since only those keys are displayed which can be used sensibly at the current location. Otherwise, especially when the key-lock method is used over a large area, the user-friendliness would suffer due to a large number of locking and unlocking options. The mobile control device can also transfer an electronic key to another mobile control device. For this purpose, authentication is carried out to check the identity and authenticity of the other mobile control device and / or the user of the other mobile control device. In the best case, an electronic copy of the key is transferred to the other mobile control device, preferably in electronic form, via an air interface. The electronic key board therefore includes the option of authorized locking authorizations. <Desc / Clms Page number 5> In an expedient embodiment, the transferred key is provided with a validity period or an expiry date. The expiry of the period of validity or the reaching of the expiry time is advantageously checked by the electronic lock assigned to the transferred key in order to rule out manipulation of the other electronic control unit. Certain keys can be excluded from disclosure to minimize the risk of unauthorized use of

the keys. It can also be provided that keys passed on cannot be passed on again. For example, keys can be passed on in an authorized manner within a family, for example to children. Disclosure by the children to third parties can be excluded. Another application example arises in the case of a hotel stay in which the hotel guest is to be given the opportunity for a limited period of time to be able to lock or unlock the hotel room door or an underground car park. According to an advantageous further development, an electronic key can be pretensioned in order to open the assigned electronic lock automatically or upon simple user confirmation when the mobile control device reaches a predetermined surrounding area of the lock. Prior to the pretensioning of a key, the authorization of the user is preferably checked by transferring a secret or by checking a biometric feature. The pretensioning of a key is expediently provided with a period of validity or an expiry date in order to prevent a pretensioned key from unintentionally opening the associated electronic lock. <Desc / Clms Page number 6> According to a further expedient method possibility, the closed state of the electronic lock is queried by the mobile control device via the communication link. A forgetful user can thus insure himself via a remote query of the locked state of an electronic lock and save himself the time-consuming and often time-consuming task of subsequently checking the closed state. In a further advantageous embodiment, location information of the electronic lock can be queried by the mobile control

device via the communication link. In particular, the location coordinates of the lock can be queried and / or the information as to whether the lock is still at the location where it was last closed. It goes without saying that this possibility is used above all in the case of locks which are attached in a mobile manner, for example on a motor vehicle. The location coordinates of the lock can be determined by the lock, for example, via the location information supplied by a mobile radio system or via GPS or a comparable service. The mobile control device is advantageously formed by a mobile phone or a mobile computing unit, for example a so-called digital assistant (PDA) with a mobile radio extension. For security reasons, the control functions for the electronic lock are preferably implemented in a security module, such as a SIM (Subscriber Identity Module), a USIM (Universal Subscriber Identity Module) or an R-UIM (Removable User Identity Module). Alternatively, the control functions can also be located as a program on the mobile control device, for example as J2ME (Java 2 Micro Edition) - <Desc / Clms Page number 7> Applet in a JAVA-compatible mobile phone. In this case, known security mechanisms such as, for example, signature and encryption functions of the WIM (Wireless Application Protocol Identity Module) are expediently used to secure the data on the air interface from the chip card area. The authentication for checking the identity and authenticity of a mobile control device and / or a lock is preferably carried out according to a

challenge-response method. A secret key of a crypto-algorithm is the shared secret of the mobile control device and the electronic lock. One of the communication partners sends the other a random number, which is encrypted with the crypto-algorithm and sent back to the questioner. If the questioner applies the inverse function of the crypto-algorithm to the number received and compares the result with the originally sent random number, he can conclude, if there is a match, that the other participant knows the secret key and is therefore authentic. Depending on the function provided below, one-sided or mutual authentication can be carried out. The invention also includes a mobile control device which is designed and set up to carry out the described method. In particular, the mobile control device is formed by a mobile phone or a mobile computing unit with a mobile radio extension. Furthermore, the invention comprises a lock and key arrangement with a mobile control device and one or more electronic locks, which are designed and set up to carry out the described method. The mobile control device is also advantageous here <Desc / Clms Page number 8> formed by a cell phone or a mobile computing unit with cell phone expansion. An embodiment and advantages of the invention are explained below with reference to the figure. The single figure shows a schematic representation of possible uses of an electronic key board integrated in a mobile phone according to an embodiment of the invention. In addition to the conventional functionalities, the mobile telephones 10, 12 and 14

each contain an electronic key board with a plurality of electronic keys. The electronic lock 20 exemplifies the electronic locks assigned to the keys. The functions of the key board described below are each implemented in a secure environment of the mobile telephones 10, 12, 14, such as a SIM. To control the closed state of the lock 20, the mobile telephone 10 establishes a bidirectional communication connection to the electronic lock 20, in the exemplary embodiment using the packet-oriented GPRS data service. Since the amount of data exchanged is very small (only a few bytes), the communication costs between the mobile phone 10 and the lock 20 are negligible. The bidirectional communication link allows conventional authentication methods, such as ChallengeResponse, to be carried out between the mobile telephone 10 and the lock 20 without great effort. Depending on the following functions, one-sided or mutual authentication is used. <Desc / Clms Page number 9> A first use case is to query the closed state of the lock 20. The mobile phone 10 sends a corresponding request 30 to the lock 20. When the querying mobile phone 10 is successfully authenticated, the lock 20 returns a closed state information 32, that is, the information as to whether the lock is open or locked. The information is then shown on the display of the mobile phone 10 for the user. In a second use case, the mobile phone 10 queries the location of the lock 20 via a corresponding request 40. This query can be used in particular in the case of mobile locks, for example the door lock of a motor vehicle.

As an answer 42, the lock 20 can return the location coordinates of the lock or, if desired, only return the information as to whether the lock 20 is still at the location of the last locking. The lock 20 determines its location coordinates, for example, via the location information of the mobile radio system or via GPS. The transfer of the locking authorization for the lock 20 to another mobile phone 12 is illustrated as a third use case. For this purpose, after prior identification and / or authentication of the other mobile telephone 12, an electronic copy of the key is made and transmitted to the other mobile telephone 12 in electronic form 52 via the air interface. The copied key is provided with an expiry date which is communicated to the lock 20 by the first mobile telephone 10 (reference number 50). In the event of an attempt to access by the other mobile telephone 12, the lock 20 then first checks whether the copied key 52 is still valid. <Desc / Clms Page number 10> The electronic lock 20 can, for example, represent the lock of a hotel room door for which a hotel guest is granted the locking authorization for the duration of his stay. The three use cases described, for example, each require a paid connection in the case of a GSM or UMTS network, since data must be transmitted. The pretensioning of an electronic key for the lock 20 is illustrated for a further mobile phone 14. Pretensioning the key means that the assigned lock 20 is opened automatically as soon as the mobile phone 14 reaches a predetermined surrounding area 22 of the lock 20 by a spatial movement 60. In the

exemplary embodiment, this is the case at point 62. Alternatively, an opening question such as "Open lock?" appear on the display of the mobile telephone 14 and the lock 20 can be opened upon simple confirmation. In the exemplary embodiment, the prestressed state of a key is provided with a period of validity after which the prestressing of the key is released. This is illustrated in the movement path 64, which never brings the mobile phone 14 into the surrounding area 22 of the lock 20 until the validity period has expired. When the period of validity at point 66 expires, the key's pre-tensioned state disappears; subsequent entry into the surrounding area 22 then does not result in an automatic action. The key board of the mobile telephone 10 typically contains several keys, the properties of which in the exemplary embodiment are in the form of a table <Desc / Clms Page number 11> are stored in a memory of the mobile phone 10. The first two entries in this table may have the form and content shown in Table 1. Table 1 : EMI11.1 <Tb> <tb> Lock ID <SEP> 1234 <SEP> 9876 <Tb> <Tb> <Tb> <Tb> <Tb> <Tb> <tb> Connection type <SEP> GSM <SEP> WLAN <Tb> <Tb> <Tb> <Tb> <Tb> <Tb> <tb> Authentication <SEP> ge-MSISDN <SEP> of the <SEP> mobile tele-challenge response, <SEP> <Tb> <Tb> <Tb> <Tb> <Tb> <tb> opposite <SEP> lock <SEP> fons <SEP> on the opposite side <Tb> <Tb> <Tb> <Tb> <Tb> <Tb> <tb> Identification <SEP> of the <SEP> no <SEP> language <Tb> <Tb> <Tb> <Tb> <tb> user <Tb> <Tb> <Tb> <Tb> <Tb> <Tb>

<tb> location function <SEP> lock <SEP> stationary <SEP> mobile, <SEP> coordinates <SEP> <Tb> <Tb> <Tb> <Tb> <tb> the <SEP> when locking the <SEP> <Tb> <Tb> <Tb> <Tb> <Tb> <tb> saved <Tb> <Tb> <Tb> <Tb> <Tb> <Tb> <tb> Functions <SEP> Lock <SEP> Open, <SEP> Close, <SEP> Open, <SEP> Close, <Tb> <Tb> <Tb> <Tb> <Tb> <Tb> <tb> query <SEP> closing state <SEP> query <SEP> closing state, <Tb> <Tb> <Tb> <Tb> <Tb> <Tb> <tb> Remove <SEP> lock location <Tb> <Tb> <Tb> <Tb> <Tb> <Tb> <tb> Forwarding <SEP> Lock-permitted <SEP> not <SEP> allowed <Tb> <Tb> <Tb> <Tb> <Tb> <tb> authorization <Tb>

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	553	hotel AND (door SAME lock SAME phone) AND @ad < "20100302"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/10/06 05:33 PM
L2	235	hotel AND (door SAME lock SAME phone) AND (duration OR expir$5) AND @ad < "20100302"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2021/10/06 05:33 PM

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

UNITED STATES PATENT AND TRADEMARK OFFICE

USPTO Automated Interview Request (AIR)

Nov 5 2021

This paper requesting to schedule and/or conduct an interview is appropriate because:

This submission is requested to be accepted as an authorization for this interview to communicate via the internet. Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with the undersigned concerning scheduling of the interview via video conference, instant messaging, or electronic mail, and to conduct the interview in accordance with office practice including video conferencing.

Name(s):
John R. Kasha

S-signature:
/John Kasha/

Registration Number:
53100

U.S. Application Number:
96000367

Confirmation Number:
7090

E-mail Address:
john.kasha@kashalaw.com

Phone Number:
+1 7038671886

Proposed Time of Interview:
12-10-2021 1:00 PM ET

Alternative Proposed Time(s) of Interview:
12-9-2021 1:00 PM ET

Alternative Proposed Time(s) of Interview:
12-8-2021 1:00 PM ET

Prefered Interview Type:
Video Conference

I am the applicant or applicant's representative for this application.

Topic for Discussion:

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.
96/000,367	08/04/2021	9373205	LBT0010-CON-SE	7090

67050 7590 12/16/2021

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

EXAMINER	
CARLSON, JEFFREY D	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
12/16/2021	PAPER

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.

Ex Parte Reexamination Interview Summary	Control No. 96/000,367	Patent Under Reexamination 9373205	
	Examiner JEFFREY D CARLSON	Art Unit 3992	AIA (FITF) Status No

All participants (USPTO personnel, patent owner, patent owner's representative):

(1) JEFFREY CARLSON - PTO	(3) John Kasha - for Patent Owner
(2) Mike Fuelling, Michelle Tarae - PTO	(4) William Redmann, Chris Outwater - Inventors

Date of Interview: 13 December 2021

Type: a) ☐ Telephonic b) ☑ Video Conference
c) ☐ Personal (copy given to: 1) ☐ patent owner 2) ☐ patent owners representative)

Exhibit shown or demonstration conducted: d) ☐ Yes e) ☑ No.
If Yes, brief description: _____

Agreement with respect to the claims f) ☐ was reached. g) ☑ was not reached. h) ☐ N/A.
Any other agreement(s) are set forth below under "Description of the general nature of what was agreed to..."

Claim(s) discussed: 1,5-6 and 25-26 .

Identification of prior art discussed: Brondrup, WO 2005017840 .

Description of the general nature of what was agreed to if an agreement was reached, or any other comments:
See Continuation Sheet .

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims patentable, if available, must be attached. Also, where no copy of the amendments that would render the claims patentable is available, a summary thereof must be attached.)

A FORMAL WRITTEN RESPONSE TO THE LAST OFFICE ACTION MUST INCLUDE PATENT OWNER'S STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. (See MPEP § 2281). IF A RESPONSE TO THE LAST OFFICE ACTION HAS ALREADY BEEN FILED, THEN PATENT OWNER IS GIVEN **ONE MONTH** FROM THIS INTERVIEW DATE TO PROVIDE THE MANDATORY STATEMENT OF THE SUBSTANCE OF THE INTERVIEW
(37 CFR 1.560(b)). THE REQUIREMENT FOR PATENT OWNERS STATEMENT CAN NOT BE WAIVED.
EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).

/JEFFREY D CARLSON/ Primary Examiner, Art Unit 3992		/CMT/ Primary Examiner, Art Unit 3992

cc: Requester (if third party requester)

Continuation of Description of the general nature of what was agreed to if an agreement was reached, or any other comments:

Patent Owner provided an agenda/remarks and proposed amendments (see attached).

Patent Owner proposes to add language from claims 5 and 6 into claim 1 as well as to add new claims 25 and 26.

Patent Owner argues that it would not have been obvious to combine the references because Brondrup already successfully keeps track of the reservation intervals without the need for a clock at the door lock. And to do so would be superfluous.

Patent Owner references the claimed certificate as comprising a “start time” and that the processor “ compares an interval of a reservation that includes a start time” to a current time in order to open the lock.

Patent Owner argues that neither Brondrup nor WO 2005017840 provide “a validity period of a reservation for a door opening request” and that WO 2005017840 teaches a copy of a key to be checked for validity after the reservation has started. Examiner notes that each of Brondrup and WO 2005017840 certainly include reservation periods in order to only allow current reservation holders into the appropriate hotel rooms . Examiner notes that the rejection is also based on the combination of references and that the WO 2005017840 was relied upon for its teachings to equip a lock with time-based validity-checking capabilities. Inasmuch as pertinent, the examiner also treats a validity period as a “reservation”.

Patent Owner argues that the patent is directed to an improvement for its ability to issue a key before the use/stay, due to the asserted start time. This was explained in the context of a cell phone losing connectivity in a parking garage, and such example was believed to be referring to a charging station. Examiners will again review the amended claims (and patent owner's scope of enablement) and each of the applied references’ teachings when the response is filed.

Examiner noted that claim 25 would be subject to a 112 2nd rejection for its method steps appearing in this device claim (as was the case for claims 1-12). Examiner also questioned how a lock can be further defined by features of an unclaimed reseravation system. Patent Owner to consider including a reservation system as part of claim 1. Examiner reminded Patent Owner that the claims cannot be broadened with respect to the patented claims.

Agenda for Interview of App. 96/000,367 on 12/13/2021

Below are the arguments the Patent Owner intends to make in the Interview at 1:00 pm on Monday, December 13, 2021.

Claim 5

Claim 5 of the '205 Patent recites that the processor of the access device (lock) has access to the current time, the reservation certificate includes data representative of an interval of the reservation, and the lock is activated for the interval of the reservation. In other words, the lock gets the current time, receives an interval of the reservation from the certificate, and activates the lock for the interval of the reservation if the current time is within the interval of the reservation.

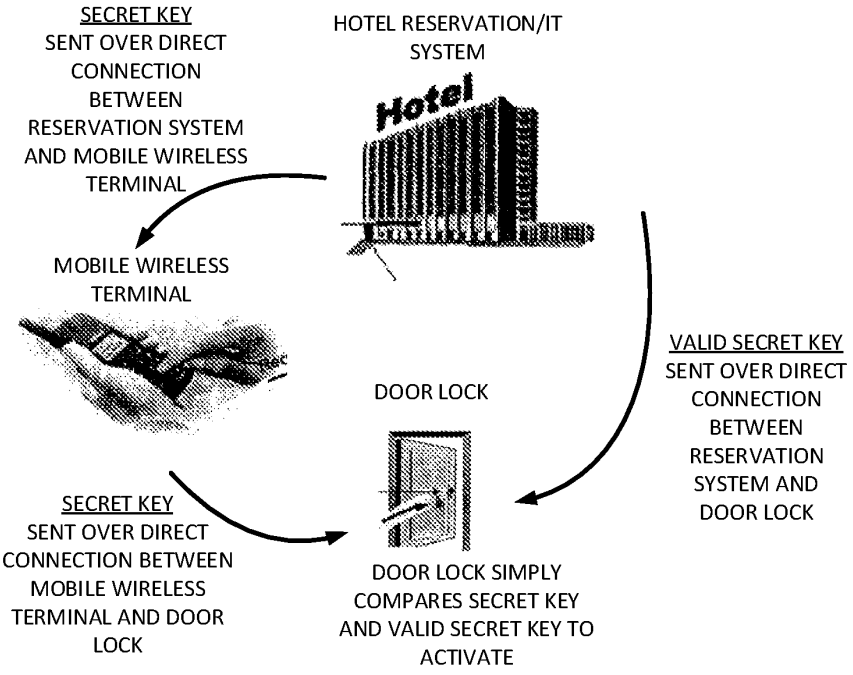
In the OA on page 13, claim 5 is rejected as being obvious over Brondrup in view of the '840 Application. The Examiner asserts that Brondrup discloses a reservation certificate that includes data "representative of" the interval of the reservation because the key token (reference number) of Brondrup is "tied to" the reservation. The Examiner admits that Brondrup does not disclose a door lock processor with access to the current time.

However, on pages 13-14 of the OA, the Examiner finds that the '840 Application suggests that its lock has access to the current time. The Examiner asserts that the '840 Application teaches a key that "can be provided with a period of validity or an expiry date in order to limit access to the room to the appropriate time interval" and a lock that "itself checks the expiration/validity period before allowing access."

The Examiner asserts that it would be obvious to combine the two references because "comparing the reservation interval with the current date/time … allows access only for a currently valid reservation. This represents an obvious alternative for determining valid

reservation status at the time of requesting access. One of ordinary skill would recognize that the lock would require access to the current time (and day) in order to 'check' the expiry of the validity period."

The Patent Owner respectfully disagrees that it would be obvious to combine Brondrup and the '840 Application's disclosure of comparing an expiry time on an electronic lock because it is an obvious alternative for determining a valid reservation status. The combination of Brondrup and the '840 Application is ***not an obvious alternative*** because the lock of Brondrup already has access to and determines the reservation status through its direct communication channel with the reservation system. Drawing 1, shown below, depicts the direct connection between the reservation system and the door lock in Brondrup.



DRAWING 1 (BRONDRUP)

Brondrup does not need to check an expiry period because it only places the valid secret key on the door lock during the interval of the reservation. Essentially, because of the second communication channel, the reservation system of Brondrup is able to keep track of the interval of the reservation rather than the lock.

In other words, the skilled person would not modify Brondrup to send an interval of the reservation with its key token to a mobile device that, in turn, sends it to a lock, and would not modify Brondrup to require its lock to compare it to a current time. The skilled person would not make this modification since ***it is superfluous to the method Brondrup currently employs***. In other words, adding this to Brondrup would increase the cost and reduce the efficiency of the method of Brondrup by providing the same information in two different ways. Currently, the lock of Brondrup simply determines if the key provided by a mobile wireless terminal matches a valid key provided by the reservation system. No timekeeping or time comparison is needed on the lock of Brondrup.

To move prosecution forward, however, the Patent Owner has further amended claim 1 of the '205 Patent to include elements of claim 5 and claim 6. As described above, claim 5 of the '205 Patent recites that the processor has access to the current time and activates the door lock during an interval of the reservation. Claim 6 of the '205 Patent recites that the interval of the reservation "is specified by a start time and one of an end time and a duration." Specifically, the Patent Owner has amended claim 1 to further recite that (1) a reservation certificate comprises an interval of a reservation that includes at least ***a start time of the reservation*** and, (2) when a current reservation certificate has been presented, the processor compares an interval of a

reservation of the current reservation certificate to a current time accessible to the processor, determines the current time is within the interval of the reservation, and activates the door lock during the interval of the reservation. Col. 5, lns. 43-47 of the '205 Patent, for example, specify that a certificate includes a "reservation start time."

In rejecting claim 6, on page 15 of the OA, the Examiner asserts that "[g]iven the obviousness laid out for claim 5, one of ordinary skill would have recognized either of 1) start time and end time or 2) start time and duration as two obvious and essentially equivalent and alternative ways to define, determine and discriminate the validity period of a user's hotel reservation for a door opening request." The Examiner essentially argues that a start time is an obvious way to define a validity period of a reservation for a door opening request.

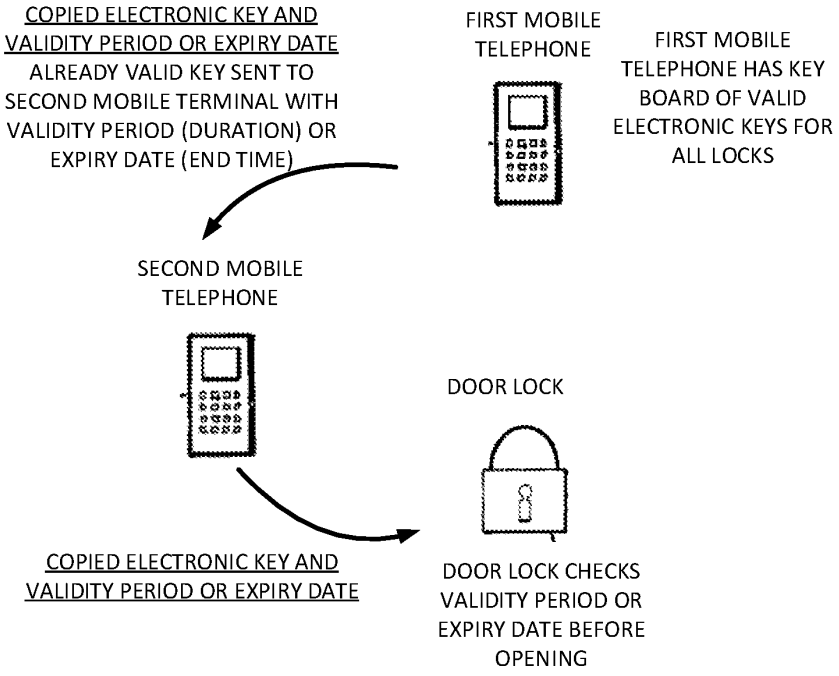
The Patent Owner submits, however, that neither Brondrup nor the '840 Application teaches or suggests providing a validity period ***of a reservation*** for a door opening request. Brondrup certainly does **not** teach or suggest providing a validity period of a reservation with a key token sent to the lock. As described above, Brondrup would not teach or suggest this because the lock of Brondrup has access to all the reservation information through its direct communication with the reservation system. The Examiner also admits that the lock of Brondrup does not have the current time, so a validity period would be of no use to Brondrup. In other words, providing a validity period of a reservation with a key token would be superfluous and useless in Brondrup.

The '840 Application also does not teach or suggest providing a validity period "of a reservation" for a door opening request. Instead, the '840 Application discloses the validity period or expiry date "of a copied key" of an already valid electronic key for opening a lock. The '840 Application ***discloses nothing about a reservation or reservation system***. Thus, the '840 Application could not possibly teach sending a reservation certificate with a start time of the reservation.

The '840 Application does disclose copying ***an already valid*** electronic key of a hotel room and determining if it is expired. The '840 Application, therefore, instead describes how "a key" is received and checked for expiration after a customer's stay or reservation at a hotel has already started. As a result, the '840 Application cannot be checking the validity period "of a reservation."

In other words, the electronic keys of the '840 Application are wireless versions of the well-known magnetic cards issued by hotels at the start of a customer's stay. These magnetic cards are referred to as "key cards" and have an expiration date just like the electronic keys of the '840 Application. These key cards do not need the start time of the reservation since they are issued when the reservation may have already started. Even if they were to have a start time, this start time would be the start time of the validity of the key and not the start time of the reservation.

Drawing 2, shown below, depicts the copying of a valid key in the '840 Application.



DRAWING 2 ('840 Application)

One of ordinary skill in the art would recognize that, in the '840 Application, the ability of one mobile phone to copy an electronic key and transfer it to another mobile phone is completely akin to the magnetic card writers copying keys onto the magnetic cards currently used by hotels. This is why, for example, a mobile phone is copying an electronic key and not a central server of the hotel's reservations system in the '840 Application. An originating mobile phone can be located in each hotel just like a magnetic card writer. A hotel customer, therefore, using either the current magnetic card writers and magnetic cards or the system of the '840 Application, has to obtain the key at the time of arrival of their stay.

In contrast, the '205 Patent is directed to an improvement in which the key includes the interval of the reservation and can, therefore, be issued before the stay. In other words, the "start

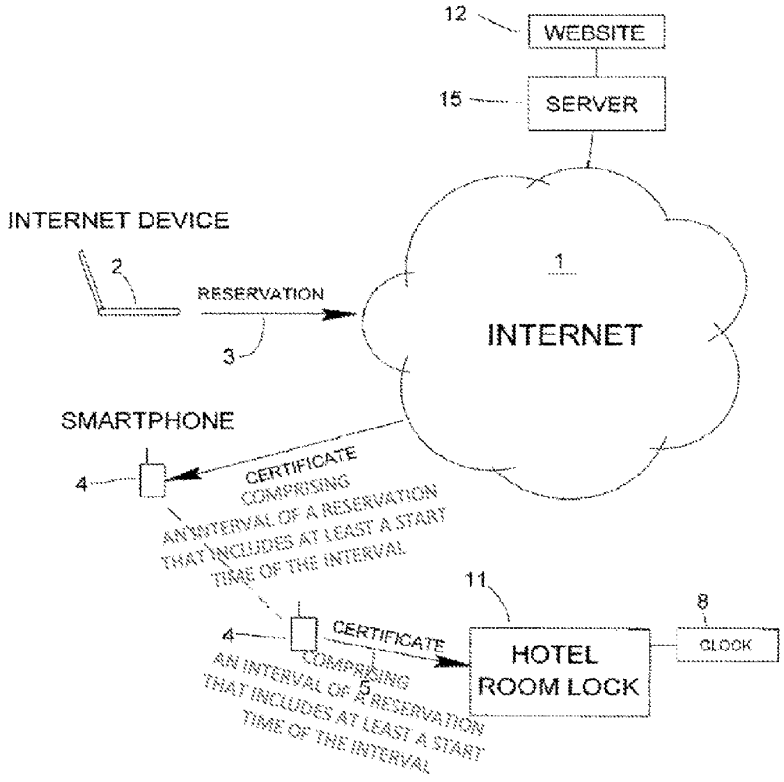
time" of the reservation makes it possible to issue a reservation certificate before the stay. The start time prevents access to the room before the reservation starts. This allows a hotel customer to bypass the hotel desk and proceed directly to their room. Essentially, this makes a hotel a self-service type business. This is a significant improvement over the current magnetic card writers and magnetic cards and the system of the '840 Application.

In summary, claim 1 is amended to recite that:

(1) a reservation certificate comprises an interval of a reservation that includes at least ***a start time of the reservation*** and,

(2) when a current reservation certificate has been presented, the processor compares an interval of a reservation of the current reservation certificate to a current time accessible to the processor, determines the current time is within the interval of the reservation, and activates the door lock during the interval of the reservation.

Annotated Figure 5 of '205 Patent, shown below, depicts how a reservation certificate that comprises an interval of a reservation that, in turn, includes at least a start time of the reservation is communicated in the '205 Patent.



ANNOTATED
FIG. 5

New claims 25 and 26, shown below, further distinguish the present application by describing how the start time of the reservation originates and is communicated. The start time of a reservation is entered by a user ahead of time. *See* the '205 Patent at col. 7, lns. 15-18. This start time is then included in the reservation certificate at creation by the reservation server, sent to the smartphone, and presented to the lock as part of the interval of the reservation. *See* the '205 Patent at col. 4, lns. 1-6 and col. 5, lns. 41-47. Neither Brondrup nor the '840 Application, either alone or in combination, describes this origination and communication of a start time.

In summary, claim 1 is allowable over Brondrup and the '840 Application because:

1. Brondrup does not teach or suggest using a reservation certificate that includes an interval of a reservation with a ***start time of the reservation*** to activate a lock because Brondrup already has access to all reservation information via its direct communication to the reservation system (the Examiner admits Brondrup has no means of determining the current time, so a start time of the reservation is of no use to Brondrup), and
2. the '840 Application does not teach or suggest using a reservation certificate that includes an interval of a reservation with a ***start time of the reservation*** to activate a lock because the '840 Application is only directed to determining the expiry of an already valid hotel key and is not directed to determining the start time of a reservation or anything about a reservation (the '840 Application could not teach or suggest the start time of the reservation since it has no access to a reservation system).

Finally, the access device of claim 1 is an improvement over Brondrup and the '840 Application because:

1. it does not require using a separate communication channel to the reservation system like Brondrup, making it less costly to implement and making it less susceptible to disruptions with the separate communication channel and, therefore, more reliable, and
2. it does not require that an electronic key be issued at the time of the customer's stay like the '840 Application, but instead allows the reservation certificate to be issued before the stay, potentially making the hotel a self-service type business.

Claim Amendments

1. (amended) An access device for use in an access control system, the access device comprising:

a processor (16) having control of a door lock (11); and a communication module (17) connected to the processor, the processor able to receive a reservation certificate (5) that comprises an interval of a reservation that includes at least a start time of the reservation presented by a portable terminal (4) through the communication module; wherein, when a current reservation certificate has been presented, the processor compares an interval of a reservation that includes a start time of the reservation of the current reservation certificate to a current time accessible to the processor, determines the current time is within the interval of the reservation, and activates the door lock during the interval of the reservation [when a current reservation certificate has been presented].

2. (amended) The access device of claim 1 wherein the processor determines the current time is within the interval of the reservation by determining if the current time is within the start time of the reservation of the reservation of the current reservation certificate and a predetermined duration and activates the door lock from the start time [for] up to the [a] predetermined duration.

3. (original) The access device of claim 2 wherein the predetermined duration is all day.

4. (amended) The access device of claim 1 wherein the interval of the reservation certificate further comprises [comprise data representative of] a duration and the processor activates the door lock from the start time of the reservation of the current reservation certificate [for] up to a [the] duration of the reservation of the current reservation certificate.

5. (amended) The access device of claim 6 [1] wherein the processor activates the door lock from the start time of the reservation of the current reservation certificate up to an end time of the reservation of the current reservation certificate [has access to the current time, the reservation certificate comprises data representative of an interval of the reservation, and the processor activates the door lock during the interval].

6. (amended) The access device of claim 1 [5] wherein the interval further comprises [is specified by a start time and one of] an end time [and a duration].

7. (original) The access device of claim 1 further comprising: a memory to which the processor has access, the memory containing a public key for a server authorized to issue the reservation certificate; wherein at least a portion of the reservation certificate is encrypted by the server using a private key and the processor verifies that the reservation

certificate is genuine by decrypting the portion with the public key.

8. (original) The access device of claim 1 further comprising: a memory to which the processor has access, the memory containing a symmetric key; wherein at least a portion of the reservation certificate is encrypted by a server using the symmetric key and the processor verifies that the reservation certificate is genuine by decrypting the portion with the symmetric key.

9. (original) The access device of claim 1 wherein the processor verifies that the reservation certificate is genuine.

10. (original) The access device of claim 1 further comprising: an identification to which the processor has access, the identification corresponding to one of the access device and the door lock, wherein the processor determines that the reservation certificate comprises data representative of the identification.

11. (original) The access device of claim 1 further comprising: a memory to which the processor has access, the memory containing a private key of the access device; wherein at least a portion of the reservation certificate is encrypted by a server using a corresponding public key for the access device and the processor decrypts the portion with the private key.

12. (amended) The access device of claim 1 wherein the processor has access to a server through the communication module and the processor reports to the server that the door lock was activated on the basis of the reservation certificate.

13. (amended) A method for use by an access device in an access control system, the method comprising:

a) accepting, by a processor through a communication module, a reservation certificate that comprises an interval of a reservation that includes at least a start time of the reservation presented with a portable terminal;

b) determining, by the processor, that the reservation certificate is current by comparing the interval to a current time accessible to the processor and determining if the current time is within the interval; and

c) activating, by the processor on the basis of the reservation certificate being current, a door lock.

14. (amended) The method of claim 13 wherein determining if the current time is within the interval comprises determining if the current time is within the start time of the reservation and a predetermined duration and wherein the certificate is current from the start time [for] up to the [a] predetermined duration.

15. (original) The method of claim 14 wherein the predetermined duration is all day.

16. (amended) The method of claim 13 wherein the interval of the reservation certificate further comprises [data representative of] a duration and the certificate is current from the start time [for] up to the duration.

17. (amended) The method of claim 18 [13] wherein the certificate is current from the start time up to the end time [the processor has access to the current time and the reservation certificate comprises data representative of an interval of the reservation, and the certificate is current for up to the interval].

18. (amended) The method of claim 13 [17] wherein the interval further comprises [is specified by a start time and one of] an end time [and a duration].

19. (original) The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a private key for which the corresponding public key is stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the public key, and the c) activating is on the further basis of the reservation certificate being genuine.

20. (original) The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a symmetric key stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the symmetric key, and the c) activating is on the further basis of the reservation certificate being genuine.

21. (original) The method of claim 13 wherein the b) determining by the processor is further that the reservation certificate is genuine, and the c) activating is on the further basis of the reservation certificate being genuine.

22. (original) The method of claim 13 wherein the processor has access to an identification, the identification corresponding to one of the access device and the door lock, wherein the b) determining by the processor is further that the reservation certificate comprises data representative of the identification, and the c) activating is on the further basis of the reservation certificate comprising data representative of the identification.

23. (original) The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a public key for which the corresponding private key is stored in a memory accessible to the processor, the method further comprising the step of: d) decrypting the portion, by the processor, with the private key.

24. (original) The method of claim 13 wherein the processor has access to a server through the communication module, the method further comprising the step of: d) reporting to the server that the door lock was activated on the basis of the reservation certificate.

25. (new) The access device of claim 1, wherein, before presenting the current reservation certificate to the processor, the portable terminal receives the current reservation certificate from a reservation server, and wherein, before the reservation server sends the current reservation certificate to the portable terminal, the reservation server receives the start time of the reservation of the current reservation certificate from a user.

26. (new) The method of claim 13, further comprising:
before accepting the reservation certificate by the processor, receiving by the portable terminal the reservation certificate from a reservation server; and
before sending the reservation certificate to the portable terminal, receiving the start time of the reservation of the reservation certificate from a user by the reservation server.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Docket No. LBT0010-CON-SE
Control No. 96/000,367
Confirmation No. 7090

U.S. Patent No. 9,373,205
Art Unit: 3992
Examiner: Carlson, Jeffrey D

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

I hereby certify that this correspondence is being transmitted to the United States Patent & Trademark Office via electronic submission or facsimile on the date indicated below:

12/20/2021 /Kelly L. Kasha/
Date Kelly L. Kasha

PATENT OWNER'S STATEMENT OF THE INTERVIEW

Dear Sir/Madam:

In accordance with 37 CFR 1.560(b), the Patent Owner states that the following subject matter was discussed in the video interview (hereinafter the "Interview") conducted between the Patent Owner's representatives and the Examiners on December 13, 2021. The Patent Owner very much appreciates the Examiners' time and discussion during the interview.

Patent Owner presented the arguments provided in the Agenda attached hereto as Appendix 1.

The Examiners:

1. Found that the interval of the reservation of the claims can include a validity period of a hotel stay or any validity period of an electronic key.
2. Did not find the Patent Owner's proposal to include "a start time of the reservation" in the independent claims to be persuasive.
3. Pointed the Patent Owner to page 36 of the English translation of International Patent Application Publication No. WO 2005/017840 (hereinafter the '840 Application") as

describing how the '840 Application uses a period of validity or an expiry date in the context of a hotel door lock.

4. Reiterated that the Patent Owner could remove the rejection of the claims under 35 U.S.C. § 112 by including language such as "the processor is configured to."

Respectfully submitted,

/John R. Kasha/
John R. Kasha
Reg. No. 53,100
Attorney for the Patent Owner

Customer No. 67050
Date: December 20, 2021

APPENDIX 1 OF 1

(18 PAGES INCLUDING THIS COVER PAGE)

Agenda for Interview of App. 96/000,367 on 12/13/2021

Below are the arguments the Patent Owner intends to make in the Interview at 1:00 pm on Monday, December 13, 2021.

Claim 5

Claim 5 of the '205 Patent recites that the processor of the access device (lock) has access to the current time, the reservation certificate includes data representative of an interval of the reservation, and the lock is activated for the interval of the reservation. In other words, the lock gets the current time, receives an interval of the reservation from the certificate, and activates the lock for the interval of the reservation if the current time is within the interval of the reservation.

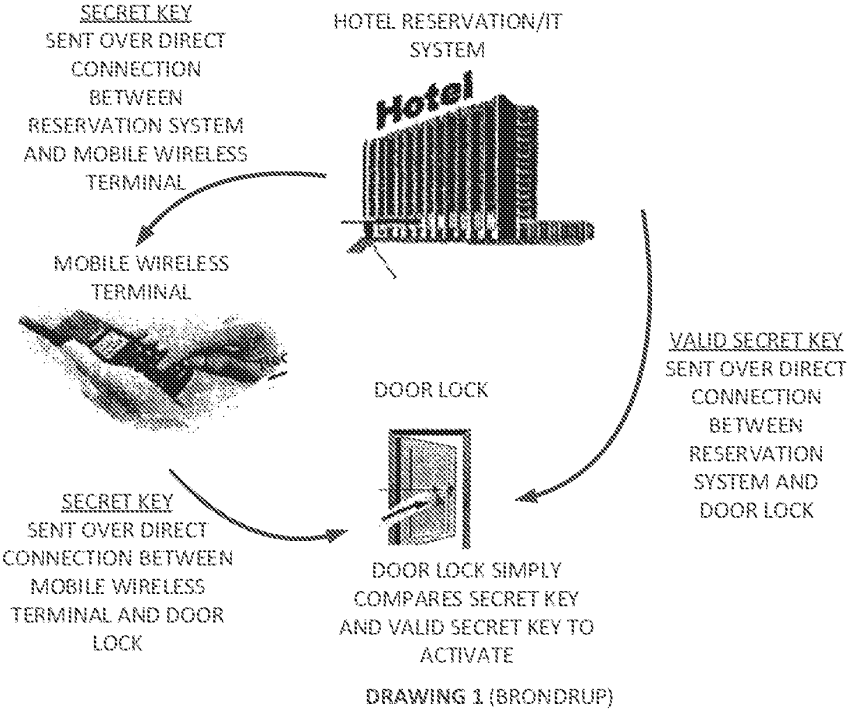
In the OA on page 13, claim 5 is rejected as being obvious over Brondrup in view of the '840 Application. The Examiner asserts that Brondrup discloses a reservation certificate that includes data "representative of" the interval of the reservation because the key token (reference number) of Brondrup is "tied to" the reservation. The Examiner admits that Brondrup does not disclose a door lock processor with access to the current time.

However, on pages 13-14 of the OA, the Examiner finds that the '840 Application suggests that its lock has access to the current time. The Examiner asserts that the '840 Application teaches a key that "can be provided with a period of validity or an expiry date in order to limit access to the room to the appropriate time interval" and a lock that "itself checks the expiration/validity period before allowing access."

The Examiner asserts that it would be obvious to combine the two references because "comparing the reservation interval with the current date/time … allows access only for a currently valid reservation. This represents an obvious alternative for determining valid

reservation status at the time of requesting access. One of ordinary skill would recognize that the lock would require access to the current time (and day) in order to 'check' the expiry of the validity period."

The Patent Owner respectfully disagrees that it would be obvious to combine Brondrup and the '840 Application's disclosure of comparing an expiry time on an electronic lock because it is an obvious alternative for determining a valid reservation status. The combination of Brondrup and the '840 Application is ***not an obvious alternative*** because the lock of Brondrup already has access to and determines the reservation status through its direct communication channel with the reservation system. Drawing 1, shown below, depicts the direct connection between the reservation system and the door lock in Brondrup.



DRAWING 1 (BRONDRUP)

Brondrup does not need to check an expiry period because it only places the valid secret key on the door lock during the interval of the reservation. Essentially, because of the second communication channel, the reservation system of Brondrup is able to keep track of the interval of the reservation rather than the lock.

In other words, the skilled person would not modify Brondrup to send an interval of the reservation with its key token to a mobile device that, in turn, sends it to a lock, and would not modify Brondrup to require its lock to compare it to a current time. The skilled person would not make this modification since ***it is superfluous to the method Brondrup currently employs***. In other words, adding this to Brondrup would increase the cost and reduce the efficiency of the method of Brondrup by providing the same information in two different ways. Currently, the lock of Brondrup simply determines if the key provided by a mobile wireless terminal matches a valid key provided by the reservation system. No timekeeping or time comparison is needed on the lock of Brondrup.

To move prosecution forward, however, the Patent Owner has further amended claim 1 of the '205 Patent to include elements of claim 5 and claim 6. As described above, claim 5 of the '205 Patent recites that the processor has access to the current time and activates the door lock during an interval of the reservation. Claim 6 of the '205 Patent recites that the interval of the reservation "is specified by a start time and one of an end time and a duration." Specifically, the Patent Owner has amended claim 1 to further recite that (1) a reservation certificate comprises an interval of a reservation that includes at least ***a start time of the reservation*** and, (2) when a current reservation certificate has been presented, the processor compares an interval of a

reservation of the current reservation certificate to a current time accessible to the processor, determines the current time is within the interval of the reservation, and activates the door lock during the interval of the reservation. Col. 5, lns. 43-47 of the '205 Patent, for example, specify that a certificate includes a "reservation start time."

In rejecting claim 6, on page 15 of the OA, the Examiner asserts that "[g]iven the obviousness laid out for claim 5, one of ordinary skill would have recognized either of 1) start time and end time or 2) start time and duration as two obvious and essentially equivalent and alternative ways to define, determine and discriminate the validity period of a user's hotel reservation for a door opening request." The Examiner essentially argues that a start time is an obvious way to define a validity period of a reservation for a door opening request.

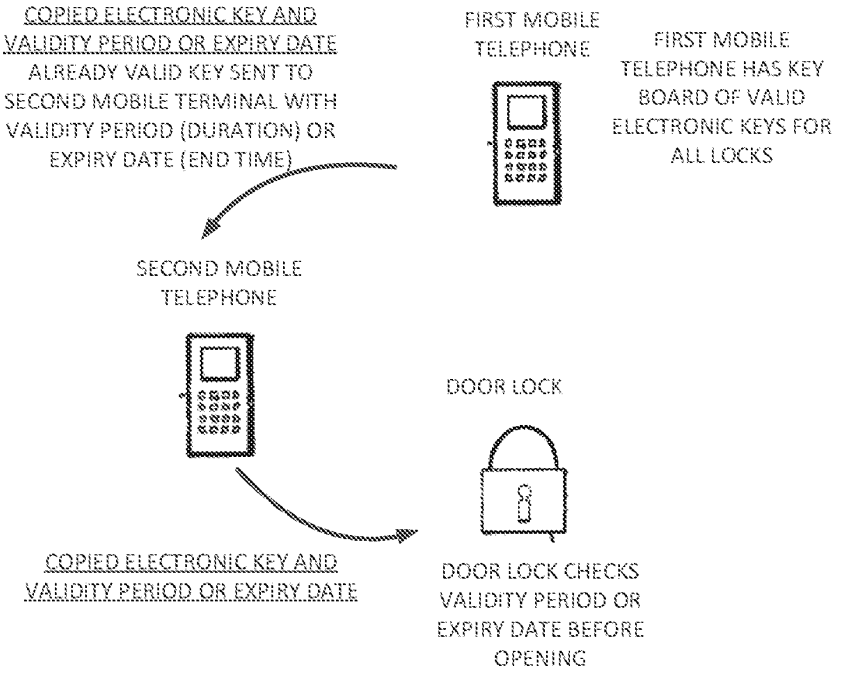
The Patent Owner submits, however, that neither Brondrup nor the '840 Application teaches or suggests providing a validity period ***of a reservation*** for a door opening request. Brondrup certainly does **not** teach or suggest providing a validity period of a reservation with a key token sent to the lock. As described above, Brondrup would not teach or suggest this because the lock of Brondrup has access to all the reservation information through its direct communication with the reservation system. The Examiner also admits that the lock of Brondrup does not have the current time, so a validity period would be of no use to Brondrup. In other words, providing a validity period of a reservation with a key token would be superfluous and useless in Brondrup.

The '840 Application also does not teach or suggest providing a validity period "of a reservation" for a door opening request. Instead, the '840 Application discloses the validity period or expiry date "of a copied key" of an already valid electronic key for opening a lock. The '840 Application ***discloses nothing about a reservation or reservation system***. Thus, the '840 Application could not possibly teach sending a reservation certificate with a start time of the reservation.

The '840 Application does disclose copying ***an already valid*** electronic key of a hotel room and determining if it is expired. The '840 Application, therefore, instead describes how "a key" is received and checked for expiration after a customer's stay or reservation at a hotel has already started. As a result, the '840 Application cannot be checking the validity period "of a reservation."

In other words, the electronic keys of the '840 Application are wireless versions of the well-known magnetic cards issued by hotels at the start of a customer's stay. These magnetic cards are referred to as "key cards" and have an expiration date just like the electronic keys of the '840 Application. These key cards do not need the start time of the reservation since they are issued when the reservation may have already started. Even if they were to have a start time, this start time would be the start time of the validity of the key and not the start time of the reservation.

Drawing 2, shown below, depicts the copying of a valid key in the '840 Application.



DRAWING 2 ('840 Application)

One of ordinary skill in the art would recognize that, in the '840 Application, the ability of one mobile phone to copy an electronic key and transfer it to another mobile phone is completely akin to the magnetic card writers copying keys onto the magnetic cards currently used by hotels. This is why, for example, a mobile phone is copying an electronic key and not a central server of the hotel's reservations system in the '840 Application. An originating mobile phone can be located in each hotel just like a magnetic card writer. A hotel customer, therefore, using either the current magnetic card writers and magnetic cards or the system of the '840 Application, has to obtain the key at the time of arrival of their stay.

In contrast, the '205 Patent is directed to an improvement in which the key includes the interval of the reservation and can, therefore, be issued before the stay. In other words, the "start

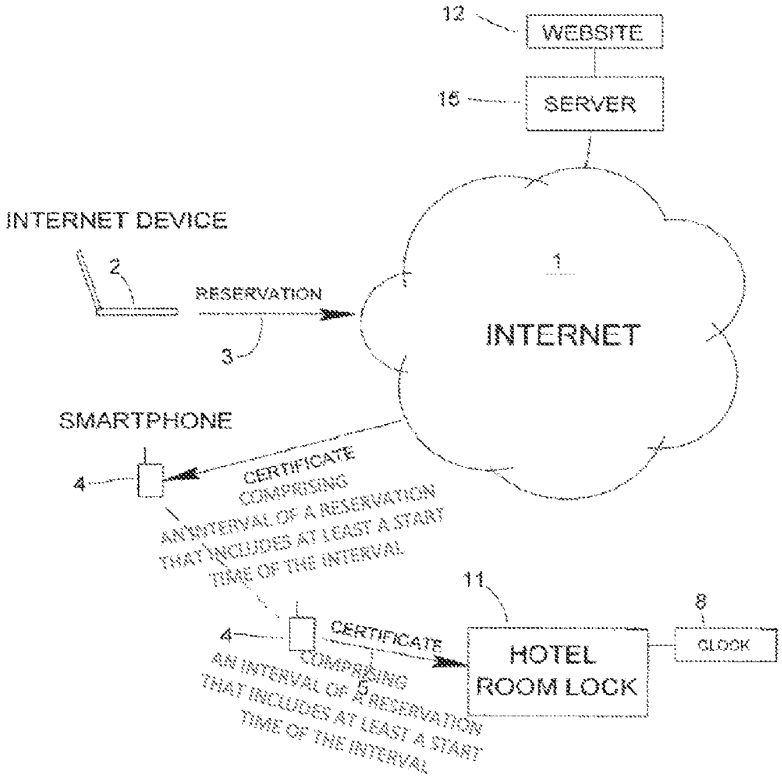
time" of the reservation makes it possible to issue a reservation certificate before the stay. The start time prevents access to the room before the reservation starts. This allows a hotel customer to bypass the hotel desk and proceed directly to their room. Essentially, this makes a hotel a self-service type business. This is a significant improvement over the current magnetic card writers and magnetic cards and the system of the '840 Application.

In summary, claim 1 is amended to recite that:

(1) a reservation certificate comprises an interval of a reservation that includes at least ***a start time of the reservation*** and,

(2) when a current reservation certificate has been presented, the processor compares an interval of a reservation of the current reservation certificate to a current time accessible to the processor, determines the current time is within the interval of the reservation, and activates the door lock during the interval of the reservation.

Annotated Figure 5 of '205 Patent, shown below, depicts how a reservation certificate that comprises an interval of a reservation that, in turn, includes at least a start time of the reservation is communicated in the '205 Patent.



ANNOTATED
FIG. 5

New claims 25 and 26, shown below, further distinguish the present application by describing how the start time of the reservation originates and is communicated. The start time of a reservation is entered by a user ahead of time. *See* the '205 Patent at col. 7, lns. 15-18. This start time is then included in the reservation certificate at creation by the reservation server, sent to the smartphone, and presented to the lock as part of the interval of the reservation. *See* the '205 Patent at col. 4, lns. 1-6 and col. 5, lns. 41-47. Neither Brondrup nor the '840 Application, either alone or in combination, describes this origination and communication of a start time.

In summary, claim 1 is allowable over Brondrup and the '840 Application because:

1. Brondrup does not teach or suggest using a reservation certificate that includes an interval of a reservation with a ***start time of the reservation*** to activate a lock because Brondrup already has access to all reservation information via its direct communication to the reservation system (the Examiner admits Brondrup has no means of determining the current time, so a start time of the reservation is of no use to Brondrup), and
2. the '840 Application does not teach or suggest using a reservation certificate that includes an interval of a reservation with a ***start time of the reservation*** to activate a lock because the '840 Application is only directed to determining the expiry of an already valid hotel key and is not directed to determining the start time of a reservation or anything about a reservation (the '840 Application could not teach or suggest the start time of the reservation since it has no access to a reservation system).

Finally, the access device of claim 1 is an improvement over Brondrup and the '840 Application because:

1. it does not require using a separate communication channel to the reservation system like Brondrup, making it less costly to implement and making it less susceptible to disruptions with the separate communication channel and, therefore, more reliable, and
2. it does not require that an electronic key be issued at the time of the customer's stay like the '840 Application, but instead allows the reservation certificate to be issued before the stay, potentially making the hotel a self-service type business.

Claim Amendments

1. (amended) An access device for use in an access control system, the access device comprising:

a processor (16) having control of a door lock (11); and a communication module (17) connected to the processor, the processor able to receive a reservation certificate (5) that comprises an interval of a reservation that includes at least a start time of the reservation presented by a portable terminal (4) through the communication module; wherein, when a current reservation certificate has been presented, the processor compares an interval of a reservation that includes a start time of the reservation of the current reservation certificate to a current time accessible to the processor, determines the current time is within the interval of the reservation, and activates the door lock during the interval of the reservation [when a current reservation certificate has been presented].

2. (amended) The access device of claim 1 wherein the processor determines the current time is within the interval of the reservation by determining if the current time is within the start time of the reservation of the reservation of the current reservation certificate and a predetermined duration and activates the door lock from the start time [for] up to the [a] predetermined duration.

3. (original) The access device of claim 2 wherein the predetermined duration is all day.

4. (amended) The access device of claim 1 wherein the interval of the reservation certificate further comprises [comprise data representative of] a duration and the processor activates the door lock from the start time of the reservation of the current reservation certificate [for] up to a [the] duration of the reservation of the current reservation certificate.

5. (amended) The access device of claim 6 [1] wherein the processor activates the door lock from the start time of the reservation of the current reservation certificate up to an end time of the reservation of the current reservation certificate [has access to the current time, the reservation certificate comprises data representative of an interval of the reservation, and the processor activates the door lock during the interval].

6. (amended) The access device of claim 1 [5] wherein the interval further comprises [is specified by a start time and one of] an end time [and a duration].

7. (original) The access device of claim 1 further comprising: a memory to which the processor has access, the memory containing a public key for a server authorized to issue the reservation certificate; wherein at least a portion of the reservation certificate is encrypted by the server using a private key and the processor verifies that the reservation

certificate is genuine by decrypting the portion with the public key.

8. (original) The access device of claim 1 further comprising: a memory to which the processor has access, the memory containing a symmetric key, wherein at least a portion of the reservation certificate is encrypted by a server using the symmetric key and the processor verifies that the reservation certificate is genuine by decrypting the portion with the symmetric key.

9. (original) The access device of claim 1 wherein the processor verifies that the reservation certificate is genuine.

10. (original) The access device of claim 1 further comprising: an identification to which the processor has access, the identification corresponding to one of the access device and the door lock, wherein the processor determines that the reservation certificate comprises data representative of the identification.

11. (original) The access device of claim 1 further comprising: a memory to which the processor has access, the memory containing a private key of the access device; wherein at least a portion of the reservation certificate is encrypted by a server using a corresponding public key for the access device and the processor decrypts the portion with the private key.

12. (amended) The access device of claim 1 wherein the processor has access to a server through the communication module and the processor reports to the server that the door lock was activated on the basis of the reservation certificate.

13. (amended) A method for use by an access device in an access control system, the method comprising:

a) accepting, by a processor through a communication module, a reservation certificate that comprises an interval of a reservation that includes at least a start time of the reservation presented with a portable terminal;

b) determining, by the processor, that the reservation certificate is current by comparing the interval to a current time accessible to the processor and determining if the current time is within the interval; and

c) activating, by the processor on the basis of the reservation certificate being current, a door lock.

14. (amended) The method of claim 13 wherein determining if the current time is within the interval comprises determining if the current time is within the start time of the reservation and a predetermined duration and wherein the certificate is current from the start time [for] up to the [a] predetermined duration.

15. (original) The method of claim 14 wherein the predetermined duration is all day.

16. (amended) The method of claim 13 wherein the interval of the reservation certificate further comprises [data representative of] a duration and the certificate is current from the start time [for] up to the duration.

17. (amended) The method of claim 18 [13] wherein the certificate is current from the start time up to the end time [the processor has access to the current time and the reservation certificate comprises data representative of an interval of the reservation, and the certificate is current for up to the interval].

18. (amended) The method of claim 13 [17] wherein the interval further comprises [is specified by a start time and one of] an end time [and a duration].

19. (original) The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a private key for which the corresponding public key is stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the public key, and the c) activating is on the further basis of the reservation certificate being genuine.

20. (original) The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a symmetric key stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the symmetric key, and the c) activating is on the further basis of the reservation certificate being genuine.

21. (original) The method of claim 13 wherein the b) determining by the processor is further that the reservation certificate is genuine, and the c) activating is on the further basis of the reservation certificate being genuine.

22. (original) The method of claim 13 wherein the processor has access to an identification, the identification corresponding to one of the access device and the door lock, wherein the b) determining by the processor is further that the reservation certificate comprises data representative of the identification, and the c) activating is on the further basis of the reservation certificate comprising data representative of the identification.

23. (original) The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a public key for which the corresponding private key is stored in a memory accessible to the processor, the method further comprising the step of: d) decrypting the portion, by the processor, with the private key.

24. (original) The method of claim 13 wherein the processor has access to a server through the communication module, the method further comprising the step of: d) reporting to the server that the door lock was activated on the basis of the reservation certificate.

25. (new) The access device of claim 1, wherein, before presenting the current reservation certificate to the processor, the portable terminal receives the current reservation certificate from a reservation server, and wherein, before the reservation server sends the current reservation certificate to the portable terminal, the reservation server receives the start time of the reservation of the current reservation certificate from a user.

26. (new) The method of claim 13, further comprising:
before accepting the reservation certificate by the processor, receiving by the portable terminal the reservation certificate from a reservation server; and
before sending the reservation certificate to the portable terminal, receiving the start time of the reservation of the reservation certificate from a user by the reservation server.

Electronic Acknowledgement Receipt	
EFS ID:	44560962
Application Number:	96000367
International Application Number:	
Confirmation Number:	7090
Title of Invention:	Access Control System and Method for Use by an Access Device
First Named Inventor/Applicant Name:	9373205
Customer Number:	67050
Filer:	John Kasha
Filer Authorized By:	
Attorney Docket Number:	LBT0010-CON-SE
Receipt Date:	20-DEC-2021
Filing Date:	04-AUG-2021
Time Stamp:	13:21:18
Application Type:	Supplemental Examination
Patent Number:	

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-CON-SE_amendment_12_20_2021.pdf	454318 810f129d4d2adf32b054b8a57a6479245c7b485d	no	29
Warnings:					
Information:					
2	Applicant summary of interview with examiner	LBT0010-CON-SE_po_stmt_of_int_12_20_2021.pdf	415991 02766c185d1a7b4d852ce59dedd483ee69e81da4	no	20
Warnings:					
Information:					
		Total Files Size (in bytes):	870309		

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.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Docket No. LBT0010-CON-SE
Control No. 96/000,367
Confirmation No. 7090

U.S. Patent No. 9,373,205
Art Unit: 3992
Examiner: Carlson, Jeffrey D

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

I hereby certify that this correspondence is being transmitted to the United States Patent & Trademark Office via electronic submission or facsimile on the date indicated below:

12/20/2021 /Kelly L. Kasha/
Date Kelly L. Kasha

AMENDMENT

Dear Sir/Madam:

In response to the Non-Final Office Action mailed October 18, 2021 (hereinafter the "NFOA"), the Patent Owner submits the following amendment:

In The Claims:

Please amend the claims as follows:

1. (amended) An access device for use in an access control system, the access device comprising:

a processor (16) having control of a door lock (11); and a communication module (17) connected to the processor, the processor is configured to[able to] receive a reservation certificate (5) presented by a portable terminal (4) through the communication module;

wherein, when a current reservation certificate that comprises an interval of a reservation is presented by the portable terminal, the processor is configured to compare the interval of the reservation of the current reservation certificate to a current time accessible to the processor, determine the current time is within the interval of the reservation, and activate[s] the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation[when a current reservation certificate has been presented].

2. (amended) The access device of claim 1 wherein the processor is configured to determine the current time is within the interval of the reservation by determining if the current time is within a start time of the interval of the reservation of the current reservation certificate and a predetermined duration and is configured to activate[s] the door lock to allow the portable terminal to unlock the door lock from the start time[for] up to the[a] predetermined duration.

3. (amended) The access device of claim 2 wherein the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation from the start time up to the predetermined duration that is all day.

4. (amended) The access device of claim 1 wherein the interval of the reservation of the current reservation certificate comprises a start time and [comprise data representative of] a duration and the processor is configured to activate[s] the door lock to allow the portable terminal to unlock the door lock from the start time [for] up to the duration.

5. (amended) The access device of claim 6 [1] wherein the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the end time[has access to the current time, the reservation certificate comprises data representative of an interval of the reservation, and the processor activates the door lock during the interval].

6. (amended) The access device of claim 1 [5] wherein the interval of the reservation of the current reservation certificate comprises a start time and [is specified by a start time and one of] an end time [and a duration].

7. (amended) The access device of claim 1 further comprising:

a memory to which the processor has access, the memory is configured to comprise [containing] a public key for a server of the access system configured [authorized] to issue the current reservation certificate;

wherein at least a portion of the current reservation certificate is encrypted by the server using a private key and the processor is configured to verify [verifies] that the current reservation certificate is genuine by decrypting the portion with the public key.

8. (amended) The access device of claim 1 further comprising:

a memory to which the processor has access, the memory is configured to comprise [containing] a symmetric key;

wherein at least a portion of the current reservation certificate is encrypted by a server of the access system configured configured to use [using] the symmetric key and the processor is configured to verify [verifies] that the current reservation certificate is genuine by decrypting the portion with the symmetric key.

9. (amended) The access device of claim 1 wherein the processor is configured to verify [verifies] that the current reservation certificate is genuine.

10. (amended) The access device of claim 1 further comprising:

an identification to which the processor has access, the identification corresponding to one of the access device and the door lock, wherein the processor is configured to determine [determines] that the current reservation certificate comprises data representative of the identification.

11. (amended) The access device of claim 1 further comprising:

a memory to which the processor has access, the memory is configured to comprise [containing] a private key of the access device;

wherein at least a portion of the current reservation certificate is encrypted by a server of the access system configured to use [using] a corresponding public key for the access device and the processor is configured to decrypt [decrypts] the portion with the private key.

12. (amended) The access device of claim 1 wherein the processor has access to a server of the access system through the communication module and the processor is configured to report [reports] to the server that the door lock was activated on the basis of the current reservation certificate.

13. (amended) A method for use by an access device in an access control system, the method comprising:

a) accepting, by a processor through a communication module, a reservation certificate that comprises an interval of a reservation presented with a portable terminal;

b) determining, by the processor, that the reservation certificate presented by the portable terminal is current by comparing the interval of the reservation to a current time accessible to the processor and determining if the current time is within the interval of the reservation; and

c) activating, by the processor on the basis of the reservation certificate being current, a door lock to allow the portable terminal to unlock the door lock during the interval of the

reservation.

14. (amended) The method of claim 13 wherein determining if the current time is within the interval of the reservation comprises determining if the current time is within a start time of the interval of the reservation and a predetermined duration and wherein the certificate is current from the start time [for] up to the [a] predetermined duration.

15. (original) The method of claim 14 wherein the predetermined duration is all day.

16. (amended) The method of claim 13 wherein the interval of the reservation of the reservation certificate further comprises [data representative of] a start time and a duration and the reservation certificate is current from the start time [for] up to the duration.

17. (amended) The method of claim 18 [13] wherein the reservation certificate is current from the start time up to the end time [the processor has access to the current time and the reservation certificate comprises data representative of an interval of the reservation, and the certificate is current for up to the interval].

18. (amended) The method of claim 13 [17] wherein the interval of the reservation comprises a start time and [is specified by a start time and one of] an end time [and a duration].

19. (original) The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a private key for which the corresponding public key is stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the public key, and the c) activating is on the further basis of the reservation certificate being genuine.

20. (original) The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a symmetric key stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the symmetric key, and the c) activating is on the further basis of the reservation certificate being genuine.

21. (original) The method of claim 13 wherein the b) determining by the processor is further that the reservation certificate is genuine, and the c) activating is on the further basis of the reservation certificate being genuine.

22. (original) The method of claim 13 wherein the processor has access to an identification, the identification corresponding to one of the access device and the door lock, wherein the b) determining by the processor is further that the reservation certificate comprises data representative of the identification, and the c) activating is on the further basis of the reservation certificate comprising data representative of the identification.

23. (original) The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a public key for which the corresponding private key is stored in a memory accessible to the processor, the method further comprising the step of: d) decrypting the portion, by the processor, with the private key.

24. (original) The method of claim 13 wherein the processor has access to a server through the communication module, the method further comprising the step of: d) reporting to the server that the door lock was activated on the basis of the reservation certificate.

REMARKS

Claims 1-24 of Patent No. 9,373,205 (hereinafter the "'205 Patent") are subject to reexamination. Claims 1-14 and 16-18 have been amended. No new matter has been added, and the scope of the claims has not been enlarged.

Support for the amendments to independent claims 1 and 13 can be found at least in col. 1, lns. 42-47, col. 2, lns. 17-19, col. 5, ln. 63 to col. 6, ln. 3, and Fig. 5 of the '205 Patent.

The Patent Owner thanks the Examiners for participating in the video interview (hereinafter the "Interview") held on December 13, 2021. A summary of the Interview (hereinafter the "Interview Summary") is submitted herewith on a separate paper.

As described in the Interview Summary, the Examiners found that the "interval of the reservation" of the claims can include a validity period of a hotel stay or any validity period of an electronic key. As a result, the Examiners did not find the amendments proposed in the Patent Owner's Agenda attached to the Interview Summary to be persuasive. Consequently, the Patent Owner hereby withdraws the amendments and arguments presented in the Patent Owner's Agenda attached to the Interview Summary.

However, as described in the Interview Summary, the Examiners did point the Patent Owner to page 36 of the English translation of International Patent Application Publication No. WO 2005/017840 (hereinafter the "'840 Application") as describing how the '840 Application uses a period of validity or an expiry date in the context of a door lock. The Patent Owner thanks the Examiners for directing the Patent Owner's attention to this section of the '840 Application. As described below, the Patent Owner's review of page 36 of the '840 Application provided the basis for the Patent Owner's amendments and arguments provided herein.

In light of the Patent Owner's amendments and arguments provided below, the Patent Owner respectfully requests that a certificate of reexamination be issued confirming the patentability of the '205 Patent.

Claim Rejections under 35 U.S.C. § 112

On page 2, the NFOA rejects claims 1-12 as being indefinite. The NFOA finds these claims confusing in their claim scope for their apparent method steps. The NFOA recommends using language such as "the processor is configured to." The Patent Owner thanks the NFOA for the suggestion. The Patent Owner has amended claims 1-12 to include the suggested language.

Withdrawal of the rejection under 35 U.S.C. § 112 is respectfully requested.

Original Dependent Claim 5

Original dependent claim 5 of the '205 Patent recited that (i) the processor of the access device (lock) has access to the current time, (ii) the reservation certificate includes data representative of an interval of the reservation, and (iii) the lock is activated for the interval of the reservation. In other words, the lock gets the current time, receives an interval of the reservation from the certificate, and activates the lock for the interval of the reservation if the current time is within the interval of the reservation.

On page 13, the NFOA asserts that claim 5 is unpatentable over U.S. Patent Application Publication No. US 2003/0208386 (hereinafter "Brondrup") in view of the '840 Application. The NFOA asserts that Brondrup discloses a reservation certificate that includes data "representative of" the interval of the reservation because the key token (reference number) of Brondrup is "tied to" the reservation. The NFOA admits that Brondrup does not disclose a door lock processor with access to the current time.

However, on pages 13-14, the NFOA finds that the '840 Application suggests that its lock has access to the current time. The NFOA asserts that the '840 Application teaches a key that "can be provided with a period of validity or an expiry date in order to limit access to the room to the appropriate time interval" and a lock that "itself checks the expiration/validity period before allowing access."

The NFOA asserts that it would be obvious to combine the two references because "comparing the reservation interval with the current date/time … allows access only for a currently valid reservation. This represents an obvious alternative for determining valid reservation status at the time of requesting access. One of ordinary skill would recognize that the lock would require access to the current time (and day) in order to 'check' the expiry of the validity period."

No Motivation to Combine

The Patent Owner respectfully disagrees that it would be obvious to combine Brondrup and the '840 Application's disclosure of comparing an expiry time on an electronic lock because it is an obvious alternative for determining a valid reservation status. The combination of Brondrup and the '840 Application is ***not an obvious alternative*** because the lock of Brondrup already has access to and determines the reservation status through its direct (second) communication channel with the reservation system.

Annotated Fig. 3 of Brondrup, shown below, depicts the direct connection between the reservation system and the door lock in Brondrup. Brondrup does not need to check an expiry period because it only places the valid secret key on the door lock during the interval of the reservation. Essentially, because of the second communication channel, the reservation system of Brondrup can keep track of the interval of the reservation rather than the lock.

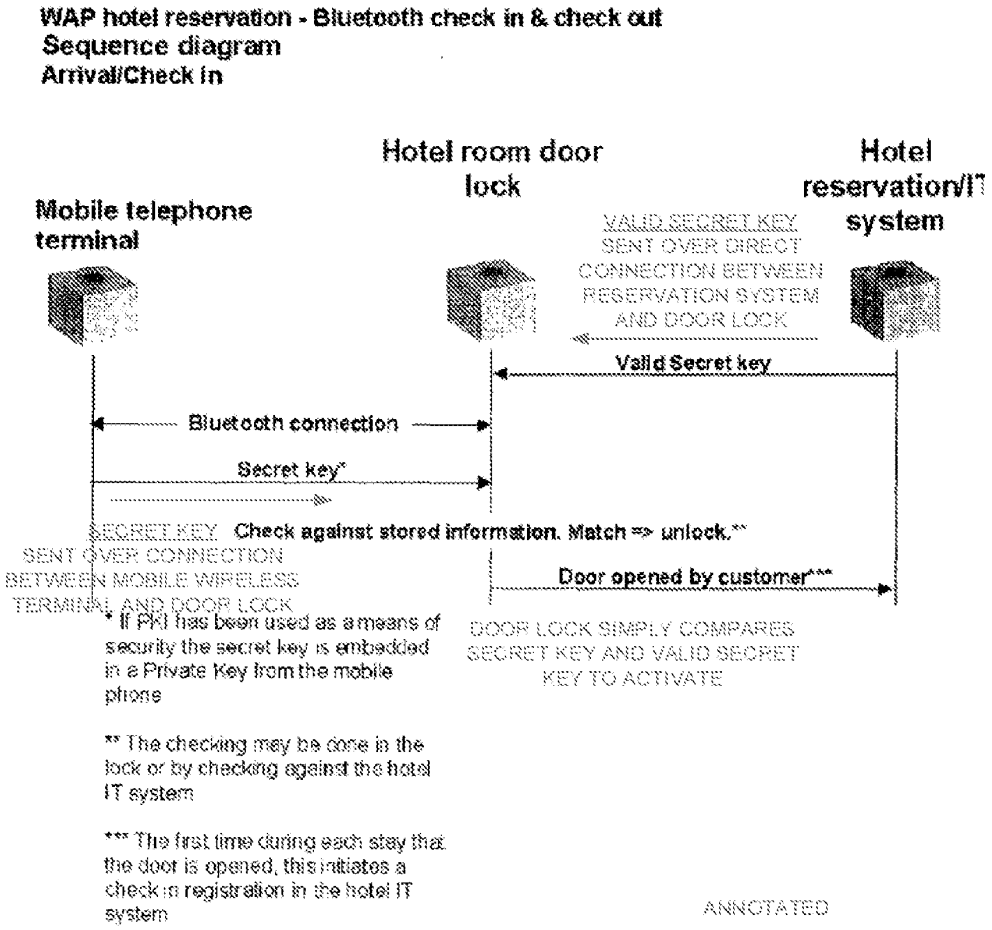


Fig. 3

In other words, the skilled person would not modify Brondrup to send an interval of the reservation with its key token to a mobile device that, in turn, sends it to a lock, and would not modify Brondrup to require its lock to compare it to a current time. The skilled person would not make this modification since ***it is superfluous to the method Brondrup currently employs***. In other words, adding this to Brondrup would increase the cost and reduce the efficiency of the method of Brondrup by providing the same information in two different ways. Currently, the

lock of Brondrup simply determines if the key provided by a mobile wireless terminal matches a valid key provided by the reservation system. No timekeeping or time comparison is needed on the lock of Brondrup.

The NFOA states that it would be obvious to combine the two references because the combination is an obvious alternative for determining valid reservation status. However, the NFOA provides no clear articulation of the reasons(s) why the claimed invention would have been obvious as required by MPEP § 2141 (III). As described in MPEP § 2143 quoting In re Os, 844 F.3d 1359, 1361, 121 USPQ2d 1209, 1211 (Fed. Cir. 2017), "[a]absent some articulated rationale, a finding that a combination of prior art would have been 'common sense' or 'intuitive' is no different than merely stating the combination 'would have been obvious.'"

Independent Claim 1 Amendments

To move prosecution forward, however, the Patent Owner has further amended claim 1 of the '205 Patent to include all the elements of claim 5 and to include additional elements to further distinguish the elements of claim 5 over Brondrup and the '840 Application. First of all, original dependent claim 5 of the patent recited that the reservation certificate comprises "data representative of" an interval of a reservation.

Claim 1 is amended to affirmatively recite that the current reservation certificate comprises an interval of a reservation. In other words, the "data representative of" language of original claim 5 is removed. Support for the direct inclusion of an interval of the reservation within a reservation certificate can be found in at least col. 2, lns. 17-19 of the '205 Patent.

Secondly, claim 1 is amended to recite that, when a current reservation certificate is presented by the portable terminal, the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation. Original

claim 1 of the patent did not describe allowing the same portable terminal to "unlock" the door lock during the interval of the reservation. Instead, original claim 1 of the patent recited only that the processor "activates" the door lock when a current reservation certificate has been presented. Support for allowing the same portable terminal that sends the interval of the reservation to also "unlock" the door lock during the interval of the reservation can be found in at least col. 1, lns. 42-47, col. 5, ln. 63 to col. 6, ln. 3, and Fig. 5 of the '205 Patent.

Together the elements added to claim 1, in addition to the elements of claim 5, provide that, (1) when a portable terminal presents a current reservation certificate that includes an interval of the reservation to a processor of an access device, (2) the processor is configured to activate the door lock to allow the same portable terminal to unlock the door lock the processor controls during the interval of the reservation.

Additional Elements Do Not Enlarge the Scope of Claim 1

MPEP § 2258 (III) provides that claims in a reexamination proceeding must not enlarge the scope of the claims. MPEP § 2258 (III)(A) describes that "[a] claim presented in a reexamination proceeding 'enlarges the scope' of the claims of the patent being reexamined where the claim is broader than each and every claim of the patent."

The Patent Owner submits that the two elements added to amended claim 1 in addition to the elements of original dependent claim 5 of the patent do not broaden amended claim 1 so that it is broader than each and every claim of the patent. On the contrary, the Patent Owner submits that the two elements added to amended claim 1 only narrow the claim in comparison to each and every claim of the patent.

Specifically, additional element (1) of amended claim 1 narrows the claim with respect to original dependent claim 5 of the patent. As described above, original dependent claim 5 of the

patent recited that a reservation certificate includes "data representative of" an interval of a reservation. Because including an interval of a reservation is narrower than including data representative of an interval of a reservation, element (1) of amended claim 1 only narrows the claim with respect to original dependent claim 5 of the patent.

The Patent Owner further notes that, on page 13, the NFOA essentially admits that the language "comprising data representative of an interval of a reservation" allows a broader interpretation than just the language "comprising an interval of a reservation" would. Specifically, NFOA describes that the "key token" of Brondrup is interpreted as comprising data representing a reservation interval because the reservation it "is tied to" includes an interval of the reservation through its connection to the reservation system.

Regarding additional element (2) of amended claim 1, this element also narrows the claim with respect to original claim 1 of the patent. Additional element (2) recites activating the door lock to allow the portable terminal to unlock the door lock the processor controls during the interval of the reservation. In contrast, original claim 1 of the patent simply recited activating the door lock. Because further describing the type of door lock activation is narrower than simply reciting activating the door lock, element (2) of amended claim 1 narrows the claim with respect to original claim 1 of the patent. Because additional element (2) of amended claim 1 narrows the claim with respect to original claim 1 of the patent, additional element (2) does not enlarge the scope of amended claim 1.

Additional Elements of Claim 1 are Allowable over Brondrup and the '840 Application

As described above, original dependent claim 5 of the '205 Patent recited that the processor has access to the current time, the reservation certificate comprises data representative of an interval of the reservation, and the processor activates the door lock during the interval.

Amended claim 1 includes these elements and further narrows them to recite that, when the current reservation certificate that comprises an interval of the reservation is presented by the portable terminal, the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation. In other words, the ***"data representative"*** language of original claim 5 of the patent ***is removed*** in amended claim 1. Further, the language of original claim 5 of the patent is amended in claim 1 to describe that the door lock is activated ***to allow the portable terminal to unlock the door lock during the interval of the reservation***.

As described above, on page 13, the NFOA admits that Brondrup does not have access to the current time. Also on this page, the NFOA describes that the "key token" of Brondrup is interpreted as comprising data representing a reservation interval because the reservation it "is tied to" includes an interval of the reservation through its connection to the reservation system. Thus, the NFOA essentially acknowledges that Brondrup does not teach or suggest sending a key token that comprises an interval of the reservation or having access to the current time as recited in amended claim 1.

Therefore, Brondrup does not teach or suggest that, (1) when a portable terminal presents a current reservation certificate that includes an interval of the reservation to a processor of an access device, (2) the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock the processor controls during the interval of the reservation. A current reservation certificate is one for which it is determined that the current time is within the interval of the reservation of the current reservation certificate as recited in amended claim 1.

As described above, on page 13, the NFOA, however, asserts that the '840 Application teaches its electronic key "can be provided with a period of validity or expiry date in order to

limit access to the room to an appropriate time interval." Thus, regarding original dependent claim 5 of the patent, the NFOA asserts that the '840 Application discloses both sending an electronic key that comprises an interval of the reservation and having access to the current time.

The Patent Owner agrees that the '840 Application does disclose sending a period of validity or expiry date with a copied electronic key from a "controlling" mobile telephone to a door lock. However, the '840 Application discloses that

(A) the controlling mobile telephone sending the period of validity or expiry date with the copied electronic key is ***not*** sending this to unlock the door lock for itself, and

(B) the period of validity or expiry date compared to the current time is ***not*** sent by any other mobile telephone actually requesting to be allowed to unlock the door lock.

More simply, the '840 Application discloses that a controlling mobile telephone already communicating with a door lock, based on authentication, places a period of validity or expiry date with a copied electronic key.

This is done to provide locking authorization for ***another*** mobile telephone. The controlling mobile telephone, already communicating with the door lock, sends the copied key to the ***other*** mobile telephone. The ***other*** mobile telephone then can unlock the lock by ***sending only the copied key*** to the lock. The lock compares the copied key to the copied key on the lock, finds that the copied key on the lock has the period of validity or expiry date, and compares the period of validity or expiry date already on the lock to the current time to determine if the ***other*** mobile telephone should be allowed to unlock the lock.

Therefore, the Patent Owner submits that the '840 Application does ***not*** teach or suggest that,

(1) when ***a portable terminal*** presents a current reservation certificate that includes an interval of the reservation to a processor of an access device,

(2) the processor is configured to activate the door lock to allow ***the same portable terminal*** to unlock the door lock the processor controls during the interval of the reservation.

Again, a current reservation certificate is one for which it is determined that the current time is within the interval of the reservation of the current reservation certificate as recited in amended claim 1.

Period of Validity or an Expiry Date on Page 36 and in Figure 1 of the '840 Application

As described in the Interview Summary, in the Interview, the Examiner directed the Patent Owner to page 36 of the '840 Application for the disclosure of both sending an electronic key that comprises an interval of the reservation and having access to the current time. The Patent Owner thanks the Examiner for directing the Patent Owner's attention to this section. This section provides the clearest explanation of the purpose and use of a period of validity or an expiry date in the '840 Application. It provides the clearest explanation because the description is in conjunction with the only figure, Figure 1, of the '840 Application, which shows all of the components and their communication.

Annotated Figure 1 of the '840 Application is shown below. On pages 34-35, the '840 Application provides that "the mobile telephones 10, 12, and 14 each contain an electronic key board with a plurality of electronic keys." So presumably, mobile telephone 10 can have, for

example, keys 51 and 52, and mobile telephone 12 can have, for example, keys 121 and 122, as shown in Annotated Figure 1.

On page 35, the '840 Application describes that to "control the closed state of the lock 20, the mobile telephone 10 establishes a bidirectional communication connection to the electronic lock 20" that "allows conventional authentication methods." So essentially, mobile telephone 10 controls and accesses lock through bidirectional communication and authentication. Then, mobile telephone 10 is able to control lock 20 just like the reservation system of Brondrup controls the lock of Brondrup. On this page, the '840 Application further outlines a first use case in which mobile telephone 10 queries the closed state of lock 20 and a second use case where mobile telephone 10 queries the location of lock 20.

On page 36 of the '840 Application, a third use case describes the operation of an electronic key in conjunction with a period of validity or expiry:

> The transfer of the locking authorization for the lock 20 to another mobile phone 12 is illustrated as a third use case. For this purpose, after prior identification and / or authentication of the other mobile telephone 12, an electronic copy of the key is made and transmitted to the other mobile telephone 12 in electronic form 52 via the air interface. The copied key is provided with an expiry date which is communicated to the lock 20 by the first mobile telephone 10 (reference number 50). In the event of an attempt to access by the other mobile telephone 12, the lock 20 then first checks whether the copied key 52 is still valid. <Desc / Clms Page number 10> The electronic lock 20 can, for example, represent the lock of a hotel room door for which a hotel guest is granted the locking authorization for the duration of his stay.

So, in Annotated Figure 1 of the '840 Application, mobile telephone 10 is transferring "locking authorization for the lock 20 to another mobile telephone 12." To do this, mobile telephone 10 copies key 52, for example. First, mobile telephone 10 ***sends only copied key 52*** to mobile telephone 12 (reference number 52). Next, mobile telephone 10 ***provides*** copied key 52 with an expiry date, for example xx/xx, and communicates key 52 and expiry date xx/xx to lock 20 (reference number 50).

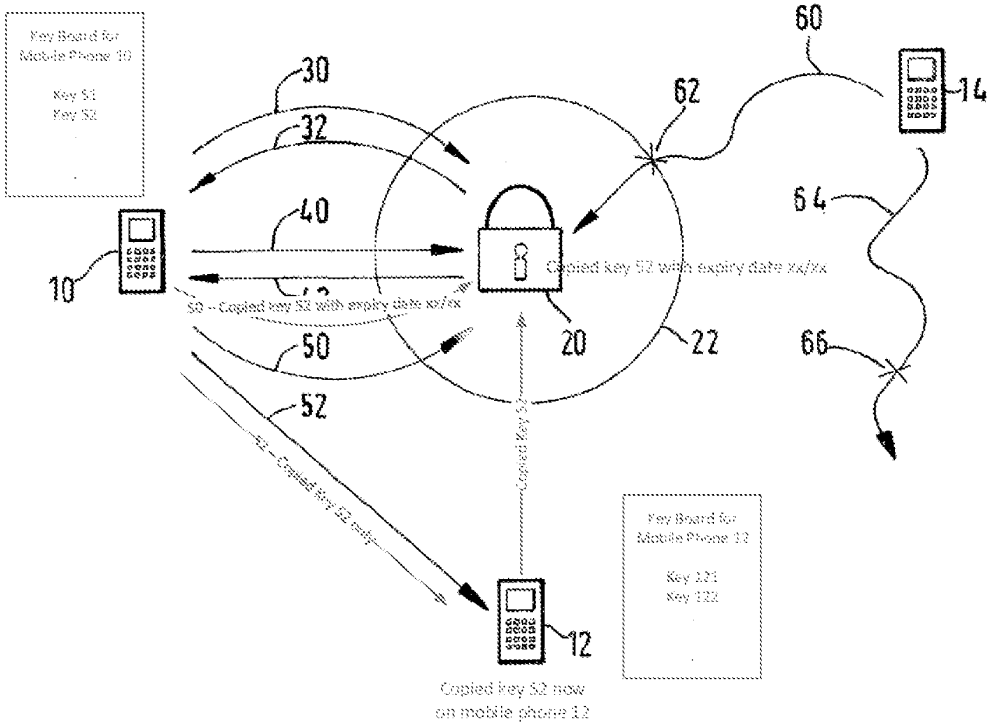
It is clear from page 36 and Figure 1 that the '840 Application does ***not*** also send the expiry date with the copied key to mobile telephone 12, and mobile telephone 12 does ***not*** send the expiry date with the copied key to lock 20. First, this is clear because the text of page 36 itself describes ***only sending copied key 52*** to mobile telephone 12 and Figure 1 depicts this communication via arrow 52 of Figure 1.

Second, this is clear because otherwise there would be ***no need*** to send the expiry date to lock 20. In other words, lock 20 would not need the expiry date if it was also receiving it from mobile telephone 12.

Third, this is clear because, if mobile telephone 12 had the expiry date, mobile phone 12 could modify it to extend the stay, or another malicious actor with access to mobile telephone 12 could modify it to extend the stay. On page 31, the '840 Application describes this latter situation. The 840 Application discloses that its lock checks the expiry date "in order to rule out manipulation of the other electronic control unit."

Returning to Annotated Figure 1 of the '840 Application, when mobile telephone 12 attempts to access lock 20, such as during a hotel stay, lock 20 checks if copied key 52, received from mobile telephone 12 (reference number 52), is valid by using expiry date xx/xx placed on lock 20 by mobile telephone 10. Consequently, lock 20 determines whether or not to activate,

when presented with an electronic key, ***not*** based on a period of validity or expiry date provided with that presented electronic key. ***Instead***, lock 20 determines whether or not to activate based on a period of validity or expiry date ***previously*** placed on lock 20 by controlling mobile telephone 10 (reference number 50). In other words, in the '840 Application, lock 20 determines whether or not to provide access based on a period of validity or expiry date ***already on*** the lock 20 and ***not based on a period of validity or expiry date presented with an electronic key by mobile telephone 12***.



In contrast to the '840 Application, the processor of amended claim 1 is configured to determine whether or not to allow ***a portable terminal*** to unlock a door lock based on an interval of the reservation ***within*** a reservation certificate ***presented by the very same portable terminal***. Thus, more specifically, unlike amended claim 1, the '840 Application does not teach or suggest

that, (1) when a portable terminal presents a current reservation certificate that includes an interval of the reservation to a processor of an access device, (2) the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock the processor controls during the interval of the reservation. Again, a current reservation certificate is one for which it is determined that the current time is within the interval of the reservation of the current reservation certificate as recited in amended claim 1.

Other Disclosures of Period of Validity or an Expiry Date in the '840 Application

Page 31, page 36, and claims 9-11 of the '840 Application all describe that a copied or transferred key can be provided with a validity period or an expiry date. Only page 36, however, describes exactly how a key copied is transferred, when a validity period or an expiry date is added to a copied key, who is sent the copied key with the validity period or expiry date, and how exactly the validity period or expiry date is used.

In other words, the disclosures on page 31 and in claims 9-11 are incomplete and, therefore, can only be construed in the context of the disclosure on page 36. The disclosures on page 31 and in claims 9-11 are also consistent with the disclosure on page 36. They cannot be construed to provide something they do not explicitly describe that also contradicts or teaches away from the disclosure on page 36 without explicitly stating that contradiction or teaching away.

For example, the disclosure on page 31 only provides that "[t]he transferred key is provided with a validity period or expiry date. The expiry of the period of validity or the reaching of the expiry time is advantageously checked by the electronic lock assigned to the transferred key in order to rule out manipulation of the other electronic control unit." These lines do not recite how the transferred key is "provided" with a period of validity or an expiry time.

They also do not describe how the expiry time is checked by the electronic lock or how the transferred key is assigned to the electronic lock.

Similarly, regarding claims 9-11 of the '840 Application, claim 9 recites that the mobile control device transfers an electronic key to another mobile device. Claim 10 recites that the transferred key is provided with a period of validity or an expiry time. Claim 11 recites that the period of validity or the expiry time is checked by the electronic lock assigned to the transferred. These claims also do not recite how the transferred key is "provided" with a period of validity or an expiry time. They also do not describe how the expiry time is checked by the electronic lock or how the transferred key is assigned to the electronic lock. The antecedent basis of "the" transferred key in claim 10 means that it is referring to claim 9. However, claim 10 does not recite that the transferred key is ***transferred with*** a period of validity or an expiry. Instead, claim 10 recites that the transferred key is ***provided with*** a period of validity or an expiry, which is not explained by claim 10.

Claim 10 does not explicitly recite how the transferred key is "provided with" a period of validity or an expiry time just like claim 11 does not recite how the electronic lock is "assigned to" the transferred key. No claim preceding claim 11 explicitly describes the assignment of the transferred key to the electronic lock. However, page 36 of '840 Application shows that the communication of the copied key with the expiry date to lock 20 is the assignment of the transferred key to the electronic lock.

In other words, the details of claims 10 and 11 of the '840 Application are provided in two back to back sentences of page 36 of the '840 Application. Thus, claims 10 and 11 are consistent with the disclosure of page 36 of the '840 Application. Specifically, the sentence of page 36 describing that "[t]he copied key is provided with an expiry date which is communicated

to the lock 20 by the first mobile telephone 10 (reference number 50)" provides details about both how the transferred key is ***provided with*** a period of validity or an expiry time in claim 10 and how the transferred key assigned to the electronic lock in claim 11 ***is assigned***. The next sentence of page 36 describing that "[i]n the event of an attempt to access by the other mobile telephone 12, the lock 20 then first checks whether the copied key 52 is still valid" provides other details about how the reaching of the expiry time ***is checked*** in claim 11.

Thus, it is also clear from the other disclosures regarding providing a copied or transferred key with a validity period or an expiry date, such as page 31 and claims 9-11 of the '840 Application, that the '840 Application does ***not*** also send the expiry date with the copied key to mobile telephone 12 and mobile telephone 12 does not send the expiry date with the copied key to lock 20.

In contrast, amended claim 1 of the '205 Patent ***can*** send an interval of the reservation from a portable terminal seeking access because the interval of the reservation is ***part of*** a reservation certificate and, therefore, harder to modify by a malicious actor.

Withdrawal of the Arguments and Amendments of the Patent Owner's Agenda

In the Patent Owner's Agenda attached to the Interview Summary on page 5, the Patent Owner likens the copied electronic key of the '840 Application to "wireless versions of the well-known magnetic cards issued by hotels" that can include an expiry date. Further, the Patent Owner provides Drawing 2 on page 6 of the Patent Owner's Agenda attached to the Interview Summary. Drawing 2 depicts a second mobile telephone of the '840 Application sending a validity period or expiry date with an electronic key to the door lock. These references and any other references in the Patent Owner's Agenda attached to the Interview Summary that suggest that the '840 Application teaches or suggests that a mobile telephone presents a validity period or

expiry date with an electronic key to the lock to allow the same mobile telephone access to open the lock ***are incorrect***.

A correct analysis of the '840 Application, as described above, shows that the only time a mobile telephone presents a validity period or expiry date with an electronic key to the lock is to authorize the lock ***for another mobile telephone***. The '840 Application does not teach or suggest that ***a mobile telephone*** presents a validity period or expiry date with an electronic key to allow ***the same mobile telephone*** that presented the validity period or expiry date to open the lock. As a result, again, the Patent Owner withdraws all the arguments and amendments proposed in the Patent Owner's Agenda attached to the Interview Summary.

Summary

Because neither Brondrup nor the '840 Application, either alone or in combination, teach or suggest that, (1) when a portable terminal presents a current reservation certificate that includes an interval of the reservation to a processor of an access device, (2) the processor is configured to activate the door lock to allow the same portable terminal to unlock the door lock the processor controls during the interval of the reservation, where the current reservation certificate is one for which it is determined that the current time is within the interval of the reservation, amended independent claim 1 is allowable over Brondrup in view of the '840 Application. More simply, Brondrup and the '840 Application simply do not teach or suggest allowing the same portable terminal that presented the reservation certificate with the interval of the reservation to unlock the door lock during that interval of the reservation as recited in amended claim 1.

Dependent claims 2-12 are allowable for the same reasons independent claim 1, from which they depend, is allowable and for the additional limitations they recite.

The independent method claim 13 is amended to include the same limitations that make claim 1 allowable. For example, amended claim 13 includes the limitations of original claim 17 of the patent, which included limitations similar to original claim 5 of the patent. As a result, amended claim 13 is allowable over Brondrup in view of the '840 Application for the same reasons as claim 1.

Dependent claims 14-24 are allowable for the same reasons independent claim 13, from which they depend, is allowable and for the additional limitations they recite.

Dependent claims 2-6, 14, and 16-18 Also Allowable based on Start Time

Original dependent claims 6 and 18 of the patent recited that the interval of the reservation included a "start time."

The NFOA did not provide a citation from either Brondrup or the '840 Application in rejecting claims 6 and 18. Instead, on page 15, the NFOA asserts that "[g]iven the obviousness laid out for claim 5, one of ordinary skill would have recognized either of 1) start time and end time or 2) start time and duration as two obvious and essentially equivalent and alternative ways to define, determine and discriminate the validity period of a user's hotel reservation for a door opening request." The NFOA appears to be relying on "common knowledge" that a start time is inherent in the secret key sent by Brondrup or in the validity period or expiry date of the '840 Application.

MPEP § 2144.03 provides that "[i]n certain circumstances where appropriate, an examiner may take official notice of facts not in the record or rely on 'common knowledge' in making a rejection, however such rejections should be judiciously applied." MPEP § 2144.03 (C) states that if an applicant traverses a factual assertion as not properly officially noticed or not

properly based on common knowledge, the examiner must support the finding with adequate evidence.

Amended dependent claims 2-6, 14, and 16-18 now recite a start time of the reservation interval. The Patent Owner hereby traverses the factual assertion on page 15 of the NFOA as not properly based on common knowledge. Specifically, the Patent Owner traverses the factual assertion that one of ordinary skill would have recognized either of 1) start time and end time or 2) start time and duration as two obvious and essentially equivalent and alternative ways to define, determine and discriminate the validity period of a user's hotel reservation for a door opening request with regard to amended dependent claims 2-6, 14, and 16-18.

As discussed in the Interview, the Patent Owner submits that the use of a "start time" is not an obvious way to define, determine, or discriminate the validity period of a door opening request. The use of a "start time" is not an obvious way to define, determine, or discriminate the validity period of a door opening request because conventionally the door opening request itself is the start time of the validity period. In other words, the door opening request itself, at the start of a stay or check-in, begins the validity period. Only in the context of the present patent where the reservation certificate with an interval of reservation can be issued before a reservation or before a stay begins is a start time necessary.

MPEP § 2144.03 (C) provides that "[i]f applicant adequately traverses the examiner's assertion of official notice, the examiner must provide documentary evidence in the next Office action if the rejection is to be maintained."

The Patent Owner submits that amended dependent claims 2-6, 14, and 16-18 are at least additionally allowable over Brondrup in view of the '840 Application because they recite a "start time."

CONCLUSION

The present amendment and response is believed to be a complete response to the issues raised in the NFOA mailed October 18, 2021. In light of the remarks herein, the Patent Owner asserts that claims 1-24 must be allowed and confirmed. If the Examiner has any questions, comments, or suggestions, the undersigned attorney earnestly requests a telephone conference.

No fees are required for filing this amendment; however, the Commissioner is authorized to charge any additional fees which may be required, or credit any overpayment, to Kasha Law LLC, Deposit Account No. 50-4075.

Respectfully submitted,

/John R. Kasha/
John R. Kasha
Reg. No. 53,100
Attorney for the Patent Owner

Customer No. 67050
Date: December 20, 2021

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
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 displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 96/000,367	Filing Date 08/04/2021	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $480 =	
☐ 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).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	12/20/2021	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 24	Minus	** 24	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0		x $480 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/RHONDA BELL/
*** 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 number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. 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 12 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.

Reexamination	Application/Control No.	Applicant(s)/Patent Under Reexamination
	96/000,367	9373205
	Certificate Date	Certificate Number

Requester Correspondence Address: ☑ Patent Owner ☐ Third Party
KASHA LAW LLC 14532 Dufief Mill Road North Potomac, MD 20878

LITIGATION REVIEW ☑	jdc (examiner initials)	(date)
Case Name		Director Initials
1:18cv3627		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER
none	

/JEFFREY D CARLSON/ Primary Examiner, Art Unit 3992	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	96/000,367	9373205
	Examiner	Art Unit
	JEFFREY D CARLSON	3992

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* 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
PE2E search - see attached	10/14/2021	jdc

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

/JEFFREY D CARLSON/ Primary Examiner, Art Unit 3992	

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.
96/000,367	08/04/2021	9373205	LBT0010-CON-SE	7090

67050 7590 01/18/2022

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

EXAMINER	
CARLSON, JEFFREY D	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
01/18/2022	PAPER

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.

EX PARTE REEXAMINATION OFFICE ACTION

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

This is a reexamination of US Patent 9,373,205. The *Ex Parte* Reexamination Order mailed 8/18/2021 indicated that a substantial new question of patentability affecting patented claims 1–24 (all claims) of the patent was raised by the request. The claims were amended 12/20/2021. Claims 1–24 are pending.

Claim Objections

Claims 5 and 6 are objected to for failing to include the proper formatting required by 37 CFR 1.520 which states:

"(d) Changes shown by markings. Any changes relative to the patent being reexamined which are made to the specification, including the claims, must include the following markings:

(1) The matter to be omitted by the reexamination proceeding must be enclosed in brackets; and

(2) The matter to be added by the reexamination proceeding must be underlined"

- Claims 5 and 6 should each underline the parent claim number added to the claims.

Claim Rejections - 35 USC § 305

Claims 13–24 are rejected under 35 U.S.C. 305 as enlarging the scope of the claim(s) of the patent being reexamined. In 35 U.S.C. 305, it is stated that "[n]o proposed amended or new claim enlarging the scope of a claim of the patent will be permitted in a reexamination proceeding... ." A claim presented in a reexamination "enlarges the scope" of the patent claim(s) where the claim is broader than any claim of the patent. A claim is broader in scope than the original claims if it contains within its scope any conceivable product or process which would not have infringed the original patent. A claim is broadened if it is broader in any one respect, even though it may be narrower in other respects.

- Claim 13 has been amended to recite "determining if the current time is within the interval of the reservation". This conditional limitation does not require that the current time be within the interval. The conditional nature of step b) does not necessarily result in the presented certificate being current or determined to be current, and therefore step c) is not necessarily performed. That the method no longer necessarily activates the door lock demonstrates broadening of patented method claim 13 and its dependent claims.
    - Changing the "if" to "that" would remove the conditional nature of the claim and would cure the improper broadening.
    - Changing the two occurrences in claim 14 of "if" to "that" would likewise remove the conditional nature of the limitations and would provide consistency between the claims.

STATEMENT OF REASONS FOR PATENTABILITY AND/OR CONFIRMATION

Claims 1–4 and 7–12 have been determined to be patentable over the prior art currently of record in this proceeding.

The following is an examiner's statement of reasons for patentability and/or confirmation of the claims found patentable in this reexamination proceeding.

Patent Owner has amended independent claim 1 and has provided reasoning why the applied items of information are insufficient to arrive at the current claim scope. Examiner agrees.

In particular, claim 1 has been amended to require at least that the processor having control of the door lock be configured to:

- receive from a requesting portable terminal, a reservation certificate including a reservation interval,
- compare the received interval to a current time,
- determine the current time to be within the interval and
- activate the door lock to unlock the lock during the interval for the requesting terminal.

Brondrup teaches a hotel door lock that can be opened via a requesting mobile phone when a current reservation is presented to the lock by the phone (Brondrup at ABSTRACT, ¶ 0036, ¶ 0026, Fig. 6). This is done by transmitting the particular token key to the particular door lock in accordance with the

reservation for check-in. Upon check-out, the particular door lock is deactivated via a key token deactivation message sent to the door lock by the system. This results in the door lock possessing an activated key token which represents a current reservation. Successfully matching a user-presented key token to a stored, active key token represents a determination that the reservation is current, that the user has checked-in and authorizes activation of the door lock so that the reservation user may unlock the door for entry as needed during the reservation interval.

Brondrup's lock does not 1) receive a reservation interval from the phone requesting entry into the room, 2) have access to the current time and 3) compare a received interval to the current time.

WO 2005017840 teaches various locks (on homes, cars) that can be opened via a requesting mobile phone A hotel door lock can be opened by a reservation holder during their particular reservation interval (WO 2005017840 at p. 31–33, 36). WO 2005017840 further teaches that an electronic key can be associated with a period of validity or expiry date in order to limit access to a particular lock during the appropriate interval, whereby the lock itself can determine whether the current time is within the interval:

"(the transferred) key is provided with a validity period or an expiry date. The expiry of the period of validity or the reaching of the expiry time is advantageously checked by the electronic lock assigned to the transferred key" (WO 2005017840 at p. 31).

WO 2005017840 however does not teach that a user requesting entry sends anything more to the lock than the key alone. The entry-requesting user in WO 2005017840 does not send a reservation interval to the lock requested to be opened. The only teachings concerning expiry/validity/intervals are in the context of a user who is authorized to transfer a copy of a key to a second user. In this use case, a validity period (perhaps defined by the authorized first user) is "communicated to the lock 20 by the first mobile telephone 10 (reference number 50)" (WO 2005017840 at p. 36, Fig. 1). The entry-requesting second user therefore has no need to transmit a validity period/interval to the lock, given that the lock already has the validity period/interval as provided by the first user. The entry-requesting second user does not appear to possess the validity period/interval such that it can be transmitted to the lock.

Conclusion

Patent owner's amendment necessitated the new grounds of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

A shortened statutory period for response to this action is set to expire two months from the mailing date of this action.

Extensions of time under 37 CFR 1.136(a) do not apply in reexamination proceedings. The provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Further, in 35 U.S.C. 305 and in 37 CFR 1.550(a), it is required that reexamination proceedings "will be conducted with special dispatch within the Office."

Extensions of time in reexamination proceedings are provided for in 37 CFR 1.550(c). A request for extension of time must specify the requested period of extension and it must be accompanied by the petition fee set forth in 37 CFR 1.17(g). Any request for an extension in a third party requested ex parte reexamination must be filed on or before the day on which action by the patent owner is due, and the mere filing of a request will not effect any extension of time. A request for an extension of time in a third party requested ex parte reexamination will be granted only for sufficient cause, and for a reasonable time specified. Any request for extension in a patent owner requested ex parte reexamination (including reexamination ordered under 35 U.S.C. 257) for up to two months from the time period set in the Office action must be filed no later than two months from the expiration of the time period set in the Office action. A request for an extension in a patent owner requested ex parte reexamination for more than two months from the time period set in the Office action must be filed on or before the day on which action by the patent owner is due, and the mere filing of a request for an extension for more than two months will not

effect the extension. The time for taking action in a patent owner requested ex parte reexamination will not be extended for more than two months from the time period set in the Office action in the absence of sufficient cause or for more than a reasonable time.

The filing of a timely first response to this final rejection will be construed as including a request to extend the shortened statutory period for an additional two months. In no event, however, will the statutory period for response expire later than SIX MONTHS from the mailing date of the final action. See MPEP § 2265.

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the Patent throughout the course of this reexamination proceeding. The third party requester (if any) is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

All correspondence relating to this ex parte reexamination proceeding should be directed:

By Mail to: Mail Stop *Ex Parte* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450

Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at:

https://efs.uspto.gov/efile/myportal/efs-registered

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Any inquiry concerning this communication should be directed to **the Central Reexamination Unit** at telephone number **517-272-7705.**

/JEFFREY D CARLSON/
Primary Examiner, Art Unit 3992

Conferees:

/SAMUEL G RIMELL/
Primary Examiner, Art Unit 3992

/M.F/
Supervisory Patent Examiner, Art Unit 3992

Office Action in Ex Parte Reexamination	**Control No.** 96/000,367	**Patent Under Reexamination** 9373205	
	Examiner JEFFREY D CARLSON	**Art Unit** 3992	**AIA (FITF) Status** No

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

a. ☑ Responsive to the communication(s) filed on 20 December 2021.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

b. ☑ This action is made FINAL.

c. ☐ A statement under 37 CFR 1.530 has not been received from the patent owner.

A shortened statutory period for response to this action is set to expire 2 month(s) from the mailing date of this letter. Failure to respond within the period for response will result in termination of the proceeding and issuance of an *ex parte* reexamination certificate in accordance with this action. 37 CFR 1.550(d). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).** If the period for response specified above is less than thirty (30) days, a response within the statutory minimum of thirty (30) days will be considered timely.

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. ☐ Notice of References Cited by Examiner, PTO-892.
2. ☐ Information Disclosure Statement, PTO/SB/08.
3. ☐ Interview Summary, PTO-474.
4. ☐ _____.

Part II SUMMARY OF ACTION

1a. ☑ Claims 1-24 are subject to reexamination.
1b. ☐ Claims _____ are not subject to reexamination.
2. ☐ Claims _____ have been canceled in the present reexamination proceeding.
3. ☑ Claims 1-4 and 7-12 are patentable and/or confirmed.
4. ☑ Claims 13-24 are rejected.
5. ☑ Claims 5-6 are objected to.
6. ☐ The drawings, filed on _____ are acceptable.
7. ☐ The proposed drawing correction, filed on _____ has been (7a) ☐ approved (7b) ☐ disapproved.
8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the certified copies have
   1 ☐ been received.
   2 ☐ not been received.
   3 ☐ been filed in Application No. _____.
   4 ☐ been filed in reexamination Control No. _____.
   5 ☐ been received by the International Bureau in PCT application No. _____.
   * See the attached detailed Office action for a list of the certified copies not received.
9. ☐ Since the proceeding appears to be in condition for issuance of an *ex parte* reexamination certificate except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte* Quayle, 1935 C.D. 11, 453 O.G. 213.
10. ☐ Other: _____

cc: Requester (if third party requester)

Electronic Acknowledgement Receipt	
EFS ID:	44877915
Application Number:	96000367
International Application Number:	
Confirmation Number:	7090
Title of Invention:	Access Control System and Method for Use by an Access Device
First Named Inventor/Applicant Name:	9373205
Customer Number:	67050
Filer:	John Kasha
Filer Authorized By:	
Attorney Docket Number:	LBT0010-CON-SE
Receipt Date:	31-JAN-2022
Filing Date:	04-AUG-2021
Time Stamp:	14:38:04
Application Type:	Supplemental Examination
Patent Number:	

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	Response After Final Action	LBT0010-CON-SE_af_response_01_31_2022.pdf	138749 e0116cfa42128612c8a98fa67be5e0320ecde8ec	no	10
Warnings:					
Information:					
			Total Files Size (in bytes):	138749	

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.

In The Claims:

Please amend the claims as follows:

1. (amended) An access device for use in an access control system, the access device comprising:

a processor (16) having control of a door lock (11); and a communication module (17) connected to the processor, the processor is configured to[able to] receive a reservation certificate (5) presented by a portable terminal (4) through the communication module;

wherein, when a current reservation certificate that comprises an interval of a reservation is presented by the portable terminal, the processor is configured to compare the interval of the reservation of the current reservation certificate to a current time accessible to the processor, determine the current time is within the interval of the reservation, and activate[s] the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation[when a current reservation certificate has been presented].

2. (amended) The access device of claim 1 wherein the processor is configured to determine the current time is within the interval of the reservation by determining if the current time is within a start time of the interval of the reservation of the current reservation certificate and a predetermined duration and is configured to activate[s] the door lock to allow the portable terminal to unlock the door lock from the start time[for] up to the[a] predetermined duration.

3. (amended) The access device of claim 2 wherein the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation from the start time up to the predetermined duration that is all day.

4. (amended) The access device of claim 1 wherein the interval of the reservation of the current reservation certificate comprises a start time and [comprise data representative of] a duration and the processor is configured to activate[s] the door lock to allow the portable terminal to unlock the door lock from the start time [for] up to the duration.

5. (twice amended) The access device of claim 6 [1] wherein the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the end time[has access to the current time, the reservation certificate comprises data representative of an interval of the reservation, and the processor activates the door lock during the interval].

6. (twice amended) The access device of claim 1 [5] wherein the interval of the reservation of the current reservation certificate comprises a start time and [is specified by a start time and one of] an end time [and a duration].

7. (amended) The access device of claim 1 further comprising:

a memory to which the processor has access, the memory is configured to comprise [containing] a public key for a server of the access system configured [authorized] to issue the current reservation certificate;

wherein at least a portion of the current reservation certificate is encrypted by the server using a private key and the processor is configured to verify [verifies] that the current reservation certificate is genuine by decrypting the portion with the public key.

8. (amended) The access device of claim 1 further comprising:

a memory to which the processor has access, the memory is configured to comprise [containing] a symmetric key;

wherein at least a portion of the current reservation certificate is encrypted by a server of the access system configured to use [using] the symmetric key and the processor is configured to verify [verifies] that the current reservation certificate is genuine by decrypting the portion with the symmetric key.

9. (amended) The access device of claim 1 wherein the processor is configured to verify [verifies] that the current reservation certificate is genuine.

10. (amended) The access device of claim 1 further comprising:

an identification to which the processor has access, the identification corresponding to one of the access device and the door lock, wherein the processor is configured to determine [determines] that the current reservation certificate comprises data representative of the identification.

11. (amended) The access device of claim 1 further comprising:

a memory to which the processor has access, the memory is configured to comprise [containing] a private key of the access device;

wherein at least a portion of the current reservation certificate is encrypted by a server of the access system configured to use [using] a corresponding public key for the access device and the processor is configured to decrypt [decrypts] the portion with the private key.

12. (amended) The access device of claim 1 wherein the processor has access to a server of the access system through the communication module and the processor is configured to report [reports] to the server that the door lock was activated on the basis of the current reservation certificate.

13. (twice amended) A method for use by an access device in an access control system, the method comprising:

a) accepting, by a processor through a communication module, a reservation certificate that comprises an interval of a reservation presented with a portable terminal;

b) determining, by the processor, that the reservation certificate presented by the portable terminal is current by comparing the interval of the reservation to a current time accessible to the processor and determining that the current time is within the interval of the reservation; and

c) activating, by the processor on the basis of the reservation certificate being current, a door lock to allow the portable terminal to unlock the door lock during the interval of the

reservation.

14. (twice amended) The method of claim 13 wherein determining that the current time is within the interval of the reservation comprises determining that the current time is within a start time of the interval of the reservation and a predetermined duration and wherein the certificate is current from the start time [for] up to the [a] predetermined duration.

15. (original) The method of claim 14 wherein the predetermined duration is all day.

16. (amended) The method of claim 13 wherein the interval of the reservation of the reservation certificate further comprises [data representative of] a start time and a duration and the reservation certificate is current from the start time [for] up to the duration.

17. (amended) The method of claim 18 [13] wherein the reservation certificate is current from the start time up to the end time [the processor has access to the current time and the reservation certificate comprises data representative of an interval of the reservation, and the certificate is current for up to the interval].

18. (amended) The method of claim 13 [17] wherein the interval of the reservation comprises a start time and [is specified by a start time and one of] an end time [and a duration].

19. (original) The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a private key for which the corresponding public key is stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the public key, and the c) activating is on the further basis of the reservation certificate being genuine.

20. (original) The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a symmetric key stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the symmetric key, and the c) activating is on the further basis of the reservation certificate being genuine.

21. (original) The method of claim 13 wherein the b) determining by the processor is further that the reservation certificate is genuine, and the c) activating is on the further basis of the reservation certificate being genuine.

22. (original) The method of claim 13 wherein the processor has access to an identification, the identification corresponding to one of the access device and the door lock, wherein the b) determining by the processor is further that the reservation certificate comprises data representative of the identification, and the c) activating is on the further

basis of the reservation certificate comprising data representative of the identification.

23. (original) The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a public key for which the corresponding private key is stored in a memory accessible to the processor, the method further comprising the step of: d) decrypting the portion, by the processor, with the private key.

24. (original) The method of claim 13 wherein the processor has access to a server through the communication module, the method further comprising the step of: d) reporting to the server that the door lock was activated on the basis of the reservation certificate.

REMARKS

Claims 1-24 of Patent No. 9,373,205 (hereinafter the "'205 Patent") are subject to reexamination. Claims 1-4 and 7-12 have been determined to be patentable over the prior art of record in this proceeding. By this amendment, claims 5-6 and 13-14 have been amended per the Examiner's suggestions. No new matter has been added, and the scope of the claims has not been enlarged.

In light of the Patent Owner's amendments provided below, the Patent Owner respectfully requests that a certificate of reexamination be issued confirming the patentability of claims 1-24 of the '205 Patent.

Claim Objections

On page 2, claims 5 and 6 are objected to. Specifically, the FOA states that claims 5 and 6 should each underline the parent claim number added to the claims. The Patent Owner has amended claims 5 and 6 accordingly.

Claim Rejections under 35 U.S.C. § 305

On page 3, claims 13-24 are rejected as enlarging the scope of the claims of the patent being reexamined. The Patent Owner thanks the Examiner for indicating that changing the word "if" to "that" in claims 13 and 14 would remove the conditional nature of these claims and would cure the improper broadening. These claims have been amended accordingly.

CONCLUSION

The present amendment and response is believed to be a complete response to the issues raised in the FOA mailed on January 18, 2022. In light of the remarks herein, the Patent Owner asserts that claims 1-24 must be allowed and confirmed. If the Examiner has any questions, comments, or suggestions, the undersigned attorney earnestly requests a telephone conference.

No fees are required for filing this amendment; however, the Commissioner is authorized to charge any additional fees which may be required, or credit any overpayment, to Kasha Law LLC, Deposit Account No. 50-4075.

Respectfully submitted,

/John R. Kasha/
John R. Kasha
Reg. No. 53,100
Attorney for the Patent Owner

Customer No. 67050
Date: January 31, 2022

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
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 displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 96/000,367	Filing Date 08/04/2021	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $480 =	
☐ 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).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	01/31/2022	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 24	Minus	** 24	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	*** 3	= 0		x $480 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/RHONDA BELL/
*** 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 number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. 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 12 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.

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.
96/000,367	08/04/2021	9373205	LBT0010-CON-SE	7090

67050 7590 02/08/2022

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

EXAMINER
CARLSON, JEFFREY D

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
02/08/2022	PAPER

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 Intent to Issue Ex Parte Reexamination Certificate	**Control No.** 96/000,367	**Patent Under Reexamination** 9373205	
	Examiner JEFFREY D CARLSON	**Art Unit** 3992	**AIA Status** No

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

1. ☑ Prosecution on the merits is (or remains) closed in this *ex parte* reexamination proceeding. This proceeding is subject to reopening at the initiative of the Office or upon petition. *Cf.* 37 CFR 1.313(a). A Certificate will be issued in view of
   (a) ☑ Patent owner's communication(s) filed: 31 January 2022.
   (b) ☐ Patent owner's failure to file an appropriate timely response to the Office action mailed: _____.
   (c) ☐ Patent owner's failure to timely file an Appeal Brief (37 CFR 41.31).
   (d) ☐ The decision on appeal by the ☐ Board of Patent Appeals and Interferences ☐ Court dated _____
   (e) ☐ Other: _____.
2. The Reexamination Certificate will indicate the following:
   (a) Change in the Specification: ☐ Yes ☑ No
   (b) Change in the Drawing(s): ☐ Yes ☑ No
   (c) Status of the Claim(s):
      (1) Patent claim(s) confirmed: _____.
      (2) Patent claim(s) amended (including dependent on amended claim(s)): 1-24
      (3) Patent claim(s) canceled: _____.
      (4) Newly presented claim(s) patentable: _____.
      (5) Newly presented canceled claims: _____.
      (6) Patent claim(s) ☐ previously ☐ currently disclaimed: _____
      (7) Patent claim(s) not subject to reexamination: _____.
3. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
4. ☑ Note the attached statement of reasons for patentability and/or confirmation. Any comments considered necessary by patent owner regarding reasons for patentability and/or confirmation must be submitted promptly to avoid processing delays. Such submission(s) should be labeled: "Comments On Statement of Reasons for Patentability and/or Confirmation."
5. ☐ Note attached NOTICE OF REFERENCES CITED (PTO-892).
6. ☐ Note attached LIST OF REFERENCES CITED (PTO/SB/08 or PTO/SB/08 substitute).
7. ☐ The drawing correction request filed on _____ is: ☐approved ☐disapproved.
8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐None of the certified copies have
   ☐been received.
   ☐not been received.
   ☐been filed in Application No. _____.
   ☐been filed in reexamination Control No. _____.
   ☐been received by the International Bureau in PCT Application No. _____.
   * Certified copies not received: _____.
9. ☐ Note attached Examiner's Amendment.
10. ☐ Note attached Interview Summary (PTO-474).
11. ☐ Other: _____.

All correspondence relating to this reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Office action.

/JEFFREY D CARLSON/ Primary Examiner, Art Unit 3992	/SAMUEL G RIMELL/ Primary Examiner, Art Unit 3992

cc: Requester (if third party requester)

STATEMENT OF REASONS FOR PATENTABILITY AND/OR CONFIRMATION

Claims 1–24 have been determined to be patentable over the prior art currently of record in this proceeding.

The following is an examiner's statement of reasons for patentability and/or confirmation of the claims found patentable in this reexamination proceeding.

Patent Owner has amended each independent claim and has provided reasoning (see 12/20/2021 remarks) why the applied items of information are insufficient to arrive at the current claim scope. Examiner agrees.

In particular, claim 1 has been amended to require at least that the processor having control of the door lock be configured to:

- receive from a requesting portable terminal, a reservation certificate including a reservation interval,
- compare the received interval to a current time,
- determine the current time to be within the interval and
- activate the door lock to unlock the lock during the interval for the requesting terminal.

Brondrup teaches a hotel door lock that can be opened via a requesting mobile phone when a current reservation is presented to the lock by the phone (Brondrup at ABSTRACT, ¶ 0036, ¶ 0026, Fig. 6). This is done by

transmitting the particular token key to the particular door lock in accordance with the reservation for check-in. Upon check-out, the particular door lock is deactivated via a key token deactivation message sent to the door lock by the system. This results in the door lock possessing an activated key token which represents a current reservation. Successfully matching a user-presented key token to a stored, active key token represents a determination that the reservation is current, that the user has checked-in and authorizes activation of the door lock so that the reservation user may unlock the door for entry as needed during the reservation interval.

Brondrup's lock does not 1) receive a reservation interval from the phone requesting entry into the room, 2) have access to the current time and 3) compare a received interval to the current time.

WO 2005017840 teaches various locks (on homes, cars) that can be opened via a requesting mobile phone A hotel door lock can be opened by a reservation holder during their particular reservation interval (WO 2005017840 at p. 31–33, 36). WO 2005017840 further teaches that an electronic key can be associated with a period of validity or expiry date in order to limit access to a particular lock during the appropriate interval, whereby the lock itself can determine whether the current time is within the interval:

"(the transferred) key is provided with a validity period or an expiry date. The expiry of the period of validity or the reaching of the expiry time is advantageously checked by the electronic lock assigned to the transferred key" (WO 2005017840 at p. 31).

WO 2005017840 however does not teach that a user requesting entry sends anything more to the lock than the key alone. The entry-requesting user in WO 2005017840 does not send a reservation interval to the lock requested to be opened. The only teachings concerning expiry/validity/intervals are in the context of a user who is authorized to transfer a copy of a key to a second user. In this use case, a validity period (perhaps defined by the authorized first user) is "communicated to the lock 20 by the first mobile telephone 10 (reference number 50)" (WO 2005017840 at p. 36, Fig. 1). The entry-requesting second user therefore has no need to transmit a validity period/interval to the lock, given that the lock already has the validity period/interval as provided by the first user. The entry-requesting second user does not appear to possess the validity period/interval such that it can be transmitted to the lock.

Independent claim 13 has similar requirements to claim 1 in method form. As such, claim 13 is also patentable for the same reasons as claim 1.

Any comments considered necessary by PATENT OWNER regarding the above statement must be submitted promptly to avoid processing delays.

Such submission by the patent owner should be labeled: "Comments on Statement of Reasons for Patentability and/or Confirmation" and will be placed in the reexamination file.

Conclusion

All correspondence relating to this ex parte reexamination proceeding should be directed:

By Mail to: Mail Stop *Ex Parte* Reexam
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at:

https://efs.uspto.gov/efile/myportal/efs-registered

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for

the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Any inquiry concerning this communication should be directed to **the Central Reexamination Unit** at telephone number **517-272-7705.**

/JEFFREY D CARLSON/
Primary Examiner, Art Unit 3992

Conferees:

/SAMUEL G RIMELL/
Primary Examiner, Art Unit 3992

/M.F/
Supervisory Patent Examiner, Art Unit 3992

Reexamination	Application/Control No.	Applicant(s)/Patent Under Reexamination
	96/000,367	9373205
	Certificate Date	Certificate Number
		C1

Requester Correspondence Address: ☑ Patent Owner ☐ Third Party
KASHA LAW LLC 14532 Dufief Mill Road North Potomac, MD 20878

LITIGATION REVIEW ☑	jdc (examiner initials)	03 February 2022 (date)
Case Name		Director Initials
1:18cv3627		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER
none	

/JEFFREY D CARLSON/ Primary Examiner, Art Unit 3992	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	96/000,367	9373205
	Examiner	Art Unit
	JEFFREY D CARLSON	3992

CPC						
Symbol					Type	Version
G07C	/	9	/	27	F	2020-01-01
B60L	/	53	/	57	I	2019-02-01
B60L	/	53	/	68	I	2019-02-01
B60L	/	53	/	14	I	2019-02-01
B60L	/	53	/	665	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	/	30	I	2019-02-01
B60L	/	53	/	65	I	2019-02-01
G07C	/	9	/	20	I	2020-01-01
G07C	/	9	/	29	I	2020-01-01
H04M	/	1	/	72412	I	2021-01-01
H04W	/	12	/	069	I	2021-01-01
G06Q	/	10	/	02	I	2013-01-01
G06Q	/	20	/	045	I	2013-01-01
G06Q	/	20	/	32	I	2013-01-01
G06Q	/	20	/	322	I	2013-01-01
G06Q	/	20	/	3223	I	2013-01-01
G06Q	/	20	/	3278	I	2013-01-01
G06Q	/	20	/	38215	I	2013-01-01
G06Q	/	20	/	3829	I	2013-01-01
G06Q	/	30	/	06	I	2013-01-01
G06Q	/	50	/	06	I	2013-01-01
G07F	/	5	/	26	I	2013-01-01
G07F	/	15	/	005	I	2013-01-01
H04L	/	9	/	3268	I	2013-01-01
H04L	/	63	/	0428	I	2013-01-01
H04L	/	63	/	0823	I	2013-01-01
H04L	/	9	/	3247	I	2013-01-01
H04L	/	9	/	3263	I	2013-01-01

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	24	
/JEFFREY D CARLSON/ Primary Examiner, Art Unit 3992	03 February 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	5

U.S. Patent and Trademark Office

Part of Paper No.: 20220106

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	96/000,367	9373205
	Examiner	Art Unit
	JEFFREY D CARLSON	3992

CPC						
Symbol					Type	Version
H04L	/	63	/	102	I	2013-01-01
H04W	/	12	/	08	I	2013-01-01
H04W	/	4	/	023	I	2013-01-01
H04W	/	4	/	021	I	2013-01-01
H04W	/	4	/	40	A	2018-02-01
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
G06Q	/	2240	/	00	A	2013-01-01
H04L	/	63	/	0442	A	2013-01-01
H04L	/	2209	/	84	A	2013-01-01
H04L	/	2209	/	56	A	2013-01-01
H04L	/	2209	/	80	A	2013-01-01
Y02T	/	10	/	70	A	2013-01-01
Y02T	/	10	/	7072	A	2013-01-01
Y02T	/	10	/	72	A	2013-01-01
Y02T	/	90	/	12	A	2013-01-01
Y02T	/	90	/	14	A	2013-01-01
Y02T	/	90	/	16	A	2013-01-01
Y02T	/	90	/	167	A	2013-01-01
Y04S	/	30	/	14	A	2013-01-01

CPC Combination Sets							
Symbol					Type	Set	Ranking	Version
	/		/					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	24	
/JEFFREY D CARLSON/ Primary Examiner, Art Unit 3992	03 February 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	5

U.S. Patent and Trademark Office — Part of Paper No.: 20220106

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	96/000,367	9373205
	Examiner	Art Unit
	JEFFREY D CARLSON	3992

INTERNATIONAL CLASSIFICATION				
CLAIMED				
H04L	/	9	/	32
G07C	/	9	/	00
G06Q	/	20	/	04
H04L	/	29	/	06
G07F	/	15	/	00
G07F	/	5	/	26
G06Q	/	30	/	06
G06Q	/	20	/	38
G06Q	/	20	/	32
	/		/	

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS
1	1

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

NONE (Assistant Examiner)	(Date)	Total Claims Allowed: 24	
/JEFFREY D CARLSON/ Primary Examiner, Art Unit 3992 (Primary Examiner)	03 February 2022 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 5

U.S. Patent and Trademark Office

Part of Paper No.: 20220106

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	96/000,367	9373205
	Examiner	Art Unit
	JEFFREY D CARLSON	3992

☑ 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	10	10	19	19										
2	2	11	11	20	20										
3	3	12	12	21	21										
4	4	13	13	22	22										
5	5	14	14	23	23										
6	6	15	15	24	24										
7	7	16	16												
8	8	17	17												
9	9	18	18												

NONE (Assistant Examiner)	(Date)	Total Claims Allowed: 24	
/JEFFREY D CARLSON/ Primary Examiner, Art Unit 3992 (Primary Examiner)	03 February 2022 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 5

U.S. Patent and Trademark Office

Part of Paper No.: 20220106

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	96/000,367	9373205
	Examiner	Art Unit
	JEFFREY D CARLSON	3992

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* 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
PE2E search - see attached	10/14/2021	jdc

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

/JEFFREY D CARLSON/ Primary Examiner, Art Unit 3992	

Bibliographic Data

Application No: 96/000,367

Foreign Priority claimed: ○ Yes ◉ No

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

Verified and Acknowledged: /JEFFREY D CARLSON/ (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.
08/04/2021	705	3992	LBT0010-CON-SE
RULE			

APPLICANTS

INVENTORS

9373205,

URBAN INTEL, INC., SEATTLE, WA, UNITED STATES

PATENT OWNER,

CONTINUING DATA

This application is a SER of 14603434 01/23/2015 PAT 9373205

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

13582467 is a 371 of PCT/US2011/026781 03/02/2011

PCT/US2011/026781 has PRO of 61309813 03/02/2010

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

STATE OR COUNTRY

ADDRESS

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

FILING FEE RECEIVED

$17,320

US009373205C1

(12) EX PARTE REEXAMINATION CERTIFICATE (207th)
Ex Parte Reexamination Ordered under 35 U.S.C. 257
United States Patent
Outwater et al.

(10) Number: US 9,373,205 C1
(45) Certificate Issued: *Feb. 25, 2022

(54) **ACCESS CONTROL SYSTEM AND METHOD FOR USE BY AN ACCESS DEVICE**

(71) Applicant: **Liberty PlugIns, Inc.**, Santa Barbara, CA (US)

(72) Inventors: **Chris Outwater**, Carpinteria, CA (US); **William Gibbens Redmann**, Glendale, CA (US)

(73) Assignee: **URBAN INTEL, INC.**

Supplemental Examination Request:
No. 96/000,367, Aug. 4, 2021

Reexamination Certificate for:
Patent No.: **9,373,205**
Issued: **Jun. 21, 2016**
Appl. No.: **14/603,434**
Filed: **Jan. 23, 2015**

(*) Notice: This patent is subject to a terminal disclaimer.

Related U.S. Application Data

(63) Continuation of application No. 13/582,467, filed as application No. PCT/US2011/026781 on Mar. 2, 2011, now Pat. No. 8,996,876.
(Continued)

(51) **Int. Cl.**
H04L 9/32 (2006.01)
G07C 9/00 (2020.01)
(Continued)

(52) **U.S. Cl.**
CPC ***G07C 9/27*** (2020.01); ***B60L 53/14*** (2019.02); ***B60L 53/16*** (2019.02); ***B60L 53/18*** (2019.02); ***B60L 53/30*** (2019.02); ***B60L 53/31*** (2019.02); ***B60L 53/57*** (2019.02); ***B60L 53/65*** (2019.02); ***B60L 53/665*** (2019.02); ***B60L 53/68*** (2019.02); ***G06Q 10/02*** (2013.01); ***G06Q 20/045*** (2013.01); ***G06Q 20/32*** (2013.01); ***G06Q 20/322*** (2013.01); ***G06Q 20/3223*** (2013.01); ***G06Q 20/3278*** (2013.01); ***G06Q 20/3829*** (2013.01); ***G06Q 20/38215*** (2013.01); ***G06Q 30/06*** (2013.01); ***G06Q 50/06*** (2013.01); ***G07C 9/20*** (2020.01); ***G07C 9/29*** (2020.01); ***G07F 5/26*** (2013.01); ***G07F 15/005*** (2013.01); ***H04L 9/3247*** (2013.01); ***H04L 9/3263*** (2013.01); ***H04L 9/3268*** (2013.01); ***H04L 63/0428*** (2013.01); ***H04L 63/0823*** (2013.01); ***H04L 63/102*** (2013.01); ***H04M 1/72412*** (2021.01); ***H04W 4/021*** (2013.01); ***H04W 4/023*** (2013.01); ***H04W 12/069*** (2021.01); ***H04W 12/08*** (2013.01); *B60L 2240/622* (2013.01); *B60L 2240/72* (2013.01); *B60L 2240/80* (2013.01); *B60L 2250/10* (2013.01); *G06Q 2240/00* (2013.01); *H04L 63/0442* (2013.01); *H04L 2209/56* (2013.01); *H04L 2209/80* (2013.01); *H04L 2209/84* (2013.01); *H04W 4/40* (2018.02);
(Continued)

(58) **Field of Classification Search**
None
See application file for complete search history.

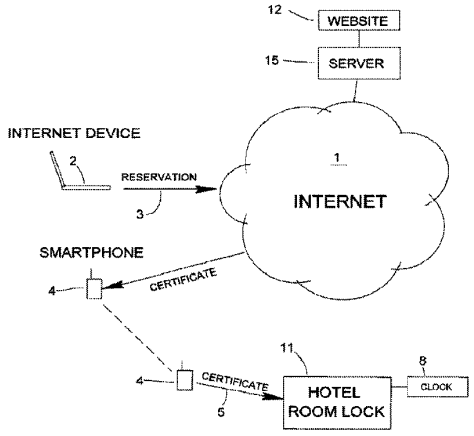
(56) **References Cited**

To view the complete listing of prior art documents cited during the supplemental examination proceeding and the resulting reexamination proceeding for Control Number 96/000,367, please refer to the USPTO's public Patent Application Information Retrieval (PAIR) system under the Display References tab.

Primary Examiner — Jeffrey D Carlson

(57) **ABSTRACT**

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
(Continued)



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.

Related U.S. Application Data

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

(51) **Int. Cl.**

G06Q 20/04	(2012.01)
H04L 29/06	(2006.01)
G07F 15/00	(2006.01)
G07F 5/26	(2006.01)
G06Q 30/06	(2012.01)
G06Q 20/38	(2012.01)
G06Q 20/32	(2012.01)
G07C 9/27	(2020.01)
B60L 53/57	(2019.01)
B60L 53/68	(2019.01)
B60L 53/14	(2019.01)
B60L 53/66	(2019.01)
B60L 53/16	(2019.01)
B60L 53/31	(2019.01)
B60L 53/18	(2019.01)
B60L 53/30	(2019.01)
B60L 53/65	(2019.01)
G07C 9/20	(2020.01)
G07C 9/29	(2020.01)
H04M 1/72412	(2021.01)
H04W 12/069	(2021.01)
G06Q 10/02	(2012.01)
G06Q 50/06	(2012.01)
H04W 12/08	(2021.01)
H04W 4/02	(2018.01)
H04W 4/021	(2018.01)
H04W 4/40	(2018.01)

(52) **U.S. Cl.**

CPC *Y02T 10/70* (2013.01); *Y02T 10/7072* (2013.01); *Y02T 10/72* (2013.01); *Y02T 90/12* (2013.01); *Y02T 90/14* (2013.01); *Y02T 90/16* (2013.01); *Y02T 90/167* (2013.01); *Y04S 30/14* (2013.01)

EX PARTE REEXAMINATION CERTIFICATE

THE PATENT IS HEREBY AMENDED AS INDICATED BELOW.

Matter enclosed in heavy brackets [ ] appeared in the patent, but has been deleted and is no longer a part of the patent; matter printed in italics indicates additions made to the patent.

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

Claims **1-14** and **16-18** are determined to be patentable as amended.

Claims **15** and **19-24**, dependent on an amended claim, are determined to be patentable.

1. An access device for use in an access control system, the access device comprising:

a processor (**16**) having control of a door lock (**11**); and a communication module (**17**) connected to the processor, the processor [able to] *is configured to* receive a reservation certificate (**5**) presented by a portable terminal (**4**) through the communication module;

wherein, *when a current reservation certificate that comprises an interval of a reservation is presented by the portable terminal,* the processor [activates] *is configured to compare the interval of the reservation of the current reservation certificate to a current time accessible to the processor, determine the current time is within the interval of the reservation, and activate* the door lock [when a current reservation certificate has been presented] *to allow the portable terminal to unlock the door lock during the interval of the reservation.*

2. The access device of claim **1** wherein the processor [activates] *is configured to determine the current time is within the interval of the reservation by determining if the current time is within a start time of the interval of the reservation of the current reservation certificate and a predetermined duration and is configured to activate* door lock [for] *to allow the portable terminal to unlock the door lock from the start time* up to [a] *the* predetermined duration.

3. The access device of claim **2** wherein *the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation from the start time up to* the predetermined duration *that* is all day.

4. The access device of claim **1** wherein the *interval of the reservation of the current* reservation certificate [comprise data representative of] *comprises a start time and* a duration and the processor [activates] *is configured to activate* the door lock [for] *to allow the portable terminal to unlock the door lock from the start time* up to the duration.

5. The access device of claim [**1**] *6* wherein the processor [has access to the current time, the reservation certificate comprises data representative of an interval of the reservation, and the processor activates the door lock during the interval] *is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the end time.*

6. The access device of claim [**5**] *1* wherein the interval [is specified by a start time and one of] *of the reservation of the current reservation certificate comprises a start time and* an end time [and a duration].

7. The access device of claim **1** further comprising:

a memory to which the processor has access, the memory [containing] *is configured to comprise* a public key for a server [authorized] *of the access system configured* to issue the *current* reservation certificate;

wherein at least a portion of the *current* reservation certificate is encrypted by the server using a private key and the processor [verifies] *is configured to verify* that the *current* reservation certificate is genuine by decrypting the portion with the public key.

8. The access device of claim **1** further comprising:

a memory to which the processor has access, the memory [containing] *is configured to comprise* a symmetric key;

wherein at least a portion of the *current* reservation certificate is encrypted by a server [using] *of the access system configured to use* the symmetric key and the processor [verifies] *is configured to verify* that the *current* reservation certificate is genuine by decrypting the portion with the symmetric key.

9. The access device of claim **1** wherein the processor [verifies] *is configured to verify* that the *current* reservation certificate is genuine.

10. The access device of claim **1** further comprising:

an identification to which the processor has access, the identification corresponding to one of the access device and the door lock, wherein the processor [determines] *is configured to determine* that the *current* reservation certificate comprises data representative of the identification.

11. The access device of claim **1** further comprising:

a memory to which the processor has access, the memory [containing] *is configured to comprise* a private key of the access device;

wherein at least a portion of the *current* reservation certificate is encrypted by a server [using] *of the access system configured to use* a corresponding public key for the access device and the processor [decrypts] *is configured to decrypt* the portion with the private key.

12. The access device of claim **1** wherein the processor has access to a server *of the access system* through the communication module and the processor [reports] *is configured to report* to the server that *the* door lock was activated on the basis of the current reservation certificate.

13. A method for use by an access device in an access control system, the method comprising:

a) accepting, by a processor through a communication module, a reservation certificate *that comprises an interval of a reservation* presented with a portable terminal;

b) determining, by the processor, that the reservation certificate *presented by the portable terminal* is current *by comparing the interval of the reservation to a current time accessible to the processor and determining that the current time is within the interval of the reservation*; and

c) activating, by the processor on the basis of the reservation certificate being current, a door lock *to allow the portable terminal to unlock the door lock during the interval of the reservation.*

14. The method of claim **13** wherein *determining that the current time is within the interval of the reservation comprises determining that the current time is within a start time of the interval of the reservation and a predetermined duration and wherein* the certificate is current [for] *from the start time* up to [a] *the* predetermined duration.

16. The method of claim 13 wherein *the interval of the reservation of* the reservation certificate *further* comprises [data representative of] *a start time and* a duration and the *reservation* certificate is current [for] *from the start time* up to the duration.

17. The method of claim [13] *18* wherein [the processor has access to the current time and the reservation certificate comprises data representative of an interval of the reservation, and the certificate is current for up to the interval] *the reservation certificate is current from the start time up to the end time*.

18. The method of claim [17] *13* wherein the interval [is specified by a start time and one of] *of the reservation comprises a start time and* an end time [and a duration].

* * * * *