

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ASSA ABLOY Global Solutions, Inc., HID Global Corp.,

Petitioners,

v.

Urban Intel Inc.,

Patent Owner.

U.S. Patent No. 11,373,474

Case No. IPR2023-00817

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I.	PRELIMINARY STATEMENT	1
II.	STATEMENT OF PRECISE RELIEF REQUESTED	1
III.	OVERVIEW OF THE COMBINATIONS	3
IV.	LEVEL OF ORDINARY SKILL IN THE ART	6
V.	CLAIM CONSTRUCTION	7
VI.	GROUND 1: CLAIMS 1-7 AND 15-25 ARE RENDERED OBVIOUS BY <i>KNUTSSON</i> IN VIEW OF <i>WOODARD</i>	7
A.	Motivation to Combine <i>Knutsson</i> and <i>Woodard</i>	7
B.	Claim 1	9
1.	[1p] “An access control system comprising:	9
2.	[1A] “an access device comprising a communication module connected to a processor having control of a door lock;”	10
3.	[1B] “an application on a portable terminal; and”	13
4.	[1C] “a server to provide a communication setting to the application, the communication setting corresponding to the access device, and to further provide a reservation certificate to the application, the reservation certificate comprising an interval of a reservation,”	16
5.	[1D] “wherein the application compares the interval of the reservation to a current time accessible to the application to determine if the reservation certificate is current and”	23
6.	[1E] “wherein, the application activates the door lock by communicating with the access device via the communication setting when the application determines that the reservation certificate is current.”	27

C.	[Claim 2] “The access control system of claim 1, wherein the communication setting is specific to the access device.”.....	30
D.	[Claim 3] “The access control system of claim 2, wherein the application notifies the user of proximity to the access device.”.....	31
E.	[Claim 4] “The access control system of claim 1, wherein the communication module does not advertise that the communication module is present.”	32
F.	[Claim 5] “The access control system of claim 1, wherein the application uses Bluetooth to communicate with the access device and the communication setting comprises a Bluetooth ID.”	33
G.	[Claim 6] “The access control system of claim 1, wherein the application uses Wi-Fi to communicate with the access device and the communication setting comprises a network SSID.”.....	34
H.	[Claim 7] “The access control system of claim 1, wherein the reservation certificate comprises the communication setting.”	36
I.	Claim 15	37
1.	[15p] “An access control system comprising:”	37
2.	[15A] “an access device comprising a communication module connected to a processor having control of a door lock;”	37
3.	[15B] “an application on a portable terminal; and”	37
4.	[15C] “a server to provide a communication setting to the application, the communication setting corresponding to the access device, and to further provide, via a first communication protocol, a reservation certificate to the application, the reservation certificate comprising an interval of a reservation,”	38
5.	[15D] “wherein the application compares the interval of the reservation to a current time accessible to the	

	application to determine if the reservation certificate is current and”	39
6.	[15E] “wherein the application activates the door lock by communicating with the access device via a second communication protocol that is different from the first communication protocol, based on use by the application of the communication setting, when the application determines that the reservation certificate is current.”	39
J.	[Claim 16] The access control system of claim 15, wherein the first communication protocol comprises a cellular protocol.....	43
K.	[Claim 17] The access control system of claim 15, wherein the first communication protocol comprises a wireless LAN protocol.....	44
L.	[Claim 18] The access control system of claim 17, wherein the wireless LAN protocol comprises Wi-Fi.	45
M.	[Claim 19] The access control system of claim 15, wherein the second communication protocol comprises a short-range wireless protocol.....	46
N.	[Claim 20] The access control system of claim 19, wherein the short-range wireless protocol comprises Bluetooth.	47
O.	[Claim 21] The access control system of claim 15, wherein the second communication protocol comprises a wireless LAN protocol.....	47
P.	[Claim 22] The access control system of claim 21, wherein the wireless LAN protocol comprises Wi-Fi.	47
Q.	[Claim 23] The access control system of claim 15, wherein the application automatically connects to the access device via the second communication protocol as the portable terminal approaches the access device.	48
R.	[Claim 24] The access control system of claim 15, wherein the reservation certificate is encrypted.....	48

S.	[Claim 25] The access control system of claim 24, wherein the encrypted reservation certificate is decrypted by the access device.....	49
VII.	GROUND 2: CLAIMS 8-14 AND 26-36 ARE RENDERED OBVIOUS BY <i>KNUTSSON</i>	49
A.	Claim 8	49
1.	[8p] “An access control system comprising:”.....	49
2.	[8A] “an access device comprising a communication module connected to a processor having control of a door lock;”	49
3.	[8B] “an application on a portable terminal; and”.....	50
4.	[8C] “a server to provide a communication setting and a reservation certificate to the application, the communication setting corresponding to the access device, and the reservation certificate comprising an interval of a reservation,”	50
5.	[8D] “wherein the processor receives the reservation certificate from the application based on use by the application of the communications setting,”	50
6.	[8E] “wherein the processor compares the interval of the reservation to a current time accessible to the processor to determine if the reservation certificate is current and”	53
7.	[8F] “wherein the processor activates the door lock when the processor determines that the reservation certificate is current.”	55
B.	[Claim 9] “The access control system of claim 8, wherein the communication setting is specific to the access device.”.....	57
C.	[Claim 10] “The access control system of claim 9, wherein the application notifies the user of proximity to the access device.”.....	57

D.	[Claim 11] “The access control system of claim 8, wherein the communication module does not advertise that the communication module is present.”	57
E.	[Claim 12] “The access control system of claim 8, wherein the application uses Bluetooth to communicate with the access device and the communication setting comprises a Bluetooth ID.”	58
F.	[Claim 13] “The access control system of claim 8, wherein the application uses Wi-Fi to communicate with the access device and the communication setting comprises a network SSID.”	58
G.	[Claim 14] “The access control system of claim 8, wherein the reservation certificate comprises the communication setting.”	58
H.	Claim 26	58
1.	[26p] “An access control system comprising:”	58
2.	[26A] “an access device comprising a communication module connected to a processor having control of a door lock;”	59
3.	[26B] “an application on a portable terminal; and”	59
4.	[26C] “a server to provide a communication setting to the application, the communication setting corresponding to the access device, and further to provide, via a first communication protocol, a reservation certificate to the application, the reservation certificate comprising an interval of a reservation,”	59
5.	[26D] “wherein the processor receives the reservation certificate from the application via a second communication protocol that is different from the first communication protocol, based on use by the application of the communication setting,”	59
6.	[26E] “wherein the processor compares the interval of the reservation to a current time accessible to the	

	processor to determine if the reservation certificate is current; and”	60
7.	[26F] “wherein the processor activates the door lock when the processor determines that the reservation certificate is current.”	60
I.	[Claim 27] “The access control system of claim 26, wherein the first communication protocol comprises a cellular protocol.”	60
J.	[Claim 28] “The access control system of claim 26, wherein the first communication protocol comprises a wireless LAN protocol.”	60
K.	[Claim 29] “The access control system of claim 28, wherein the wireless LAN protocol comprises Wi-Fi.”	61
L.	[Claim 30] “The access control system of claim 26, wherein the second communication protocol comprises a short-range wireless protocol.”	61
M.	[Claim 31] “The access control system of claim 30, wherein the short-range wireless protocol comprises Bluetooth.”	61
N.	[Claim 32] “The access control system of claim 26, wherein the second communication protocol comprises a wireless LAN protocol.”	61
O.	[Claim 33] “The access control system of claim 32, wherein the wireless LAN protocol comprises Wi-Fi.”	62
P.	[Claim 34] “The access control system of claim 26, wherein the application automatically connects to the access device via the second communication protocol as the portable terminal approaches the access device.”	62
Q.	[Claim 35] “The access control system of claim 26, wherein the reservation certificate is encrypted.”	62
R.	[Claim 36] “The access control system of claim 35, wherein the encrypted reservation certificate is decrypted by the access device.”	62

VIII.	GROUND 3: CLAIM 3 IS RENDERED OBVIOUS BY <i>KNUTSSON</i> IN VIEW OF <i>WOODARD</i> AND <i>BRÖNDRUP</i>	63
A.	Motivation to Combine <i>Knutsson</i> , <i>Woodard</i> , and <i>Bröndrup</i>	63
B.	[Claim 3] The access control system of claim 2, wherein the application notifies the user of proximity to the access device.	64
IX.	GROUND 4: CLAIM 4 IS RENDERED OBVIOUS BY <i>KNUTSSON</i> IN VIEW OF <i>WOODARD</i> AND <i>ADAMS</i>	66
A.	Motivation to Combine <i>Knutsson</i> , <i>Woodard</i> , and <i>Adams</i>	66
B.	[Claim 4] The access control system of claim 1, wherein the communication module does not advertise that the communication module is present.....	68
X.	GROUND 5: CLAIM 10 IS RENDERED OBVIOUS BY <i>KNUTSSON</i> IN VIEW OF <i>BRÖNDRUP</i>	69
A.	Motivation to Combine <i>Knutsson</i> and <i>Bröndrup</i>	69
B.	[Claim 10] “The access control system of claim 9, wherein the application notifies the user of proximity to the access device.”.....	69
XI.	GROUND 6: CLAIM 11 IS RENDERED OBVIOUS BY <i>KNUTSSON</i> IN VIEW OF <i>ADAMS</i>	70
A.	Motivation to Combine <i>Knutsson</i> and <i>Adams</i>	70
B.	[Claim 11] “The access control system of claim 8, wherein the communication module does not advertise that the communication module is present.”	70
XII.	GROUND 7: CLAIMS 6, 17, AND 18 ARE RENDERED OBVIOUS BY <i>KNUTSSON</i> IN VIEW OF <i>WOODARD</i> AND <i>JAIN</i>	71
A.	Motivation to Combine <i>Knutsson</i> , <i>Woodard</i> , and <i>Jain</i>	71
B.	[Claim 6] “The access control system of claim 1, wherein the application uses Wi-Fi to communicate with the access device and the communication setting comprises a network SSID.”.....	72

C.	[Claim 17] “The access control system of claim 15, wherein the first communication protocol comprises a wireless LAN protocol.”	74
D.	[Claim 18] “The access control system of claim 17, wherein the wireless LAN protocol comprises Wi-Fi.”	75
XIII.	GROUND 8: CLAIMS 13, 28, AND 29 ARE RENDERED OBVIOUS BY <i>KNUTSSON</i> IN VIEW OF <i>JAIN</i>	76
A.	Motivation to Combine <i>Knutsson</i> and <i>Jain</i>	76
B.	[Claim 13] “The access control system of claim 8, wherein the application uses Wi-Fi to communicate with the access device and the communication setting comprises a network SSID.”	76
C.	[Claim 28] “The access control system of claim 26, wherein the first communication protocol comprises a wireless LAN protocol.”	77
D.	[Claim 29] The access control system of claim 28, wherein the wireless LAN protocol comprises Wi-Fi.	77
XIV.	DISCRETIONARY DENIAL IS IMPROPER	77
XV.	MANDATORY NOTICES	81
A.	Real Parties-in-Interest	81
B.	Related Matters	82
C.	Lead and Back-Up Counsel, and Service Information	82
XVI.	GROUNDS FOR STANDING	83
XVII.	CONCLUSION	83

LIST OF EXHIBITS

Exhibit	Description
Ex-1001	U.S. Patent No. 11,373,474 (“the ’474 patent”)
Ex-1002	Prosecution File History of U.S. Patent No. 11,373,474
Ex-1003	Declaration of Benjamin B. Bederson
Ex-1004	Curriculum Vitae of Ben Bederson
Ex-1005	WO Publication No. 2008/076074 A1 to Knutsson et al. (“Knutsson”)
Ex-1006	Request for Reexamination of U.S. Patent No. 11,373,474 filed May 11, 2023, Reexamination No. 90/015231
Ex-1007	Preliminary Infringement Contentions Attachment C, <i>Liberty Access Technologies Licensing LLC v. ASSA ABLOY AB</i> , 2:22-cv-507-JRG-RSP (E.D. Tex. May 15, 2023)
Ex-1008	U.S. Patent Publication No. 2009/0219133 A1 to Woodard et al. (“Woodard”)
Ex-1009	WO Publication No. 2001/063425 A1 to Bröndrup (“Bröndrup”)
Ex-1010	U.S. Patent Publication No. 2009/0070272 A1 to Jain (“Jain”)
Ex-1011	Complaint, <i>Liberty Access Technologies Licensing LLC v. ASSA ABLOY AB</i> , 2:22-cv-00507, Dkt. 1 (E.D. Tex. Dec. 30, 2022).
Ex-1012	U.S. Patent Publication No. 2007/0053313 A1 to Adams et al. (“Adams”)
Ex-1013	U.S. Patent Publication No. 2008/0065774 A1 to Keeler
Ex-1014	U.S. Patent Publication No. 2007/0064673 A1 to Bhandaru et al.
Ex-1015	Complaint, <i>ASSA ABLOY Global Solutions, Inc. v. Liberty Access Technologies Licensing LLC</i> , 1:23-cv-00756, Dkt. 1 (N.D. Ill. Feb. 7, 2023).

I. PRELIMINARY STATEMENT

Petitioners request *inter partes* review of claims 1-36 of U.S. Patent No. 11,373,474 (Ex-1001), assigned to Urban Intel Inc. (“Urban”).

The ’474 patent describes allowing a terminal (smartphone) to activate a door lock when the door lock receives a reservation certificate from the terminal. Ex-1001, Abstract. But this concept of unlocking a door using a smartphone was known in the art well before the ’474 patent. It was, in fact, invented by Petitioner.

The primary reference in this Petition, *Knutsson*, is owned by Petitioner ASSA ABLOY Global Solutions, Inc., through its related entity, Phoniro AB. It discloses processors with communication modules configured to receive a reservation certificate from a mobile phone with an application, a server that provides a data object with access data to the mobile phone with the application, and the application of the mobile phone determining whether the reservation certificate is current and activating the door lock if it is—the exact process claimed by the ’474 patent.

Alone or when combined in routine, predictable ways with the secondary references herein, *Knutsson*—not considered by the USPTO during prosecution of the ’474 patent—renders all claims of the ’474 patent obvious.

II. STATEMENT OF PRECISE RELIEF REQUESTED

Petitioners respectfully request review under 35 U.S.C. § 311 of claims 1-36

of the '474 patent over the following references and grounds.

Reference	Publication/Filing Date	Relevant Prior Art Pre-AIA Statute ¹
WO Publication 2008/076074 (“ <i>Knutsson</i> ”)	Published June 26, 2008	35 U.S.C. § 102(b)
U.S. Patent No. 2009/0219133 A1 (“ <i>Woodard</i> ”)	Published September 3, 2009	35 U.S.C. §§ 102(a), (e)
WO Publication 2001/063425 A1 Bröndrup (“ <i>Bröndrup</i> ”)	August 30, 2001	35 U.S.C. § 102(b)
U.S. Patent Publication No. 2009/0070272 A1 (“ <i>Jain</i> ”)	Published March 12, 2009	35 U.S.C. §§ 102(a), (e)
U.S. Patent Publication No. 2007/0053313 A1 to Adams et al. (“ <i>Adams</i> ”)	Published March 8, 2007	35 U.S.C. § 102(b)

Ground	References	Basis	Challenged Claim(s)
1	<i>Knutsson, Woodard</i>	§ 103	1-7, 15-25
2	<i>Knutsson</i>	§ 103	8-14, 26-36
3	<i>Knutsson, Woodard, Bröndrup</i>	§ 103	3

¹ Petitioners list a statute(s) for convenience, but Petitioners also rely on any applicable pre-AIA 35 U.S.C. § 102 statute.

4	<i>Knutsson, Woodard, Adams</i>	§ 103	4
5	<i>Knutsson, Bröndrup</i>	§ 103	10
6	<i>Knutsson, Adams</i>	§ 103	11
7	<i>Knutsson, Woodard, Jain</i>	§ 103	6, 17, 18
8	<i>Knutsson, Jain</i>	§ 103	13, 28, 29

III. OVERVIEW OF THE COMBINATIONS

The '474 patent was filed on January 3, 2022, and claims priority to U.S. Provisional Application No. 61/309,813, filed March 2, 2010. March 2, 2010, is thus the '474 patent's earliest possible priority date.

The '474 patent describes a smart phone or terminal to activate a door lock using a web site or server, and that a door lock receives a reservation certificate presented by the terminal through a communication module. Ex-1001, Abstract. Representative claim 1 of the '474 patent is listed below:

	Claim Limitation
1p	An access control system comprising:

1A	an access device comprising a communication module connected to a processor having control of a door lock;
1B	an application on a portable terminal; and
1C	a server to provide a communication setting to the application, the communication setting corresponding to the access device, and to further provide a reservation certificate to the application, the reservation certificate comprising an interval of a reservation,
1D	wherein the application compares the interval of the reservation to a current time accessible to the application to determine if the reservation certificate is current and
1E	wherein, the application activates the door lock by communicating with the access device via the communication setting when the application determines that the reservation certificate is current. ²

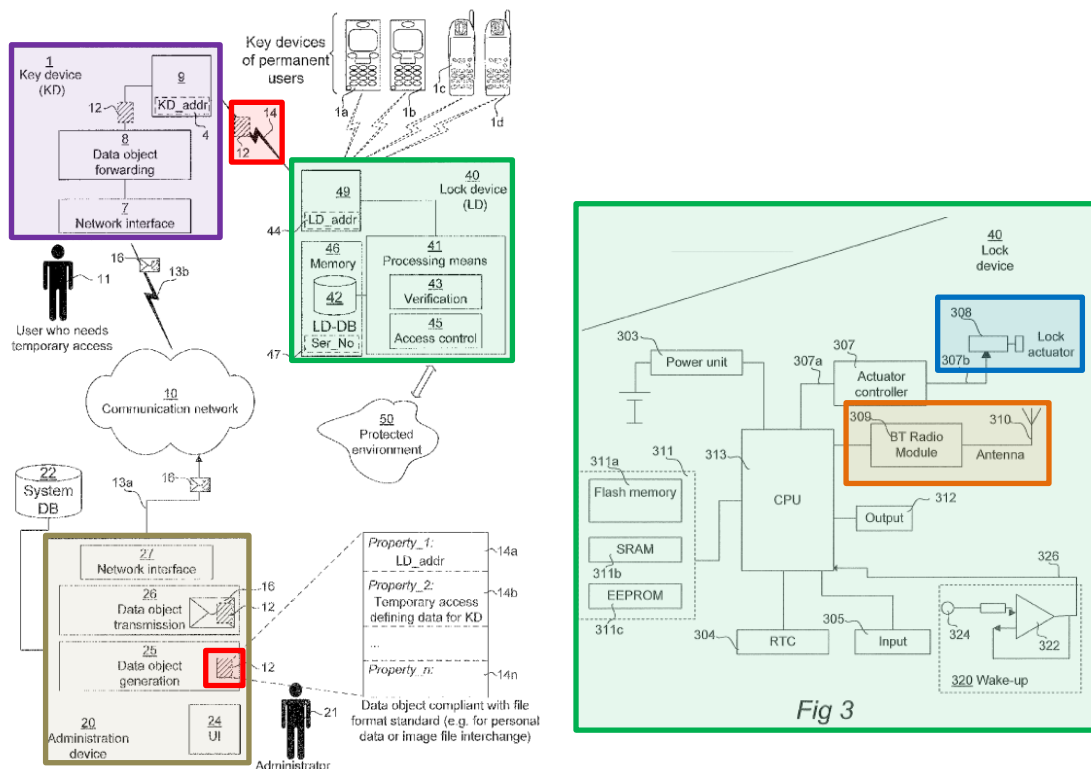
Knutsson, the primary Petitioner-owned reference relied upon, discloses processors of access devices with communication modules configured to receive a communication setting from a server, and an application that receives a reservation certificate and communicates with the access device to allow unlocking of a door lock if the reservation certificate is current, like those claimed by the '474 patent.

Knutsson discloses or renders obvious almost all limitations of the independent claims and many dependent claims of the '474 patent (**Grounds 1, 2**). *Knutsson* discloses “[a]n access control system” that includes an administration

² All colors, annotations, and emphases herein are added to cited figures and quotations unless otherwise stated.

device, or server, that creates and sends a data object with the temporary access defining data to a key device to forward to the lock device to gain access.

Knutsson, 10:13-21. *Knutsson* discloses that its “lock device 40 will be integrated with or coupled to a lock mechanism in the lockable door or garage port and in particular have a controllable lock actuator configured to unlock the lock mechanism upon detection and successful authorization of the key device 1.” *Id.*, 10:24-30. *Knutsson*’s “lock device 40 has a Bluetooth® radio module 309 with an antenna 310.” *Id.*, 17:18-19; Ex-1003, ¶53.



Id., FIGS. 1, 3.

Certain claim limitations in the '474 patent further require an application of a mobile terminal to check the time of a reservation certificate (claims 1-7, 15-25, **Ground 1**). *Knutsson* does not expressly disclose this limitation, but *Woodard* does. Ex-1003, ¶54.

Certain dependent claims in the '474 patent further require the application of the mobile terminal to notify the user of proximity to the lock (claims 3 and 10, **Grounds 3, 5**). To the extent that it is argued that *Knutsson* does not expressly disclose notifying the user, *Bröndrup* does. Ex-1003, ¶¶55-56.

Certain dependent claims in the '474 patent further require the communication module does not advertise that the communication module is present (claims 4 and 11, **Grounds 4, 6**). To the extent that it is argued that *Knutsson* does not expressly disclose this limitation, *Adams* does. Ex-1003, ¶¶57-58.

Certain dependent claims in the '474 patent further require the communication setting to be a network SSID (claims 6 and 13, **Grounds 7, 8**) or that the first communication protocol is Wi-Fi (claims 17, 18, 28, 29, **Grounds 7, 8**). To the extent that it is argued that *Knutsson* does not expressly disclose these limitations, *Jain* does. Ex-1003, ¶¶59-60.

IV. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art (“POSA”) at the time of the purported invention would have had a Bachelor of Science degree in Computer Science or an

equivalent field, with at least two years of academic or industry experience with wireless systems or comparable experience. Additional education could substitute for professional experience and vice versa. Ex-1003, ¶46.

V. CLAIM CONSTRUCTION

Only claim terms “in controversy” need be construed in IPR “and only to the extent necessary to resolve the controversy.” *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (citation omitted), *cert. denied*, 138 S. Ct. 1695 (2018). For the purposes of this IPR, the plain meaning of each claim term can be applied. Petitioners reserve the right to contend that any of the Challenged Claims is indefinite.

VI. GROUND 1: CLAIMS 1-7 AND 15-25 ARE RENDERED OBVIOUS BY *KNUTSSON* IN VIEW OF *WOODARD*

A. Motivation to Combine *Knutsson* and *Woodard*

As explained in Section III, claims 1-7 and 15-25 require the application to compare the interval of the reservation to a current time that is not expressly disclosed by *Knutsson*. Ex-1003, ¶62. A POSA, however, would have been motivated to implement *Woodard*’s application at the mobile terminal into *Knutsson*’s key device 1 because *Woodard* discloses “automatically controlling access to an electronic lockbox utilizing showing appointment data maintained by a central showing management system.” *Woodard*, [0010]; Ex-1003, ¶62.

A POSA would have incorporated *Woodard*'s central management functionality into *Knutsson*'s access system to achieve a central management system and “complete the lockbox access record.” *Woodard*, [0013]; Ex-1003, ¶63. *Woodard* discloses that its key device 104 would transmit “certain access data to the central computer system/database 200 for further processing,” and that the “ability to track, store and centrally process these access data are a valuable tool.” *Woodard*, [0004]; Ex-1003, ¶63. Dr. Bederson opines that “a POSA would have been motivated to combine *Woodard*'s central management system and *Knutsson*'s key device 1, administrative device 20, and lock device 40 so *Knutsson*'s administrative device 20 would be able to ‘track, store and centrally process [the] access data.’” Ex-1003, ¶63 (quoting *Woodard*, [0004]). The combination of *Knutsson* and *Woodard* would ensure the devices are working from common times and a common database. Ex-1003, ¶63.

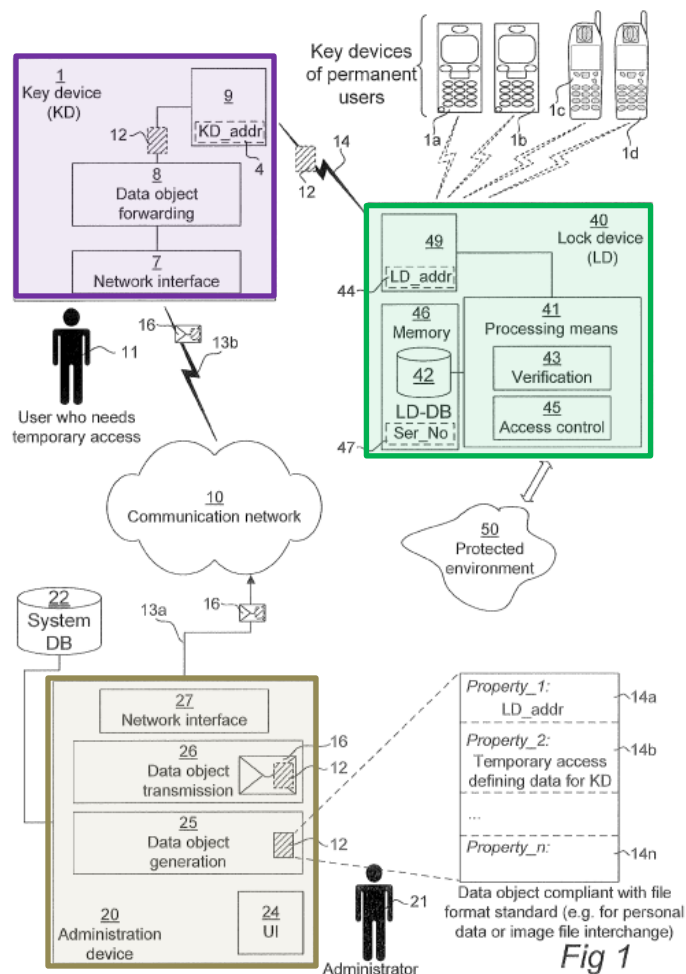
A POSA would have had reasonable expectations of success combining *Woodard* and *Knutsson* because *Woodard* and *Knutsson* disclose similar key devices, such as *Woodard*'s “electronic key device 104, ... a cell phone,” *Woodard*, [0003], and *Knutsson*'s key device, a mobile phone, *Knutsson*, 4:32-5:4, to communicate with access devices like *Woodard*'s lockbox 103, *Woodard*, [0048], or *Knutsson*'s lock device 40 to open a lock. *Knutsson*, 10:24-30; Ex-1003, ¶64.

B. Claim 1

Knutsson in view of *Woodard* renders obvious claim 1. Ex-1003, ¶65.

1. [1p] “An access control system comprising:

Knutsson renders obvious [1p] because *Knutsson* discloses “[a]n access control system ... to provide temporary access for a wireless key device to a lock device.” *Knutsson*, Abstract. *Knutsson* discloses “Fig 1 is a schematic illustration of an access control system, including an administration device, a wireless key device and a lock device.” *Id.*, 9:27-28; Ex-1003, ¶66.

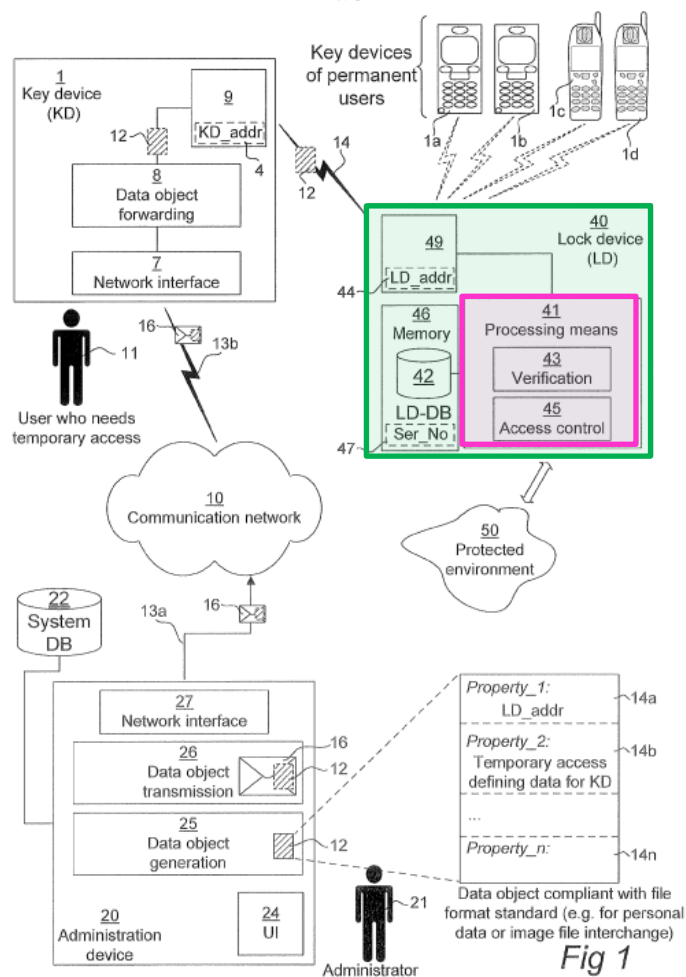


Knutsson, FIG. 1.

2. [1A] “an access device comprising a communication module connected to a processor having control of a door lock;”

Knutsson renders obvious [1A] because *Knutsson*’s “lock device 40 has processing means 41,” such as a CPU (processor) for controlling a door lock.

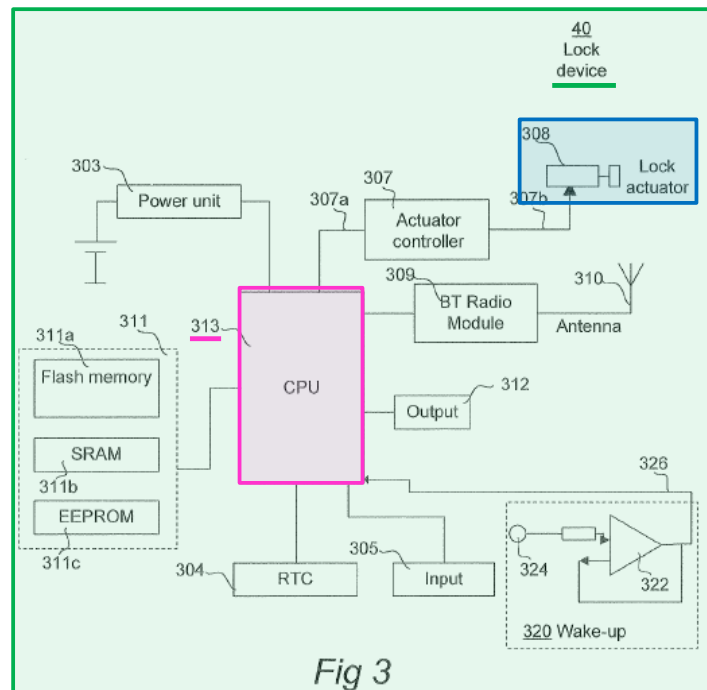
Knutsson, 16:6-10, 17:11-13, 20:7-11; Ex-1003, ¶67.



Knutsson, FIG. 1.

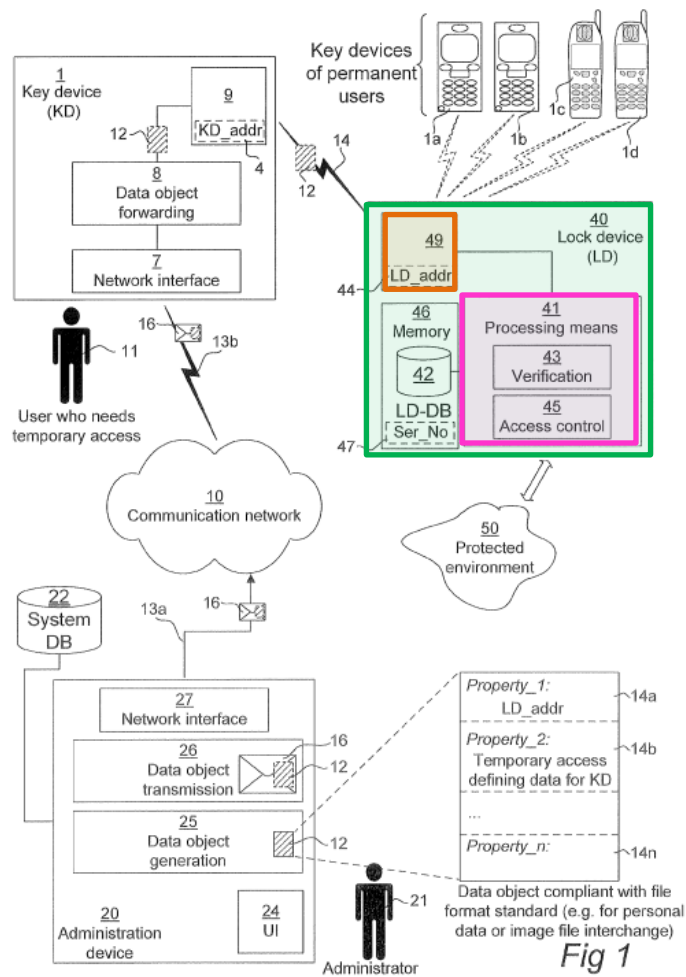
Knutsson's "FIG. 3 is a schematic block diagram illustrating internal components and modules of a lock device," that controls a lock actuator. *Id.*, 9:31-32; Ex-1003, ¶68.

Knutsson's lock device (access device) includes "CPU [313]" that is the "processing means 41." *Id.*, 17:11-13. *Knutsson*'s CPU 313 (processor) controls the door lock because *Knutsson* discloses that "[a]n actuator controller 307 ... provide[s] a control signal 307b for engaging of disengaging the lock actuator 308" (*id.*, 17:4-6), and "CPU 313 ... generates the control signal 307a to the actuator controller 307 ... [to] cause unlocking of the lock," and thus allows "opening of the door." *Id.*, 20:7-11; Ex-1003, ¶69.



Knutsson, FIG. 3.

Knutsson's communication means 49 corresponds to the claimed "communication module." *Knutsson* discloses its "CPU 313 ... perform[s] a method for wireless automatic unlocking in response to the appearance and proper authentication of a key device." *Id.*, 17:9-11. *Knutsson* discloses "the lock device 40 has short-range wireless data communication means 49 in the form of a Bluetooth® transceiver." *Id.*, 12:3-7. *Knutsson* discloses "the lock device 40 has a Bluetooth® radio module 309 with an antenna 310" where the Bluetooth® radio module 309 is the "communication means 49." *Id.*, 17:18-20. Further, *Knutsson* discloses the lock device's processor is connected to its communication means because "the lock device compris[es]: short-range wireless data communication means ... capable of receiving from said key device a data object which originates from said administration device ... [and] processing means, associated with said short-range wireless data communication means." *Id.*, 7:5-12; FIG. 1; Ex-1003, ¶70.



Knutsson, FIG. 1.

3. [1B] “an application on a portable terminal; and”

Knutsson renders obvious [1B] because *Knutsson* discloses a key device such as a mobile terminal (portable terminal) that uses applications. Ex-1003, ¶¶67-68. *Knutsson* discloses that “a mobile terminal is used as the wireless key device,” *id.*, 5:15-18, and also refers to the mobile terminal as a “mobile phone,” as shown below. *Id.*, 4:32-5:4; Ex-1003, ¶¶71-72.

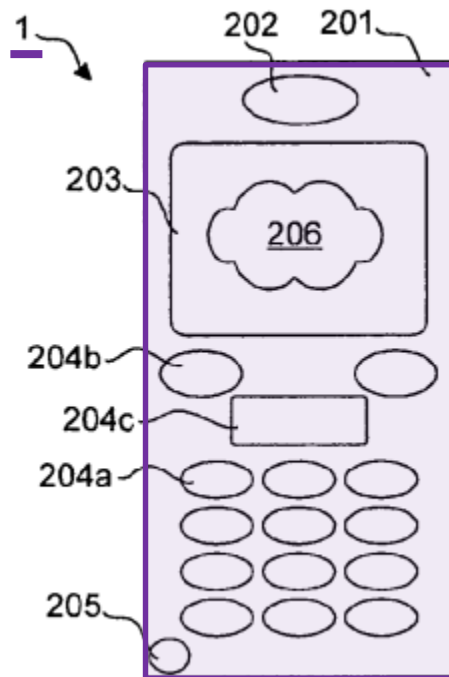
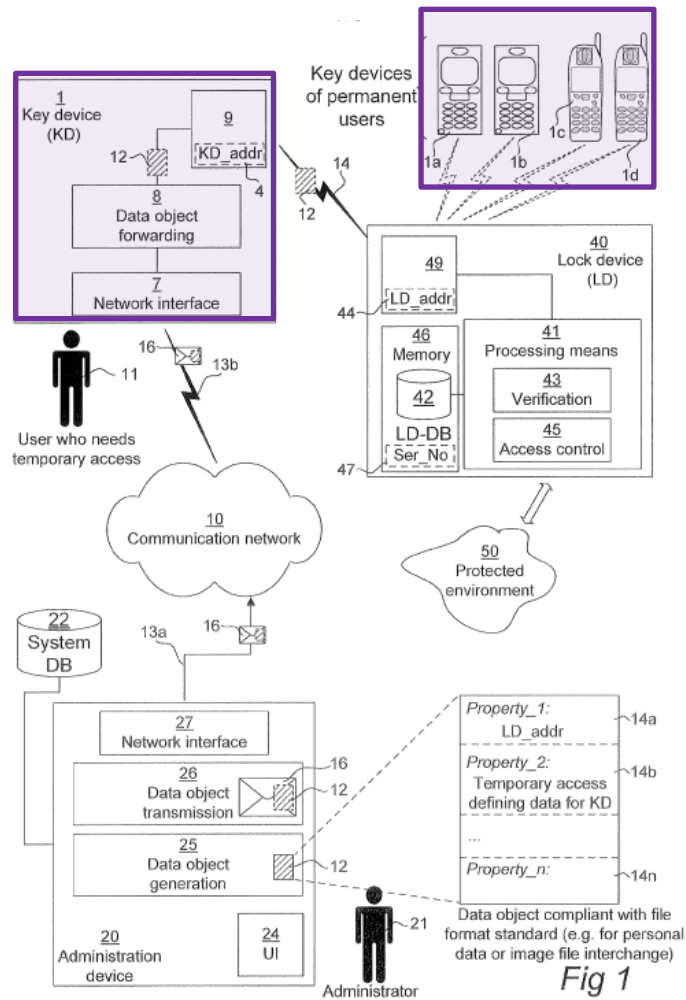


Fig 2



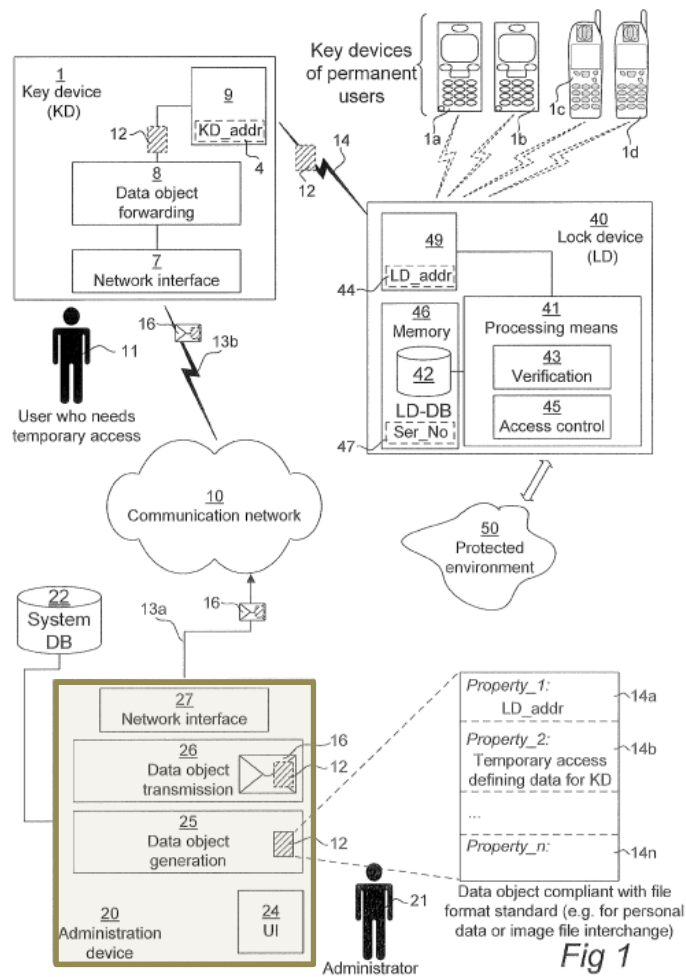
Knutsson, FIGS. 1, 2

Knutsson discloses that its “mobile terminal” (portable terminal) includes “a messaging application and a contacts application (or in the form of a **combined application** for messaging and contacts)” where its application “receives ... and detects the attached vCard 12,” shows properties of the vCard, allows storage of the vCard 12, and allows a command of sending the vCard. *Id.*, 14:12-17, 14:20-23; Ex-1003, ¶73. *Knutsson*’s mobile terminal or key device’s functionality would

be controlled through a software application through graphical interface 206 so the user could control functions of the key device. *Knutsson*, 13:25-28; Ex-1003, ¶73.

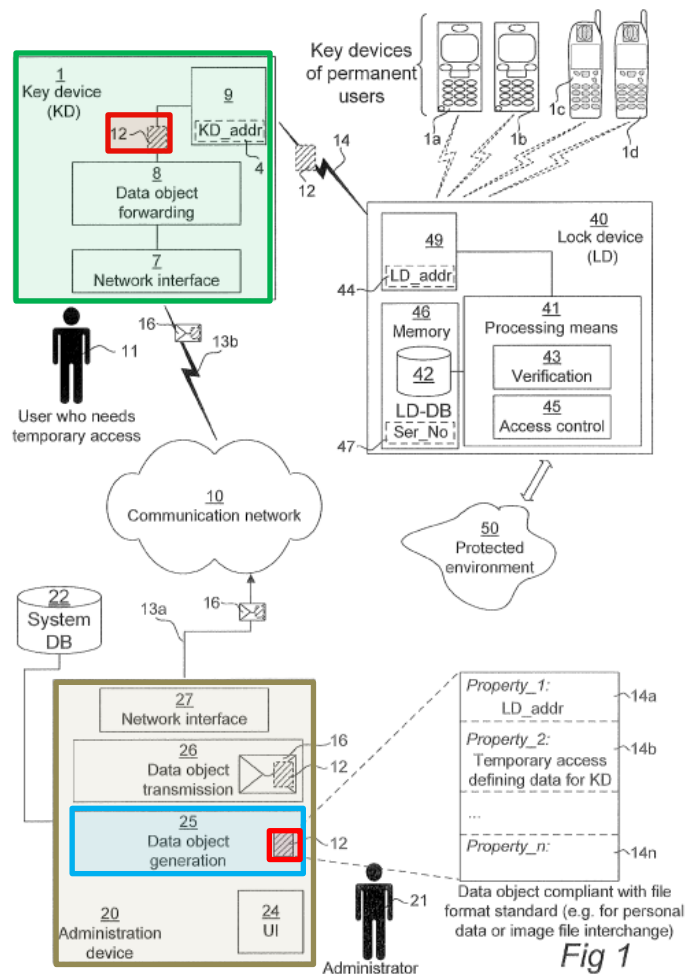
4. [1C] “a **server** to provide a **communication setting** to the application, the communication setting corresponding to the access device, and to further provide a **reservation certificate** to the application, the reservation certificate comprising an **interval of a reservation**,”

Knutsson renders obvious [1C]. Ex-1003, ¶74. *Knutsson*’s administrative device 20 corresponds to the claimed “server,” because *Knutsson* discloses its “**administration device** may advantageously **be a server computer**.” *Knutsson*, 5:11-12. *Knutsson* shows administrative device 20 in FIG. 1. Ex-1003, ¶74.



Knutsson, FIG. 1.

Knutsson renders obvious the claimed “server to provide a communication setting to the application,” because *Knutsson* discloses administration device 20 includes “[t]he data object generation module 25 [that] is configured to create a data object 12.” *Id.*, 11:24-26, FIG. 1; Ex-1003, ¶78. *Knutsson* discloses the digital message 16 to the key device 1 attaches “the data object 12 (vCard).” *Id.*, 13:6-9. Further, “[t]he key device also has data object forwarding functionality 8 capable of receiving the digital message 16.” *Id.*, 13:31-34; Ex-1003, ¶78.



Knutsson, FIG. 1.

Knutsson renders obvious the claimed “communication setting” because it discloses “**created data object 12** is then assigned the **data** which is necessary for the lock device 40 to be able to grant temporary access for the key device 1,” where “[t]his **necessary data includes a communication identifier** (‘LD_addr’ in Fig 1) of the lock device 40.” *Id.*, 11:32-12:1; Ex-1003, ¶77. Claim 7 of the ’474 patent states “the reservation certificate comprises the communication setting,” confirming that the reservation certificate and the communication setting of [1C]

can be sent together. Thus, *Knutsson*'s data object 12 including a communication identifier (communication setting) renders obvious this claim limitation. Ex-1003, ¶77.

Knutsson renders obvious the claimed "communication setting corresponding to the access device" because *Knutsson* discloses its communication identifier is "**a communication identifier ('LD_addr' in Fig 1) of the lock device 40.**" *Knutsson*, 11:32-12:1; Ex-1003, ¶78. The '474 patent gives examples of communications settings "such as the network SSID, passcodes, IP addresses, **Bluetooth ID**, etc." Ex-1001, 4:62-67. *Knutsson* discloses the same example, teaching that "the communication identifier may ... be the unique **Bluetooth communication address**," i.e., its **Bluetooth ID**. *Knutsson*, 3:30-33. Thus, *Knutsson*'s communication identifier of its lock device corresponds to the claimed "communication setting corresponding to the access device." Ex-1003, ¶78.

Knutsson's data object 12 corresponds to the claimed, "reservation certificate." Ex-1003, ¶79. *Knutsson* discloses, "[t]he **created data object 12** is then assigned the data which is necessary for the lock device 40 to be able to **grant temporary access for the key device 1.**" *Id.*, 11:24-11:25. *Knutsson* discloses, "the temporary access defining data assigned to the second vCard property 14b includes temporal data which defines one or more time frames during which access is permitted for the key device 1 to the protected environment 50." *Id.*, 12:21-24.

Because the data object 12 contains necessary data for temporary access, including the communication identifier and temporal data needed for a user to access a room for a time frame, a POSA would have understood that *Knutsson*'s temporary access for "a room, apartment, commercial or public premises, garage, cabinet, locker, etc, with a controllable physical access interface in the form of a lockable door," is a "reservation." This is confirmed by the '474 patent's discussion of a reservation as allowing access "to any access device such as a hotel room lock or the like." Ex-1001, 2:11-12; Ex-1003, ¶79.

Knutsson renders obvious the claimed "a server ... to further provide a reservation certificate to the application" because *Knutsson* discloses the digital message 16 to the key device software application, or the "combined application," from the server computer attaches "the data object 12 (vCard)." *Id.*, 13:6-9; Ex-1003, ¶80. Further, "[t]he key device also has data object forwarding functionality 8 capable of receiving the digital message 16." *Id.*, 13:31-34

Knutsson's data object 12 corresponds to the claimed "reservation certificate comprising an interval," because *Knutsson* discloses "[t]he created data object 12 is then assigned the data which is necessary for the lock device 40 to be able to **grant temporary access for the key device 1.**" *Knutsson*, 11:32-12:1; Ex-1003, ¶81. *Knutsson* explains "the temporary access defining data assigned to the second vCard property 14b includes **temporal data** which defines **one or more time**

frames during which access is permitted for the key device 1 to the protected environment 50.” *Id.*, 12:21-26. “[S]uch temporal data is specified in a calendar data format, for instance in the form of one [or] more dates and/or times which define **start and end points** for permitted temporary access.” *Id.*, 6:1-5, 11:32-12:1; FIGS. 5-6. The structure of data object 12 is shown below in FIGS. 4a-4b. Ex-1003, ¶81.

Structure of generated data object 12:

```
begin:vcard
14c~fn:Temp access for <user 11> to <LD 40>.
14d~uid:<Unique identifier for the generated vCard>
14a~x-phoniro;LD_addr:<Bluetooth address of lock device 40>
14e~x-phoniro;Name:<Name of user 11>
14b~x-phoniro;Valid_from:<Start date, Start_time>
x-phoniro;Valid_until:<End date, End time>
x-phoniro;Max_usage:<Integer value for maximum No of
accesses available for user 11>
14f~X-phoniro;Checksum:<Checksum to prevent manipulation>
end:vcard
```

Fig 4a

Example of generated data object 12:

```
begin:vcard
14c~fn:Temp access for Olle to Elm Street 12.
14d~uid:20061127-099045-99990F192713-0052
14a~x-phoniro;LD_addr:0x00281ec3
14e~x-phoniro;Name:Olle
14b~x-phoniro;Valid_from:20061128,090000
x-phoniro;Valid_until:20061128,150000
x-phoniro;Max_usage:3
14f~X-phoniro;Checksum:1EA450FFC76D8233
end:vcard
```

Fig 4b

Knutsson, FIGS. 4A-4B.

Knutsson's data object 12 includes both a start time and an end time of a temporary access that corresponds to the claimed "interval of a reservation," because an interval is defined by a starting point and an end point. Ex-1003, ¶82.

By providing start and end times, an interval is presented by *Knutsson*'s key device (portable terminal). *Knutsson*, 12:21-26; Ex-1003, ¶82. Indeed, the duration can be calculated by subtracting the start time from the end time, such that duration = end time – start time. Ex-1003, ¶82. This would have been obvious to a POSA because given any two of start time, end time, or duration, the third can be calculated using the simple, well-known formula above. *Id.* Thus, *Knutsson*'s disclosure of “temporary” access corresponds to access for a set time, or an interval. *Knutsson*, Abstract; Ex-1003, ¶82. *Knutsson* confirms this by explaining that the lock device including CPU 313 determines “whether the current time falls within any stage-1 time slot,” where the time slot corresponds to the claimed “interval.” *Knutsson*, 20:4-7; Ex-1003, ¶82.

As discussed above, *Knutsson*'s key device 1 receives data object 12, including a communication identifier and temporal data, and it sends data object 12 to lock device 40 to unlock the door. *Knutsson*, 11:32-12:1, 12:21-26; Ex-1003, ¶83.

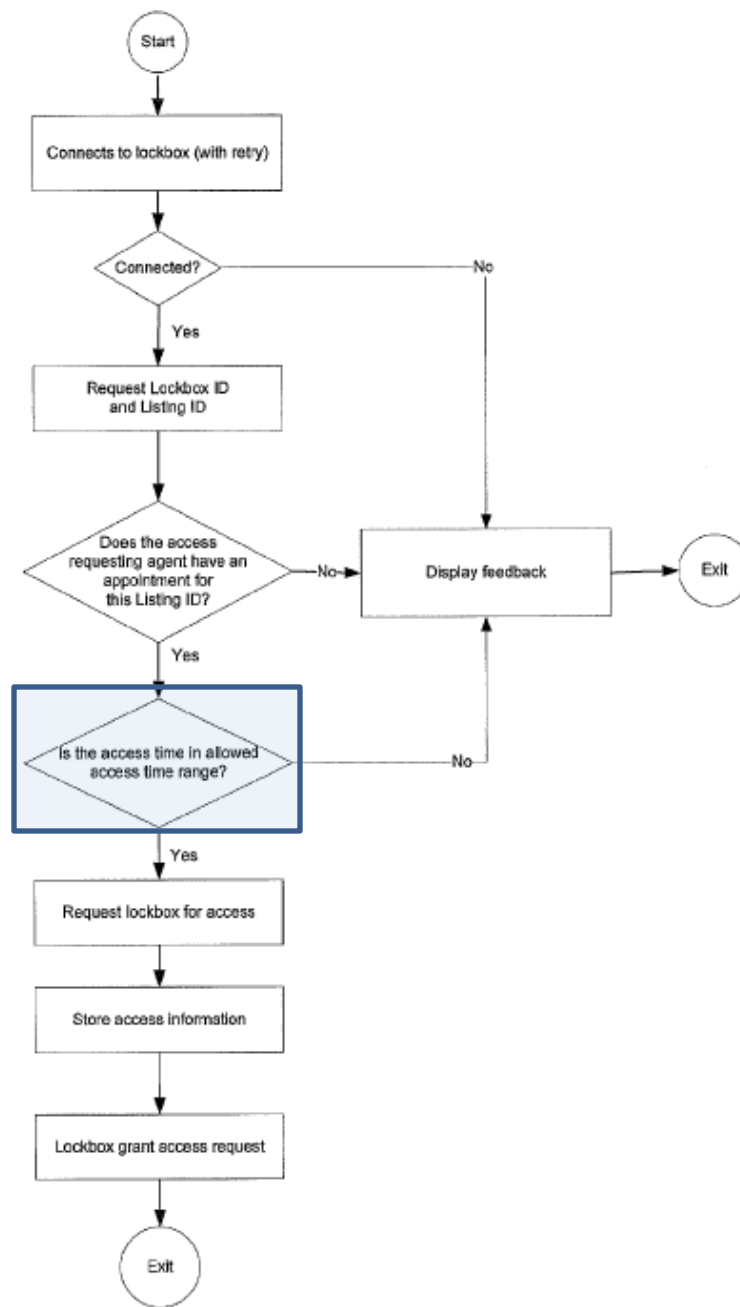
5. [1D] “wherein the application **compares the interval of the reservation to a current time** accessible to the application to determine if the reservation certificate is current and”

Knutsson in combination with *Woodard* renders obvious [1D]. Ex-1003, ¶84. *Knutsson* renders obvious the claimed “application” because *Knutsson*'s key device software application receives the data object 12, detects its contents, sends

it to lock device 40, and receives commands to open the lock. *Knutsson*, 14:12-17, 14:20-23; Ex-1003, ¶84. *Knutsson* discloses that its mobile interface includes “a messaging application and a contacts application (or in the form of a **combined application** for messaging and contacts)” where its application “receives ... and detects the attached vCard 12,” shows properties of the vCard, allows storage of the vCard 12, and allows a command of sending the vCard. *Knutsson*, 14:12-17, 14:20-23.

Knutsson does not explicitly disclose that “the application compares the interval of the reservation to a current time accessible to the application to determine if the reservation certificate is current,” but *Woodard* does. Ex-1003, ¶85. *Woodard* discloses “the logic inside the key device 104 **compares the current date and time of the internal timer with the stored showing appointment data** ... [where] the showing appointment data comprises a time range/interval.” *Woodard*, [0066]. This is shown in FIG. 10, below:

FIG. 10



Id., FIG. 10.

Woodard's key device 104 also contains an "internal timer" and it can access the "current time" through synchronization. *Id.*, [0068]; FIG. 12.

A POSA would have found it obvious to implement *Woodard*'s internal logic of comparing the interval of the appointment data to the current time into *Knutsson*'s software application of key device 1 because "it would allow *Knutsson*'s application to determine access according to the 'showing appointment data maintained by a central management system,' accomplishing the goal to 'track, store and centrally process [the] access data.'" Ex-1003, ¶86 (quoting *Woodard*, [0004], [0009]). A POSA would have found it obvious that *Knutsson*'s software application would similarly analyze and manipulate the contents of data object 12 because the contents of data object 12 are available to *Knutsson*'s software application and a POSA would have implemented code into the software application to achieve a desired functionality of the application. Ex-1003, ¶86. A POSA would have been further motivated to combine the internal logic of *Woodard*'s key device 104 with *Knutsson*'s software application of key device 1 for the reasons discussed above in Section VI.A. *Id.*

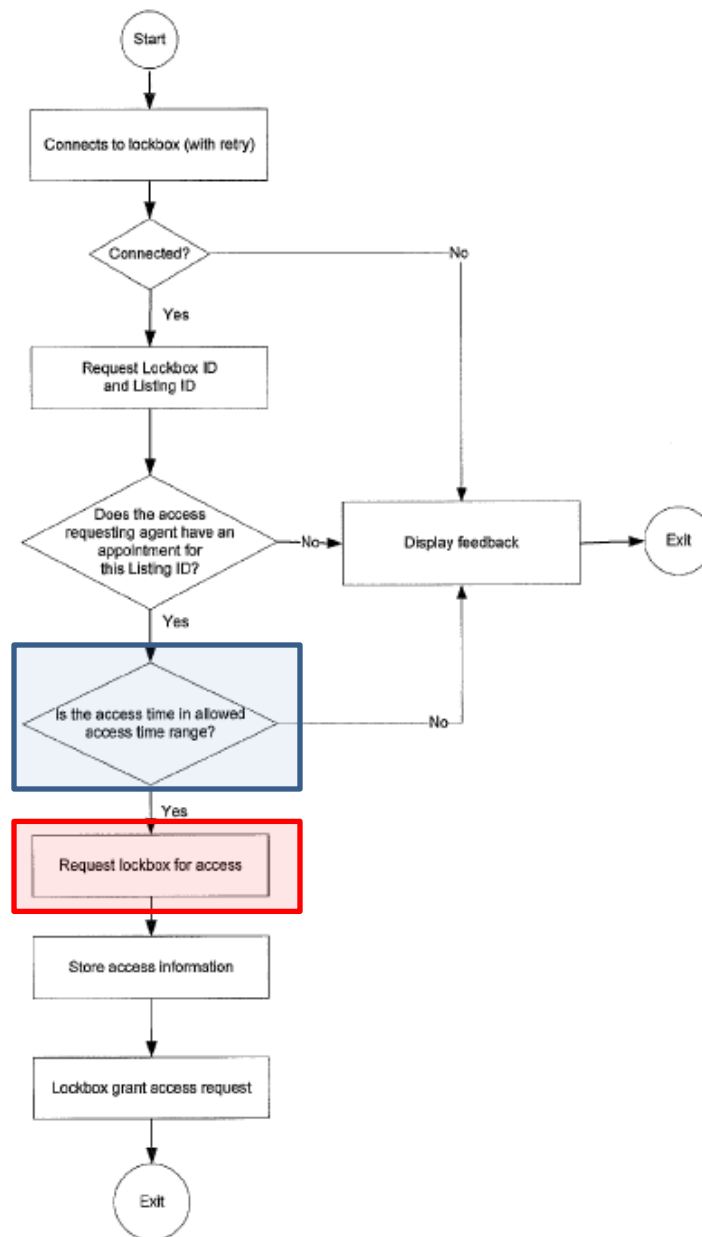
In the *Knutsson-Woodard* combination, *Knutsson*'s key device's application, similar to *Woodard*'s key device software, would receive *Knutsson*'s data object 12, similar to *Woodard*'s showing appointment data, and would compare the interval defined by start and end times in *Knutsson*'s data object 12 using *Woodard*'s internal logic to determine if the data object 12 matches the key device's internal timer. Ex-1003, ¶87.

6. [1E] “wherein, the application **activates the door lock** by communicating with the access device via the communication setting when the application determines that the reservation certificate is current.”

Knutsson in view of *Woodard* renders obvious [1E]. Ex-1003, ¶88. *Knutsson* renders obvious the claimed “application activates the door lock by communicating with the access device” because *Knutsson*’s key device is “capable of receiving the digital message 16 and forwarding the attached vCard data object 12 through short-range wireless data communication means 9 to the lock device 40.” *Knutsson*, 13:31-14:2. *Knutsson* discloses a user interaction with its key device software application that includes “an option like ‘Send by Bluetooth®’, in step 520,” where “the user 11 will cause the key device 1 to attempt to establish short-range data communication 14 with the lock device 40.” *Id.*, 14:18-23; Ex-1003, ¶88.

Knutsson does not explicitly disclose “communicating with the access device ... when the application determines that the reservation certificate is current,” but *Woodard* does. Ex-1003, ¶89. *Woodard* discloses “the showing appointment data comprises a time range/interval” and “[i]f the current access time matches the stored showing appointment time, the lockbox 103 will grant access.” *Woodard*, [0066]. Figure 10, below, shows a similar sequence of steps where **the time is checked against the access time range**, and if the current time falls in the range, then **the lockbox is requested for access**. *Id.*, FIG. 10.

FIG. 10



Id., FIG. 10.

Based on *Woodard*'s disclosure that "actual access to the lockbox 103 is controlled by logic executed inside the electronic key device 104," a POSA would have found it obvious that *Knutsson*'s key device 1, with *Woodard*'s internal logic,

would control access to an access device like *Knutsson*'s lock device 40, which is similar to *Woodard*'s lockbox 104, by establishing communication between *Knutsson*'s key device 1 and lock device 40 through a command on *Knutsson*'s application of key device 1. Ex-1003, ¶90. A POSA would have found it obvious that *Woodard*'s internal logic incorporated into *Knutsson*'s key device 1 would check the current time as compared to the data object 12 information, as discussed above in Section VI.B.5 for [1D], and that the data object 12 is forwarded to the lock device 40 which causes communication with the lock. Ex-1003, ¶90 (citing *Knutsson*, 13:31-14:2). A POSA would have been motivated to combine *Knutsson* and *Woodard*, as discussed above in Sections VI.B.5 and VI.A. Ex-1003, ¶90.

Because the communication identifier (communication setting), which can be a Bluetooth address, is conferred to the lock device 40 (access device), and the communication means is a short-range communication, such as Bluetooth, *Knutsson*, 14:18-23, a POSA would have found it obvious that *Knutsson*'s software application on key device 1 authorizes the door lock to be opened when it communicates data object 12, including the Bluetooth address, through Bluetooth to lock device 40. Ex-1003, ¶91. A POSA would have found it obvious that *Knutsson*'s mobile terminal or key device's functionality is controlled through a software application that communicates data object 12 to lock device 40, including the communication identifier, so that the application "control(s) the terminal's

functionality,” including communicating with lock device 40 to allow unlocking of the door. Ex-1003, ¶91.

C. [Claim 2] “The access control system of claim 1, wherein the communication setting is specific to the access device.”

Knutsson in view of *Woodard* renders obvious claim 2. Ex-1003, ¶92. As explained in Section VI.B.4 for [1C], *Knutsson* discloses “[t]he created data object 12 is [] assigned the data which is necessary for the lock device 40 to be able to grant temporary access for the key device 1,” where “[t]his necessary data includes a communication identifier (‘LD_addr’ in Fig 1) of the lock device 40.” *Knutsson*, 11:32-12:1. *Knutsson*’s “communication identifier (Bluetooth® address) of the lock device’s radio transceiver 49,” *id.*, 12:15-20, corresponds to the claimed “communication setting [] specific to the access device,” because the LD_addr of the communication identifier 44 must align with the corresponding lock device in order for the lock device to verify ... received data object 12 is appropriate for “the desired temporary access.” *Id.*, 12:15-20, 16:11-20; Ex-1003, ¶92. Additionally, *Knutsson* confirms the Bluetooth address on its access device may be “unique” to the access device and “assigned ... in conjunction with the manufacture thereof.” *Knutsson*, 3:30-33; Ex-1003, ¶92.

D. [Claim 3] “The access control system of claim 2, wherein the application **notifies the user of proximity** to the access device.”³

Knutsson in view of *Woodard* renders obvious claim 3. Ex-1003, ¶93. For example, *Knutsson* discloses that, “assuming that the lock device 40 is in sleep mode, the initial wake-up stage 610 is performed in steps 612, 614 and 616 by using the **proximity** sensor 324 to detect the presence of the user of key device 1 near the lock device 40.” *Knutsson*, 19:23-26. *Knutsson*’s CPU 313 (within its lock device) “check[s] whether the determined Bluetooth® address of the responding device matches one of afore-described authentication data records” and may take appropriate action “such as generating an alarm signal or ... for later reporting.” *Id.*, 20:4-6, 20:17-19. A POSA would have found it obvious that the alarm signal or report would have notified a user of *Knutsson*’s control system including an administrator of the administration device 20 or a user of the key device 1 because both are users of *Knutsson*’s access system. Ex-1003, ¶93. The alarm or report provides notification after proximity of key device 1 to lock device 40 is sensed by

³ “The user” lacks antecedent basis. For the purposes of this proceeding, Petitioners treat the user under a plain and ordinary meaning as the administration-user and/or the guest-user.

the proximity sensor. *Id.* Indeed, a POSA would have found it obvious that an alarm or report's function is to provide notice. Ex-1003, ¶93.

E. [Claim 4] “The access control system of claim 1, wherein the communication module **does not advertise that the communication module is present.”**

Knutsson in view of *Woodard* renders obvious claim 4 because *Knutsson*'s communication means 49 is in a sleep mode, incapable of sending advertising signals, until a wake-up stage is executed. Ex-1003, ¶94. *Knutsson* discloses “there may be an optional wake-up stage 518 ... [because] the lock device 40 is operable in a sleep mode and an operational mode. The purpose of the sleep mode is to keep as much as possible of the electronics in the lock device in a shut-off or disabled condition so as to minimize the power consumption during periods of inactivity.” *Knutsson*, 14:23-28. *Knutsson* discloses “the lock device 40 may be awaken[ed] and brought from its sleep mode into operational mode. The wake-up arrangement has a proximity sensor 324 positioned and configured to detect the presence of a user or key device near the lock device.” *Id.*, 14:31-34. *Knutsson* thus discloses its lock device 40 is in a sleep mode including “as much as possible of the electronics in the lock device” excluding the disclosed acoustic or vibration sensor 324 needed for wake-up. *Id.*, 14:26-28. Wake-up does not occur through communication means 49, which is in a non-operational mode, but rather through a series of knocks or proximity detection, *id.*, 15:1-7, and thus communication means 49

(communication module) is not operational in the lock device 40's sleep mode.

Ex-1003, ¶93. A POSA would have understood communication means 49 does not send or receive signals in the shut-off or disabled condition in lock device 40's sleep mode because it is not operational, and thus the non-operational sleep mode of communication means 49 renders obvious the claimed "communication module does not advertise that the communication module is present." *Id.*

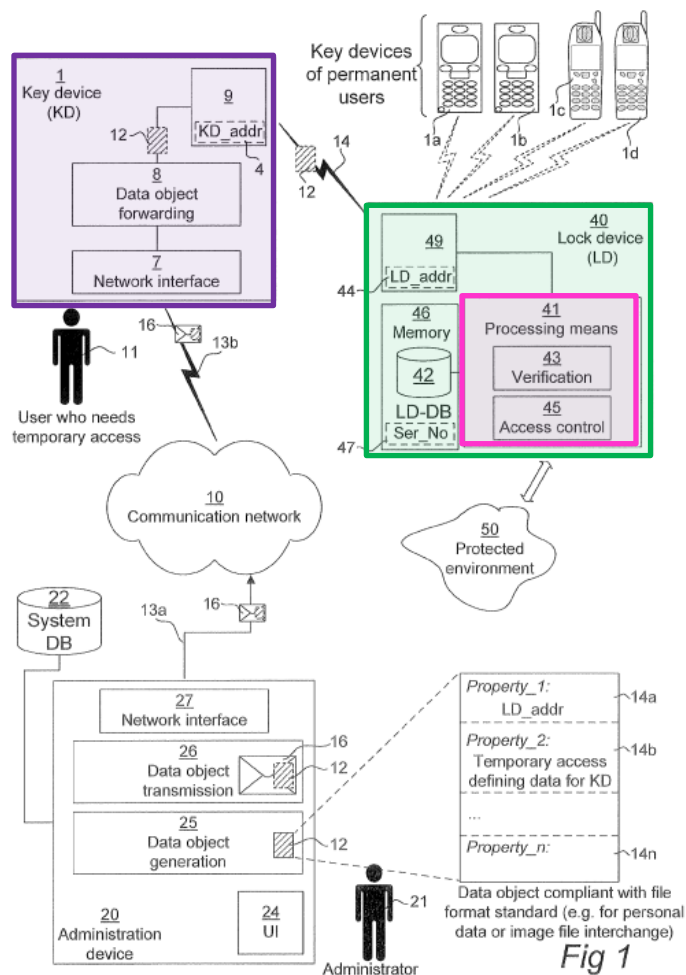
F. [Claim 5] "The access control system of claim 1, wherein the application uses **Bluetooth** to communicate with the access device and the communication setting comprises a **Bluetooth ID**."

Knutsson in view of *Woodard* renders obvious claim 5. Ex-1003, ¶95.

Knutsson discloses its mobile interface includes "a messaging application and a contacts application (or in the form of a **combined application** for messaging and contacts)" where its application "receives ... and detects the attached vCard 12," shows properties of the vCard 12, allows storage of the vCard 12, and allows a command to "Send by **Bluetooth®**" that causes sending the vCard 12 to lock device 40. *Knutsson*, 14:12-17, 14:20-23. *Knutsson* discloses "the **mobile terminal** user [receives] the digital message from the administration device, temporarily save[s] the embedded data object in the **mobile terminal** and then [forwards] it [] to the **lock device** by way of **Bluetooth®** communication." *Knutsson*, 5:18-23.

Knutsson also discloses "the **processing means** is configured to detect a

communication identifier of the key device (such as its **Bluetooth® address**).” *Id.*, 7:26-28; Ex-1003, ¶96.



Knutsson, FIG. 1.

- G. [Claim 6]** “The access control system of claim 1, wherein the application **uses Wi-Fi** to communicate with the access device and the communication setting comprises a **network SSID**.”

Knutsson in view of *Woodard* renders obvious claim 6. Ex-1003, ¶96. As explained in Section VI.F for claim 5, *Knutsson*’s “software application” on key device 1 communicates with its lock device 40 (access device) using Bluetooth.

Knutsson, 5:18-23. *Knutsson* also discloses “for the short-range wireless data communication, another communication standard is also feasible, including but not limited to ... a wireless local area network (WLAN) standard such as IEEE. 802.11.” *Knutsson*, 22:12-19. IEEE 802.11 is the Wi-Fi standard. Ex-1003, ¶96.⁴ Wi-Fi would thus be one of the short-range wireless communications used between *Knutsson*’s key device 1’s application and lock device 40. Ex-1003, ¶96.

An SSID is a “Service Set Identifier for an [extended service set (ESS) in 802.11] advertised in 802.11 management frames to aid wireless clients in discovering the ESS.” Ex-1014, [0039]-[0040]. In lay terms, an SSID is a Wi-Fi network’s name. Ex-1003, ¶97. *Knutsson* renders obvious the claimed “the communication setting comprises a network SSID” because when *Knutsson*’s key device 1 communicates with its lock device 40 over “IEEE 802.11,” (Wi-Fi), *Knutsson*, 12:3-7, 22:15-19, a POSA would have found it obvious that its communication identifier (communication setting) would not be a Bluetooth

⁴ For example, U.S. Patent Publication No. 2008/0065774 describes “[a]ccess devices may be provided as ...wireless access points, which implement the 802.11 Wireless Ethernet protocol (‘WiFi’).” Ex-1013, [0040]. As another example, U.S. Patent Publication No. 2007/0064673 states “WiFi: Refers to 802.11.” Ex-1014, [0004]; Ex-1003, ¶91.

communication address, but instead would include the network SSID associated with the Wi-Fi network over which key device 1 is communicating to lock device 40. Ex-1003, ¶97. The SSID for a Wi-Fi network would be used for 802.11 communication like *Knutsson*'s disclosed Bluetooth address for Bluetooth communication because both key device 1 and lock device 40 would know and use the SSID to communicate just as they use a Bluetooth connection to communicate where both devices know and use the Bluetooth address. Further, “[i]n 802.11 networks an ESS, identified by a[n] SSID, represents the logical wireless LAN to which wireless clients may attach themselves,” Ex-1014, [0064], and thus *Knutsson*'s key device 1 and lock device 40 would identify the Wi-Fi network to communicate over it. Ex-1003, ¶97. Thus, a POSA would have found it obvious to use the SSID as part of the communication identifier in a Wi-Fi network. Ex-1003, ¶97. Using the SSID as the identifier in a WLAN system meets *Knutsson*'s goal of being “conveniently” already available for use because the Wi-Fi name is “advertised ... to aid wireless clients” searching for it. Ex-1014, [0020], [0240], claim 49; Ex-1003, ¶97.

H. [Claim 7] “The access control system of claim 1, wherein the reservation certificate comprises the **communication setting**.”

Knutsson in view of *Woodard* renders obvious claim 7. Ex-1003, ¶98. As explained in Section VI.B.4 for [1C], *Knutsson* discloses the claimed “the

communication setting corresponding to the access device” because *Knutsson* discloses “[t]he created data object 12 is then assigned the data which is necessary for the lock device 40 to be able to grant temporary access for the key device 1,” where “[t]his necessary data includes **a communication identifier (‘LD_addr’ in Fig 1) of the lock device 40.**” *Id.*, 11:32-12:1. Thus, *Knutsson* discloses that the data object 12 (reservation certificate) comprises the communication identifier (communication setting). Ex-1003, ¶98.

I. Claim 15

Knutsson in view of *Woodard* renders obvious claim 15. Ex-1003, ¶99.

1. [15p] “An access control system comprising:”

[15p] is identical to [1p]. *Knutsson* renders obvious [15p], as explained for [1p] in Section VI.B.1. Ex-1003, ¶100.

2. [15A] “an access device comprising a communication module connected to a processor having control of a door lock;”

[15A] is identical to [1A]. *Knutsson* renders obvious [15A], as explained for [1A] in Section VI.B.2. Ex-1003, ¶101.

3. [15B] “an application on a portable terminal; and”

[15B] is identical to [1B]. *Knutsson* renders obvious [15B], as explained for [1B] in Section VI.B.3. Ex-1003, ¶102.

4. [15C] “a **server** to provide a **communication setting** to the application, the communication setting corresponding to the access device, and to further provide, via a **first communication protocol**, a reservation certificate to the application, the reservation certificate comprising an **interval of a reservation**,”

Knutsson renders obvious [15C]. Ex-1003, ¶103. As explained for [1C] in Section VI.B.4, *Knutsson* renders obvious “a server to provide a communication setting to the application, the communication setting corresponding to the access device, and to further provide ... a reservation certificate to the application, the reservation certificate comprising an interval of a reservation.” Ex-1003, ¶103.

Knutsson also at least suggests that the reservation certificate is provided to the applicant “via the first communication protocol” because *Knutsson* discloses that, “[b]eing a mobile terminal in the disclosed embodiment, the key device 1 also has a network interface 7 (Fig 1) in the form of cellular radio circuitry compliant with the mobile telecommunications network of the communication network 10.” *Knutsson*, 13:29-31. Network interface 7 is the key device’s “data interchange means for communication of data objects” where “the administration device is adapted for generating a data object.” *Id.*, 4:4-9. *Knutsson* discloses communication network 10 is a mobile telecommunications network compliant with for instance GSM, UMTS, D-AMPS, CDMA2000, FOMA or TD-SCDMA.” *Id.*, 13:12-16. Each of the listed telecommunications networks are communication

protocols for a mobile terminal, key device 1, to communicate with administrative device 20. *Knutsson* further discloses communications network 10 may “comprise a wide-area data communication network, for instance being a part of the Internet.” *Id.*, 13:15-16; Ex-1003, ¶104.

5. [15D] “wherein the **application compares the interval of the reservation to a current time** accessible to the application to determine if the reservation certificate is current and”

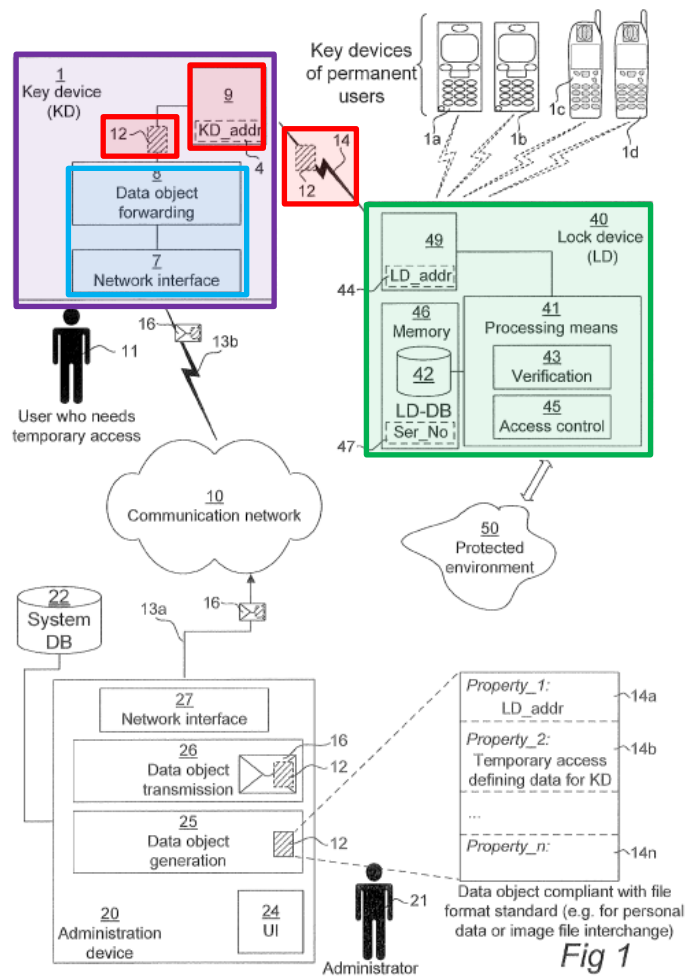
[15D] is identical to [1D]. *Knutsson* renders obvious [15D], as explained for [1D] in Section VI.B.5. Ex-1003, ¶105.

6. [15E] “wherein the **application activates the door lock by communicating with the access device via a second communication protocol** that is different from the first communication protocol, based on use by the application of the communication setting, when the application determines that the reservation certificate is current.”

Knutsson renders obvious [15E]. Ex-1003, ¶106. As explained for [1E] in Section VI.B.6, *Knutsson* in view of *Woodard* renders obvious “wherein the application activates the door lock by communicating with the access device ... when the application determines that the reservation certificate is current.” Ex-1003, ¶106.

Knutsson also renders obvious “communicating with the access device via a second communication protocol that is different from the first communication protocol, based on use by the application of the communication setting,” because

Knutsson discloses “a lock device for a protected environment, said lock device comprising short-range wireless data communication means capable of short-range wireless data communication based on a communication identifier of said lock device; a wireless key device having short-range wireless data communication means and data interchange means for communication of data objects.” *Knutsson*, 3:2-7; Ex-1003, ¶107. Referring to FIG. 1, *Knutsson* discloses “the interface 7 and functionality 8 together constitute data interchange means capable of receiving the data object 12 ... and forwarding the data object to the lock device 40 with the aid of the short-range wireless data communication means 9.” *Knutsson*, 14:3-6; Ex-1003, ¶107.



Knutsson, FIG. 1.

The “short-range wireless data communication means 9 to the lock device 40 as seen at 14,” such as *Knutsson*’s disclosure of “Bluetooth®,” “WLAN,” “802.11,” *id.*, 22:15-19, 13:31-34, is different than the “forwarding of the digital message 16, as received from the network interface 27 of the administration device 20, to the key device 1, as seen at 13b,” such as *Knutsson*’s disclosure of using “**cellular**” communication protocols including “GSM, UMTS, D-AMPS, CDMA2000, FOMA, or TD-SCDMA.” *Knutsson*, 13:12-15; Ex-1003, ¶108. Thus,

Knutsson renders obvious a communication through a cellular network or Internet (first communication protocol) from administration device 20 to key device 1 that is different than key device 1's communication through short-range communication means (second communication protocol) with lock device 40. Ex-1003, ¶108.

Knutsson discloses “short-range wireless data communication means capable of short-range wireless data communication with said key device based on a communication identifier of said lock device.” *Knutsson*, 7:6-9. Dr. Bederson states “a POSA would have found it obvious that *Knutsson*'s short-range communication (second communication protocol) is based on a communication identifier, a ‘Bluetooth® address 4,’ (communication setting) used by *Knutsson*'s mobile terminal software application (application).” Ex-1003, ¶109 (quoting *Knutsson*, 13:34-14:2). A POSA would have found it obvious that *Knutsson*'s mobile terminal (having software applications) uses *Knutsson*'s communication identifier because *Knutsson* discloses a “graphical user interface” that is capable of specifying the communication identifier. *Knutsson*, 11:1-6, 11:32-12:1; Ex-1003, ¶109. A POSA would have found it obvious that *Knutsson*'s mobile terminal having software uses the *Knutsson* communication identifier because *Knutsson* discloses “lock device 40 detects the communication identifier ... of the key device 1.” *Knutsson*, 16:4-5; Ex-1003, ¶109.

Communication occurs between the lock device 40 and the key device 1 because *Knutsson* discloses “authorization is based solely on the key device’s Bluetooth® address and the current time, both of which are detected automatically by the lock device 40 and require no interaction from the user (other than bringing the key device near the lock device 40).” *Knutsson*, 18:1-4. *Knutsson* discloses that “CPU 313 ... [checks] whether the current time falls within any stage-1 time slot defined for that Bluetooth® address” and, upon determining the current time falls within a stage-1 time slot, effectuates “engaging or disengaging the lock actuator 308 to cause unlocking when appropriate” and thus unlocking the door lock. *Id.*, 17:4-6, 20:4-7, FIG. 6 at 628-630; Ex-1003, ¶110. Because the communication identifier can be a Bluetooth address (communication setting) and is conferred to the lock device 40 (access device), and the used communication means is a short-range communication, such as Bluetooth, a POSA would have found it obvious that *Knutsson*’s software on its mobile terminal activates the door lock when it communicates the Bluetooth address through Bluetooth and when the current time is within the time slot of the data object 12. Ex-1003, ¶110.

J. [Claim 16] The access control system of claim 15, wherein the first communication protocol comprises a **cellular protocol**.

Knutsson renders obvious claim 16. Ex-1003, ¶111. As explained for [15C] in Section VI.I.4, *Knutsson* discloses that, “[b]eing a mobile terminal in the

disclosed embodiment, the key device 1 also has a network interface 7 (Fig 1) in the form of **cellular** radio circuitry compliant with the mobile telecommunications network of the communication network 10.” *Knutsson*, 13:29-31. *Knutsson*’s “communication network 10 is a mobile telecommunications network compliant with for instance GSM, UMTS, D-AMPS, CDMA2000, FOMA or TD-SCDMA.” *Id.*, 13:12-15. All of these are cellular protocols. Ex-1003, ¶111.

K. [Claim 17] The access control system of claim 15, wherein the first communication protocol comprises a **wireless LAN protocol**.

Knutsson renders obvious claim 17. Ex-1003, ¶112. As explained for [15C] in Section VI.I.4, *Knutsson* discloses that “[b]eing a mobile terminal in the disclosed embodiment, the key device 1 also has a network interface 7 ... compliant with ... the communication network 10.” *Knutsson*, 13:29-31. Network interface 7 is the key device’s “data interchange means for communication of data objects” where “the administration device is adapted for generating a data object.” *Id.*, 4:4-9. *Knutsson* discloses that communications network 10 may “comprise a wide-area data communication network, for instance being a part of the Internet.” *Id.*, 13:15-16. *Knutsson* also discloses that its devices communicate over “a **wireless local area network (WLAN)** standard.” *Id.*, 22:15-19; Ex-1003, ¶112.

Knutsson renders obvious a “wireless LAN protocol” corresponds to the claimed “first communication protocol” because *Knutsson*’s key device 1

communicates with communication network 10 to access “the Internet” through known communication methods, which *Knutsson* discloses includes WLAN standards such as HomeRF, IEEE 802.11 (Wi-Fi), and WiMax. Ex-1003, ¶113 (citing *Knutsson*, 22:18-19). Thus, *Knutsson*’s disclosure of WLAN applies to mobile terminal 1, and such a use of known communication technology would have been an obvious selection of a limited number of known communication methods of mobile terminals, including accessing the Internet. Ex-1003, ¶113.

L. [Claim 18] The access control system of claim 17, wherein the wireless LAN protocol comprises **Wi-Fi**.

Knutsson renders obvious claim 18. Ex-1003, ¶114. As explained for [15C] in Section VI.I.4, *Knutsson* discloses that “[b]eing a mobile terminal in the disclosed embodiment, the key device 1 also has a network interface 7 (Fig 1) in the form of cellular radio circuitry compliant with the mobile telecommunications network of the communication network 10.” *Knutsson*, 13:29-31. Network interface 7 is consistent with the key device’s “data interchange means for communication of data objects” where “the administration device is adapted for generating a data object.” *Id.*, 4:4-9. *Knutsson* discloses communications network 10 “comprise[s] a wide-area data communication network, for instance being a part of the Internet.” *Id.*, 13:15-16; Ex-1003, ¶114.

Knutsson renders obvious “Wi-Fi” because *Knutsson*’s key device 1 communicates with communication network 10 through *Knutsson*’s disclosed WLAN to access “the Internet.” Indeed, *Knutsson* states that its key device 1 uses short-range communication, such as WLAN and IEEE 802.11 (Wi-Fi) communications. *Knutsson*, 22:18-19. Dr. Bederson opines “a POSA would have found it obvious that *Knutsson*’s disclosure of WLAN communication including Wi-Fi would be applied to a mobile terminal 1 and that such a use of known communication technology would have been an obvious selection of a limited number of known communication methods of mobile terminals.” Ex-1003, ¶115.

M. [Claim 19] The access control system of claim 15, wherein the second communication protocol comprises a **short-range wireless protocol**.

Knutsson renders obvious claim 19. Ex-1003, ¶116. *Knutsson* discloses “a lock device for a protected environment, said lock device comprising **short-range wireless data communication means capable of short-range wireless data communication** ... [and] a wireless key device having short-range wireless data communication means and data interchange means for communication of data objects.” *Knutsson*, 3:2-7. Referring to FIG. 1, *Knutsson* discloses “the interface 7 and functionality 8 together constitute data interchange means capable of receiving the data object 12 ... and forwarding the data object to the lock device 40 with the aid of the short-range wireless data communication means 9.” *Id.*, 14:3-6; Ex-1003,

¶116. A POSA would have understood that the “short-range wireless” communication means uses a “short-range wireless protocol.” Ex-1003, ¶116.

N. [Claim 20] The access control system of claim 19, wherein the short-range wireless protocol comprises **Bluetooth**.

Knutsson renders obvious claim 20. *Knutsson* discloses the “short-range wireless data communication means 9 to the lock device 40” communicates through “**Bluetooth®**.” *Knutsson*, 13:34-14:2; Ex-1003, ¶117.

O. [Claim 21] The access control system of claim 15, wherein the second communication protocol comprises a **wireless LAN protocol**.

Knutsson renders obvious claim 21. Ex-1003, ¶118. *Knutsson* discloses the “key device also has data object forwarding functionality 8 capable of receiving the digital message 16 and forwarding the attached vCard data object 12 through short-range wireless data communication means 9 to the lock device 40,” through “a **wireless local area network (WLAN) standard**” (protocol). *Knutsson*, 13:31-34, 22:15-19, FIG. 1; Ex-1003, ¶118.

P. [Claim 22] The access control system of claim 21, wherein the wireless LAN protocol comprises **Wi-Fi**.

Knutsson renders obvious claim 22. *Knutsson* discloses the “short-range wireless data communication means 9 to the lock device 40” using “**IEEE 802.11**.” *Knutsson*, 13:31-13:34, 22:15-19. IEEE 802.11 corresponds to Wi-Fi, as explained for claim 6 in Section VI.G. Ex-1003, ¶119.

Q. [Claim 23] The access control system of claim 15, wherein the **application automatically connects to the access device** via the **second communication protocol** as the **portable terminal approaches the access device**.

Knutsson renders obvious claim 23. Ex-1003, ¶120. *Knutsson* discloses “[t]he CPU 313 is programmed to read and execute program instructions stored in a memory 311 so as to perform a method for wireless **automatic** unlocking in response to the appearance and proper authentication of a key device.” *Knutsson*, 17:9-11. *Knutsson* also discloses “authorization is based solely on the key device’s Bluetooth® address and the current time, both of which are detected **automatically** by the lock device 40 and require no interaction from the user (other than **bringing the key device near the lock device 40**).” *Id.*, 18:1-4; Ex-1003, ¶120.

Knutsson discloses that the key device communicates over a short-range communication, such as Bluetooth, *Knutsson*, 5:18-23, as further discussed in Section VI.I.6 for [15E]. Ex-1003, ¶121.

R. [Claim 24] The access control system of claim 15, wherein the reservation certificate is **encrypted**.

Knutsson renders obvious claim 24. Ex-1003, ¶122. *Knutsson* discloses “**all communication between key device and lock device may be encrypted** in accordance with an encryption algorithm.” *Knutsson*, 19:12-14. One of the communications between the key device and the lock device is the data object 12. *Id.*, 13:31-14:2. *Knutsson* similarly discloses “enhanced security is obtained by

configuring the administration device to **encrypt the contents of the generated data object.**” *Id.*, 6:13-17. *Knutsson*’s data object corresponds to the claimed “reservation certificate,” as discussed above in Section VI.B.4 for [1C]. Ex-1003, ¶122.

- S. [Claim 25] The access control system of claim 24, wherein the encrypted reservation certificate is **decrypted by the access device.**

Knutsson in view of *Woodson* renders obvious claim 25. *Knutsson* discloses the processing means of the lock device “may be configured to **decrypt** at least one of said first and second properties **of said data object using a decryption key.**” *Knutsson*, 8:19-22; Ex-1003, ¶123.

VII. GROUND 2: CLAIMS 8-14 AND 26-36 ARE RENDERED OBVIOUS BY *KNUTSSON*

A. Claim 8

Knutsson renders obvious claim 8. Ex-1003, ¶124.

1. [8p] “An **access control system** comprising:”

[8p] is identical to [1p]. *Knutsson* renders obvious [8p], as explained for [1p] in Section VI.B.1. Ex-1003, ¶125.

2. [8A] “an **access device** comprising a **communication module** connected to a **processor having control of a door lock;**”

[8A] is identical to [1A]. *Knutsson* renders obvious [8A], as explained for [1A] in Section VI.B.2. Ex-1003, ¶126.

3. [8B] “an **application** on a **portable terminal**; and”

[8B] is identical to [1B]. *Knutsson* renders obvious [8B], as explained for [1B] in Section VI.B.3. Ex-1003, ¶127.

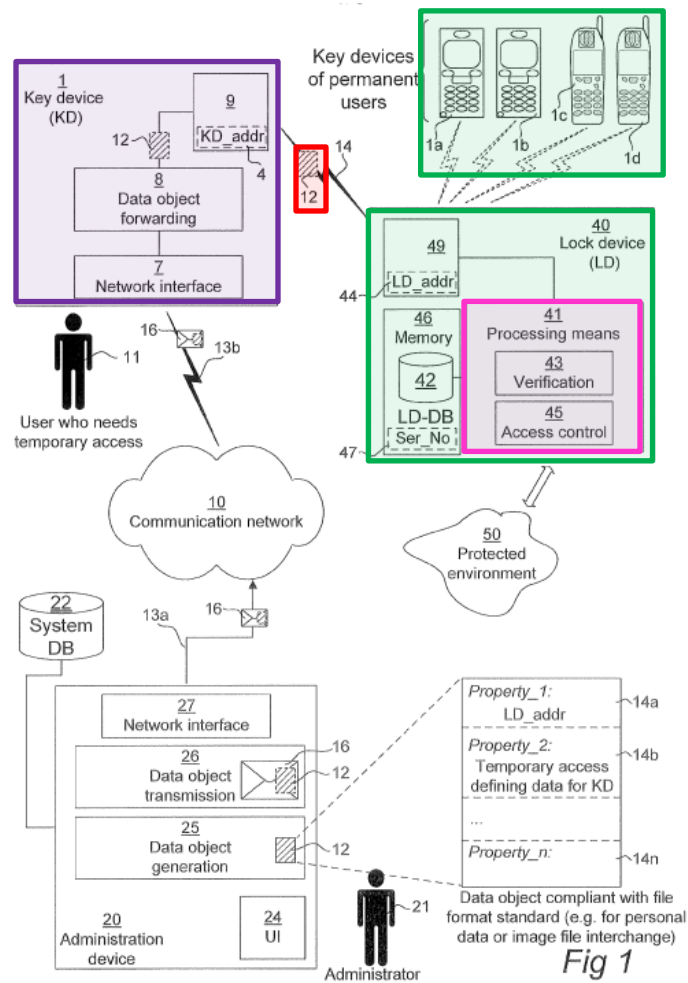
4. [8C] “a **server** to provide a **communication setting** and a reservation certificate to the application, the communication setting corresponding to the access device, and the reservation certificate comprising an **interval of a reservation**,”

[8C] is substantially similar to [1C]. *Knutsson* renders obvious [8C], as explained for [1C] in Section VI.B.4. Ex-1003, ¶128.

5. [8D] “wherein **the processor receives the reservation certificate** from the application based on use by the application of the communications setting,”

Knutsson renders obvious [8D]. Ex-1003, ¶129. As discussed above in Section VI.B.3, *Knutsson*’s key device is the claimed “portable terminal” and includes “a messaging application and a contacts application (or in the form of a **combined application** for messaging and contacts)” where its application “receives ... and detects the attached vCard 12,” shows properties of the vCard 12, allows storage of the vCard 12, and allows a command of sending the vCard 12 to lock device 40. *Knutsson*, 14:12-17, 14:20-23; Ex-1003, ¶129. *Knutsson*’s mobile terminal or key device’s functionality would be controlled through a software application through graphical interface 206 so the user could control functions of the key device. *Knutsson*, 13:25-28; Ex-1003, ¶129.

Knutsson discloses that its “lock device 40 will be integrated with or coupled to a lock mechanism in the lockable door or garage port and in particular have a controllable lock actuator configured to unlock the lock mechanism upon detection and successful authorization of the key device 1, based on the temporary access defining data.” *Knutsson*, 10:24-30. *Knutsson* discloses “[t]he key device also has data object forwarding functionality 8 capable of receiving the digital message 16 and forwarding the attached vCard data object 12 through short-range wireless data communication means 9 to the lock device 40, as seen at 14 in Fig 1.” *Id.*, 13:31-34. *Knutsson* further discloses “lock device 40 has processing means 41,” such as a CPU (processor) for controlling a door lock. *Id.*, 16:6-10, 17:11-13, 20:7-11; Ex-1003, ¶130.



Knutsson, FIG. 1.

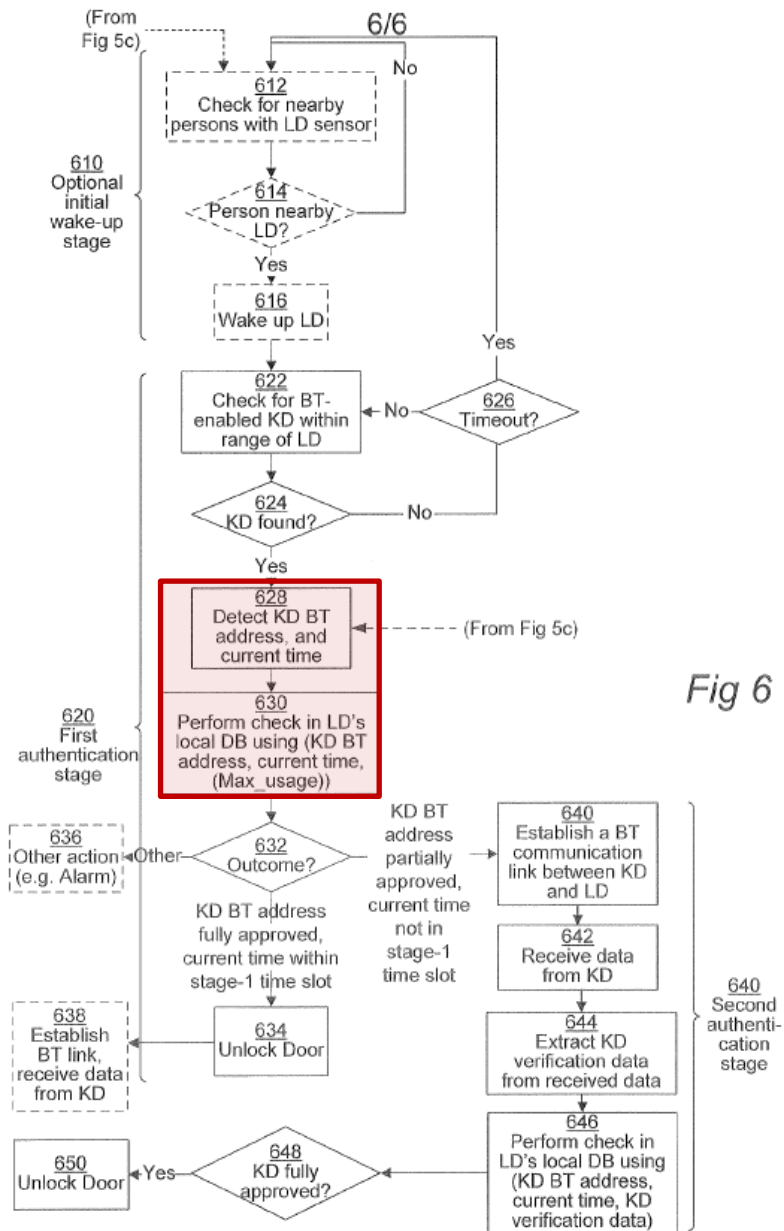
Knutsson discloses the claimed, “processor receives the reservation certificate from the application.” Ex-1003, ¶131. *Knutsson*’s software application is capable of receiving a user command to “Send by Bluetooth®” to “cause the key device 1 to attempt to establish short-range data communication 14 with the lock device 40.” *Id.*, 14:20-23. “When a Bluetooth® link 14 has been duly established between the key device 1 and lock device 40, the data object (vCard) 12 will be transmitted by the key device 1 in step 526 and be received by the lock device 40

in step 538.” *Id.*, 16:1-3. As discussed above in Section VI.B.4, *Knutsson*’s data object 12 comprises a Bluetooth address. Ex-1003, ¶131.

Because the communication identifier which, as described above, is a Bluetooth address (communication setting), is conferred to the lock device 40 (access device), and the communication means is a short-range communication, such as Bluetooth, initiated by the user command through the software application on key device 1, a POSA would have found it obvious that *Knutsson*’s data object 12, including a Bluetooth address, is sent to the lock device 40 from the application when Bluetooth is used by the application. Ex-1003, ¶132.

6. [8E] “wherein **the processor compares the interval** of the reservation **to a current time** accessible to the processor to determine if the reservation certificate is current and”

Knutsson renders obvious [8E]. Ex-1003, ¶133. *Knutsson*’s lock device 40, “includes a real-time clock 304 capable of providing the CPU 313 with an accurate value of the current time,” *Knutsson*, 17:21-22, and “the CPU 313 ... **[checks]** **whether the current time falls within any stage-1 time slot** defined for that Bluetooth® address.” *Id.*, 20:4-7; FIG. 6 at 628-630. “[T]emporal data is specified in a calendar data format, for instance in the form of one [or] more dates and/or times which define start and end points for permitted temporary access.” *Id.*, 6:4-6; Ex-1003, ¶133.



Knutsson, FIG. 6.

Knutsson’s **stage 1 authentication** determines “authorization is based solely on the key device’s Bluetooth® address and the current time.” *Id.*, 18:1-4. A

structure that the look device 40 uses to store authentication data is shown below.

Ex-1003, ¶134.

Field	Contents example #1	Contents example #2
LD ID	121	121
User name	Lars	Jonas
Key device BT ID	0x00223af3	0x002e5af4
Stage-1 time slot (1)	2005-03-24: 19-22	
Stage-1 time slot (2)	Mon-Fri: 07-15	
...		
Stage-1 time slot (n)		
Stage-2 time slot – single		
Stage-2 time slot – scheduled	00-24	Sat-Sun: 10-18
PIN code	****	****
Administrator	No	No

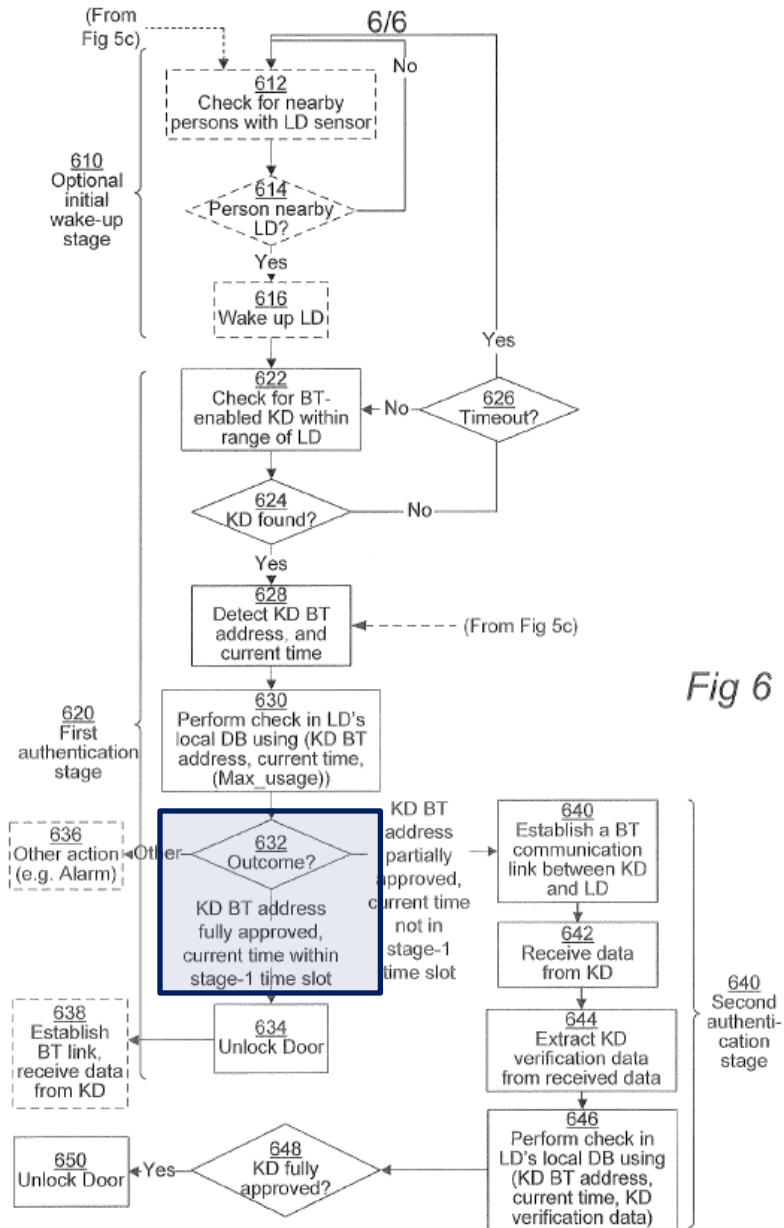
Knutsson, Table 1 at 18.

Knutsson’s time slot, from start to end times, corresponds to the claimed “interval,” because an interval is set forth by start and end points, as discussed above in Section VI.B.3. Ex-1003, ¶135.

7. [8F] “wherein the processor **activates the door lock** when the processor determines that the reservation certificate is current.”

Knutsson renders obvious [8F]. Ex-1003, ¶136. *Knutsson* discloses that its CPU 313 checks “whether the current time falls within any stage-1 time slot defined for that Bluetooth® address. If the outcome of these checks is fully positive, as checked in [step 632](#), the CPU 313 proceeds to step 634 and generates the control signal 307a to the actuator controller 307. As described above, this will

cause unlocking of the lock ... and allow[s] opening of the door.” *Knutsson*, 20:4-11; Ex-1003, ¶136.



Knutsson, FIG. 6.

In other words, *Knutsson* discloses “**authorization** is based solely on the key device’s Bluetooth® address and **the current time.**” *Id.*, 18:1-4; Ex-1003, ¶137.

- B. [Claim 9]** “The access control system of claim 8, wherein the communication setting is specific to the access device.”

Claim 9 is identical to claim 2 aside from its dependency from claim 8.

Knutsson renders obvious claim 9, as explained for claim 2 in Section VI.C. Ex-1003, ¶138.

- C. [Claim 10]** “The access control system of claim 9, wherein the application notifies the user of proximity to the access device.”

Claim 10 is identical to claim 3 aside from its dependency from claim 8.

Knutsson renders obvious claim 10, as explained for claim 3 in Section VI.D. Ex-1003, ¶139.

- D. [Claim 11]** “The access control system of claim 8, wherein the communication module does not advertise that the communication module is present.”

Claim 11 is identical to claim 4 aside from its dependency from claim 8.

Knutsson renders obvious claim 11, as explained for claim 4 in Section VI.E. Ex-1003, ¶140.

- E. [Claim 12]** “The access control system of claim 8, wherein the application uses Bluetooth to communicate with the access device and the communication setting comprises a Bluetooth ID.”

Claim 12 is identical to claim 5 aside from its dependency from claim 8.

Knutsson renders obvious claim 12, as explained for claim 5 in Section VI.F.

Ex-1003, ¶141.

- F. [Claim 13]** “The access control system of claim 8, wherein the application uses Wi-Fi to communicate with the access device and the communication setting comprises a network SSID.”

Claim 13 is identical to claim 6 aside from its dependency from claim 8.

Knutsson renders obvious claim 13, as explained for claim 6 in Section VI.G.

Ex-1003, ¶142.

- G. [Claim 14]** “The access control system of claim 8, wherein the reservation certificate comprises the communication setting.”

Claim 14 is identical to claim 7 aside from its dependency from claim 8.

Knutsson renders obvious claim 14, as explained for claim 7 in Section VI.H.

Ex-1003, ¶143.

H. Claim 26

Knutsson renders obvious claim 26. Ex-1003, ¶144.

- 1. [26p]** “An access control system comprising:”

[26p] is identical to [1A]. *Knutsson* renders obvious [26p], as explained for [1A] in Section VI.B.2. Ex-1003, ¶145.

2. **[26A]** “an access device comprising a communication module connected to a processor having control of a door lock;”

[26A] is identical to [1A]. *Knutsson* renders obvious [26A], as explained for [1A] in Section VI.B.2. Ex-1003, ¶146.

3. **[26B]** “an application on a portable terminal; and”

[26B] is identical to [1B]. *Knutsson* renders obvious [26B], as explained for [1B] in Section VI.B.3. Ex-1003, ¶147.

4. **[26C]** “a server to provide a communication setting to the application, the communication setting corresponding to the access device, and further to provide, via a first communication protocol, a reservation certificate to the application, the reservation certificate comprising an interval of a reservation,”

[26C] is identical to [15C]. *Knutsson* renders obvious [26C], as explained for [15C] in Section VI.I.4. Ex-1003, ¶148.

5. **[26D]** “wherein the processor receives the reservation certificate from the application via a second communication protocol that is different from the first communication protocol, based on use by the application of the communication setting,”

[26D] is substantially similar to [8D]. *Knutsson* renders obvious [26D], as explained for [8D] in Section VII.A.5. Regarding “a second communication protocol that is different from the first communication protocol,” *Knutsson* renders obvious this limitation, as discussed above for [15E] in Section VI.I.6. Ex-1003, ¶149.

6. [26E] “wherein the processor compares the interval of the reservation to a current time accessible to the processor to determine if the reservation certificate is current; and”

[26E] is identical to [8E]. *Knutsson* renders obvious [26E], as explained for [8E] in Section VII.A.6. Ex-1003, ¶150.

7. [26F] “wherein the processor activates the door lock when the processor determines that the reservation certificate is current.”

[26F] is identical to [8F]. *Knutsson* renders obvious [26F], as explained for [8F] in Section VII.A.7. Ex-1003, ¶151.

- I. [Claim 27] “The access control system of claim 26, wherein the first communication protocol comprises a cellular protocol.”

Claim 27 is identical to claim 16, aside from its dependency from claim 26. *Knutsson* renders obvious claim 27, as explained for claim 16 in Section VI.J; Ex-1003, ¶152.

- J. [Claim 28] “The access control system of claim 26, wherein the first communication protocol comprises a wireless LAN protocol.”

Claim 28 is identical to claim 17, aside from its dependency from claim 26. *Knutsson* renders obvious claim 28, as explained for claim 17 in Section VI.K; Ex-1003, ¶153.

- K. [Claim 29]** “The access control system of claim 28, wherein the wireless LAN protocol comprises Wi-Fi.”

Claim 29 is identical to claim 18, aside from its dependency from claim 28.

Knutsson renders obvious claim 29, as explained for claim 18 in Section VI.L;
Ex-1003, ¶154.

- L. [Claim 30]** “The access control system of claim 26, wherein the second communication protocol comprises a short-range wireless protocol.”

Claim 30 is identical to claim 19, aside from its dependency from claim 26.

Knutsson renders obvious claim 30, as explained for claim 19 in Section VI.M;
Ex-1003, ¶155.

- M. [Claim 31]** “The access control system of claim 30, wherein the short-range wireless protocol comprises Bluetooth.”

Claim 31 is identical to claim 20 aside from its dependency from claim 30.

Knutsson renders obvious claim 31, as explained for claim 20 in Section VI.N;
Ex-1003, ¶156.

- N. [Claim 32]** “The access control system of claim 26, wherein the second communication protocol comprises a wireless LAN protocol.”

Claim 32 is identical to claim 21 aside from its dependency from claim 26.

Knutsson renders obvious claim 32, as explained for claim 21 in Section VI.O;
Ex-1003, ¶157.

- O. [Claim 33]** “The access control system of claim 32, wherein the wireless LAN protocol comprises Wi-Fi.”

Claim 33 is identical to claim 22, aside from its dependency from claim 32.

Knutsson renders obvious claim 33, as explained for claim 22 in Section VI.P;
Ex-1003, ¶158.

- P. [Claim 34]** “The access control system of claim 26, wherein the application automatically connects to the access device via the second communication protocol as the portable terminal approaches the access device.”

Claim 34 is identical to claim 23, aside from its dependency from claim 26.

Knutsson renders obvious claim 34, as explained for claim 23 in Section VI.Q;
Ex-1003, ¶159.

- Q. [Claim 35]** “The access control system of claim 26, wherein the reservation certificate is encrypted.”

Claim 35 is identical to claim 24, aside from its dependency from claim 26

Knutsson renders obvious claim 35, as explained for claim 24 in Section VI.R;
Ex-1003, ¶160.

- R. [Claim 36]** “The access control system of claim 35, wherein the encrypted reservation certificate is decrypted by the access device.”

Claim 36 is identical to claim 25, aside from its dependency from claim 35.

Knutsson renders obvious claim 36, as explained for claim 25 in Section VI.S;
Ex-1003, ¶161.

VIII. GROUND 3: CLAIM 3 IS RENDERED OBVIOUS BY *KNUTSSON* IN VIEW OF *WOODARD* AND *BRÖNDRUP*

A. Motivation to Combine *Knutsson*, *Woodard*, and *Bröndrup*

As explained in Section III, claim 3 requires the application of the mobile terminal to notify the user of the proximity of the lock. Ex-1003, ¶162.

To the extent that it is argued that *Knutsson* does not disclose this element, *Bröndrup* does. Ex-1003, ¶163. A POSA would have been motivated to implement *Bröndrup*'s notification system into *Knutsson*'s lock device 40 because *Bröndrup* discloses a goal of avoiding a guest being “checked in through the reception desk, at which there is at times a long queue waiting for check in.” *Bröndrup*, 2:10-13; Ex-1003, ¶163. A POSA would thus have incorporated *Bröndrup*'s notification concepts into *Knutsson*'s access system to “integrate functions of previously separate systems to provide wireless hotel search, reservation/booking, check-in, room access control.” *Bröndrup*, 3:10-14; Ex-1003, ¶163. *Woodard* similarly discloses “automatically controlling access to an electronic lockbox utilizing showing appointment data maintained by a central showing management system.” *Woodard*, [0010]. Besides integrating separate systems to perform room access control and thus maintaining central control, a POSA would have been further motivated to implement *Bröndrup* so that *Knutsson*'s key device 1 would be

capable of check-in “without having to make a check-in at the reception desk of the hotel.” *Bröndrup*, 11:17-20; Ex-1003, ¶163.

A POSA would have had a reasonable expectation of adding *Bröndrup*’s proximity notification to *Knutsson-Woodard* because *Bröndrup*’s use of Bluetooth between a mobile terminal and a door lock to enable unlocking a nearby door is similar to *Knutsson*’s key device 1, a mobile terminal, which communicates through Bluetooth to lock device 40 when the mobile terminal draws near. Ex-1003, ¶164. *Bröndrup*, *Woodard*, and *Knutsson* disclose similar key devices such as *Bröndrup*’s “mobile terminal 1 of the system in this example includes a typical mobile telephone and processing unit 23 provided with appropriate wireless application programs,” *Bröndrup*, 6:4-7, and *Knutsson*’s key device is a mobile phone, *Knutsson*, 4:32-5:4, and *Woodard*’s “electronic key device 104, ... a cell phone.” *Woodard*, [0003]. These key devices control similar access devices like *Bröndrup*’s wireless door lock (9, 32), *Bröndrup*, Abstract, or *Knutsson*’s lock device 40, *Knutsson*, 10:24-30, or *Woodard*’s lockbox 103. *Woodard*, [0048]; Ex-1003, ¶164.

B. [Claim 3] The access control system of claim 2, wherein the application **notifies the user of proximity** to the access device.

Knutsson in view of *Woodard* and *Bröndrup* renders obvious claim 3.

Ex-1003, ¶165. To the extent it is argued that *Knutsson* does not disclose

“notifying a user,” *Bröndrup* does. *Bröndrup* discloses “[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, and unlocks the door. The user is notified of the event.” *Bröndrup*, 7:30-35. *Bröndrup* discloses that through the “wireless device in the mobile wireless terminal, the key token is transmitted to nearby wireless devices associated with electrically operable door locks.” *Id.*, 7:28-30. A POSA would have thus found it obvious that the notification would be sent to a user of the mobile phone, just like an alarm or report in *Knutsson*’s system, *id.*, 20:17-19, when the mobile terminal is near the door lock. Ex-1003, ¶165. Because the key device 1 communicates with lock device 40, a POSA would have found it obvious that *Knutsson*’s key device software application would have received *Bröndrup*’s notification because it would have been the quickest way to alert the user through an established short-range communication method. Ex-1003, ¶165. A POSA would have further found it obvious that *Bröndrup*’s short range wireless device 25 of the mobile wireless terminal 1 communicating to the door lock 32 through Bluetooth corresponds to the claimed “proximity to the access device,” because the Bluetooth communication is near to the door lock 32. *Id.* A POSA would have further been

motivated to combine *Knutsson*, *Woodard*, and *Bröndrup*, as discussed above in Section VIII.A. *Id.*

IX. GROUND 4: CLAIM 4 IS RENDERED OBVIOUS BY *KNUTSSON* IN VIEW OF *WOODARD* AND *ADAMS*

A. Motivation to Combine *Knutsson*, *Woodard*, and *Adams*

As explained in Section III, claim 4 requires that the communication module does not advertise that the communication module is present. Ex-1003, ¶166.

Knutsson renders obvious a communication module being non-operational and thus not sending advertising signals, as explained for claim 4 in Ground 1, Section VI.E. To the extent that it is argued that *Knutsson* does not disclose this element, *Adams* does. A POSA would have been motivated to implement *Adams*'s non-discoverable mode into *Knutsson*'s lock device 40. *Adams* explains the desirability of being non-discoverable because “[t]here are a greater number of security concerns when a [Bluetooth] device is discoverable” including “eavesdropping on the data transferred during the communication of two [Bluetooth] devices, and the ability to fully impersonate other [Bluetooth devices].” *Adams*, [0006]; Ex-1003, ¶167. A POSA would have thus implemented *Adams*'s non-discoverable mode into *Knutsson*'s Bluetooth-capable devices to avoid eavesdropping of protected data, such as *Knutsson*'s time and location information within its data object 12. Ex-1003, ¶167. Likewise, a POSA would

have been motivated to achieve *Woodard*'s goals of controlling access to an access device "accurately" and ensuring an "authorized" person accesses the correct property. *Woodard*, [0007]-[0009]. Additionally, a POSA would have incorporated *Adams*'s non-discoverable mode into *Knutsson*'s lock device to achieve *Knutsson*'s goal of "enhanced security" and access control for a user to enter a protected environment, *Knutsson*, 6:13-17, 10:13-14, 11:7-11, by ensuring that another device would not be able to impersonate *Knutsson*'s key device 1 and thus allow an infiltrator to access *Knutsson*'s protected environment. Ex-1003, ¶167.

A POSA would have had reasonable expectations of success implementing *Adams*'s non-discoverable mode to *Knutsson*'s lock device because *Adams* explains "[t]he Bluetooth® v1.1 and v1.2 specifications include provisions for ... [a] Non-Discoverable Mode." *Adams*, [0003]; Ex-1003, ¶168. *Knutsson* disclose key and lock devices that use Bluetooth® to communicate with each other through their Bluetooth® transceivers. *Knutsson*, 12:3-7, 13:34-14:2, 14:20-23, 15:24-25, 17:16-20. *Woodard* similarly discloses an electronic key device that connects to the electronic lock box 103 via a wireless communications link. *Woodard*, [0066], FIG. 5. Because *Knutsson*'s key and lock devices communicate through Bluetooth® and employ Bluetooth® transceivers, a POSA would have found it obvious that *Knutsson*'s devices would implement features of the Bluetooth® specifications, including the non-discoverable mode common to Bluetooth®

devices. Ex-1003, ¶164. A POSA would have further been successful in implementing *Adams*'s "Non-Discoverable Mode" because *Knutsson*'s lock device operates based on receiving a Bluetooth® address. Ex-1003, ¶168. *Adams* explains that, "[e]ven when not discoverable, a [Bluetooth] device is visible to other [Bluetooth] devices and users that are familiar with its Bluetooth® device address." *Adams*, [0005]; Ex-1003, ¶168. Thus, although *Knutsson*'s lock device is in Non-Discoverable Mode, *Knutsson*'s key device would communicate with the lock device to grant access to a protected environment because *Knutsson* explains its key device uses the lock device's Bluetooth address to communicate with the lock device. Ex-1003, ¶168.

B. [Claim 4] The access control system of claim 1, wherein the communication module **does not advertise that the communication module is present.**

Knutsson in view of *Adams* renders obvious claim 4. Ex-1003, ¶169. To the extent it is argued that *Knutsson* does not disclose "not advertis[ing] that the communication module is present," *Adams* does. *Adams* discloses "[t]he Bluetooth® v1.1 and v1.2 specifications include provisions for ... [a] **Non-Discoverable Mode.**" *Adams*, [0003]. "A [Bluetooth] device that does not respond to inquiry messages due to being in Non-Discoverable Mode or due to other baseband activity is called a silent device." *Adams*, [0004]. Because the device is "silent" in non-discoverable mode, a POSA would have understood the device

does not announce or advertise its presence. Ex-1003, ¶169. As *Adams* explains, in the Non-Discoverable Mode, “a [Bluetooth] device is visible to other [Bluetooth] devices and users that are familiar with its Bluetooth® device address.” *Adams*, [0005]. However, devices unfamiliar with the Bluetooth® device address would be unable to find the lock device because it is not discoverable (i.e., it is not advertised). Ex-1003, ¶169. A POSA would have been motivated to combine *Knutsson* and *Adams*, as discussed above in Section IX.A. *Id.*

X. GROUND 5: CLAIM 10 IS RENDERED OBVIOUS BY *KNUTSSON* IN VIEW OF *BRÖNDRUP*

A. Motivation to Combine *Knutsson* and *Bröndrup*

As explained in Section III, to the extent it is argued that *Knutsson* does not disclose the notification limitation, *Bröndrup* does. Ex-1003, ¶170. A POSA would have been motivated to combine *Knutsson* and *Bröndrup*, as disclosed in Section VIII.A. The further combination of *Woodard* in Section VIII.A does not affect the combination of *Knutsson* and *Bröndrup*, and a POSA would have been motivated to combine *Knutsson* and *Bröndrup* for the same reasons discussed above in Section VIII.A. Ex-1003, ¶171.

B. [Claim 10] “The access control system of claim 9, wherein the application **notifies the user of proximity to the access device.”**

Claim 10 is identical to claim 3 aside from its dependency from claim 9. *Knutsson* in view of *Bröndrup* renders obvious claim 10, as explained for claim 3

in Section VIII.B. The further combination of *Woodard* in Section VIII.A does not affect the combination of *Knutsson* and *Bröndrup*, and a POSA would have been motivated to combine *Knutsson* and *Bröndrup* for the same reasons discussed above in Sections VIII.A and X.A. Ex-1003, ¶172.

XI. GROUND 6: CLAIM 11 IS RENDERED OBVIOUS BY *KNUTSSON* IN VIEW OF *ADAMS*

A. Motivation to Combine *Knutsson* and *Adams*

As explained in Section III, to the extent it is argued that *Knutsson* does not disclose the communication module not advertising itself, *Adams* does, as explained for claim 4 in Ground 4, Section IX.B. Ex-1003, ¶173. The further combination of *Woodard* in Section IX.A does not affect the combination of *Knutsson* and *Adams*, and a POSA would have been motivated to combine *Knutsson* and *Adams* for the same reasons discussed above in Section IX.A. Ex-1003, ¶174.

B. [Claim 11] “The access control system of claim 8, wherein the communication module **does not advertise that the communication module is present.”**

Claim 11 is identical to claim 4 aside from its dependency from claim 8. *Knutsson* in view of *Adams* renders obvious claim 11, as explained for claim 4 in Section IX.B. A POSA would have been motivated to combine *Knutsson* and *Adams* as explained in Sections IX.A and XI.A. Ex-1003, ¶175.

**XII. GROUND 7: CLAIMS 6, 17, AND 18 ARE RENDERED OBVIOUS BY
KNUTSSON IN VIEW OF *WOODARD* AND *JAIN***

A. Motivation to Combine *Knutsson*, *Woodard*, and *Jain*

As explained in Section III, to the extent it is argued *Knutsson* does not expressly disclose the communication setting comprising an SSID, *Jain* does. Ex-1003, ¶¶176-177. A POSA would have been motivated to implement *Jain*'s SSID identifier into *Knutsson*'s lock device 40 because *Jain* discloses “[i]f the locally-stored ID matches the request ID,” the CPU 408 of card 400 associated with a mobile phone will activate the antenna 402 “to enable access.” *Jain*, [0068]; Ex-1003, ¶177. A POSA would thus have incorporated *Jain*'s SSID identifier into *Knutsson*'s access system when *Knutsson*'s access system is implemented on a Wi-Fi system. Ex-1003, ¶177. Because *Knutsson* describes that its system is implemented on an IEEE 802.11 (Wi-Fi) system, *Knutsson*, 22:15-19, it is my opinion that a POSA would have looked to *Jain* to implement the Wi-Fi system including modifying *Knutsson*'s communication identifier to be an SSID identifier. Ex-1003, ¶177. Combining *Jain*'s SSID identifier and *Knutsson*'s communication identifier would lead to predictable results of allowing access to the access device, *Knutsson*'s lock device 40. Ex-1003, ¶177. A POSA also would have found the substitution of *Jain*'s SSID identifier for a Wi-Fi network for *Knutsson*'s communication identifier would yield predictable results of allowing access when

the SSID of data object 12 matches the SSID of the lock device 40 when implementing *Knutsson*'s Wi-Fi system. Ex-1003, ¶177.

A POSA would have had reasonable expectations of success implementing *Jain*'s SSID within *Knutsson* because *Jain* and *Knutsson* disclose similar key devices, such as *Jain*'s host device that includes “a cellphone [or] a smartphone.” *Jain*, [0018], and *Knutsson*'s key device that can be a mobile phone. *Knutsson*, 4:32-5:4. Ex-1003, ¶178. These devices communicate with similar access devices like *Jain*'s computer used for “physical access control,” *Jain*, [0030], and *Knutsson*'s lock device 40 to open a lock, *Knutsson*, 10:24-30, if an identification from the key devices match the lock devices. Ex-1003, ¶178.

A POSA would have been motivated to combine *Woodard* with *Jain* and *Knutsson* for the reasons discussed in Ground 1, Section VI.A. Ex-1003, ¶178.

B. [Claim 6] “The access control system of claim 1, wherein the application **uses Wi-Fi** to communicate with the access device and the communication setting comprises **a network SSID**.”

To the extent it is argued that *Knutsson* does not expressly disclose the claimed network SSID, *Jain* does. Ex-1003, ¶180.

Jain discloses “the host device may be a cellphone such that the card 400 may request network authentication prior to activation” where authentication requires “a unique identity about the allowed network [to be] locally stored in memory such [as] a Mobile Network Code for GSM networks, a NID for CDMA

networks, **a SSID for broadband networks**, and/or identifiers.” *Jain*, [0068]. *Jain* discloses a “software plug-in” of the cellphone “may query the host device to respond with network details If the locally-stored ID matches the request ID, the CPU 408 activated the antenna 402 to enable access or otherwise services are denied.” *Id.*; Ex-1003, ¶181.

A POSA would have further been motivated to combine *Woodard*, *Knutsson*, and *Jain* for the reasons explained in Section XII.A. Ex-1003, ¶182.

A POSA would have been motivated to modify *Knutsson*’s data object 12, which includes a communication identifier for a Wi-Fi network, by incorporating *Jain*’s “unique identity about the allowed network is locally stored in memory such [as] ... a SSID for broadband networks.” *Jain*, [0068]. As *Jain* explains, this “unique identity” will be checked, and access will be granted if the identity is verified. *Jain*, like *Knutsson* and *Woodard*, discloses methods where host devices, such as mobile phones, use wireless communications with an access device, such as a processor as part of POS 114, to have “physical access control (to open gates either in a corporate environment or in a transit environment).” *Id.*, [0030], [0037]; Ex-1003, ¶183. *Jain*, like *Knutsson* and *Woodard*, uses “identifiers” and authorization methods to access services over conventional wireless networks, like Bluetooth and Wi-Fi. *Jain*, [0068]-[0069]. A POSA thus would have been motivated to combine *Knutsson*, *Woodard*, and *Jain*, and would have had a

reasonable expectation of success in doing so because all three references use similar identification methods for mobile phones for wireless access to physical controls. Ex-1003, ¶183.

C. [Claim 17] “The access control system of claim 15, wherein the first communication protocol comprises a **wireless LAN protocol**.”

Knutsson in view of *Woodard* and *Jain* renders obvious claim 17. Because claim 18 depends from claim 17, Wi-Fi is a type of “wireless LAN protocol” as stated in claim 18, and *Jain*’s disclosure of Wi-Fi thus corresponds to claim 17’s “wireless LAN protocol.” Ex-1003, ¶184.

As explained for [15C] in Section VI.I.4, *Knutsson* also discloses that its devices are capable of communicating through “a wireless local area network (WLAN) standard.” *Knutsson*, 22:15-19; Ex-1003, ¶185.

To the extent *Knutsson* does not expressly disclose the “first communication protocol comprises a wireless LAN protocol,” *Jain* does. *Jain* discloses “[i]n regards to the short-range wireless interface 508, the financial institutions 106 may wirelessly communicate with the transaction card 112f using, for example, WiFi technology.” *Jain*, [0069]. *Jain* discloses its mobile device 110 containing transaction card 112 and GUI 111, *id.*, [0021], FIG. 1, communicates with financial institution 106 as “an efficient and user-friendly means for the user to

self-manage settings and access services offered by the financial institution.” *Id.*, [0022]; Ex-1003, ¶186.

A POSA would have found it obvious that *Jain*’s use of Wi-Fi between its mobile device 110 and financial institution 106 would be implemented between *Knutsson*’s key device 1 and administrative device 20. Ex-1003, ¶187. Both *Jain* and *Knutsson* disclose mobile phones that access physical controls or locks and further that communicate with a computer, such as financial institution 106 or administrative device 20, to authenticate the access before accessing the offered services. *Id.* A POSA would have found it obvious that Wi-Fi would be used by a mobile phone to communicate with another computer because Wi-Fi was a known, conventional option for communication for mobile phones, and its implementation would have been a predictable use of one of a limited number of communication technologies. *Id.* Thus, a POSA would have found claim 17 obvious over *Knutsson* in view of *Jain* and *Woodard*, as further explained in Section XII.A. *Id.*

D. [Claim 18] “The access control system of claim 17, wherein the wireless LAN protocol comprises **Wi-Fi**.”

Knutsson in view of *Jain* and *Woodard* renders obvious claim 18, as explained for claim 17 in Section XII.C. Ex-1003, ¶188. *Jain* discloses that “the financial institutions 106 may wirelessly communicate with the transaction card 112f using, for example, **WiFi technology**.” *Jain*, [0069]. A POSA would have

been motivated to combine *Jain* and the *Knutsson-Woodard* combination, as discussed for claim 17 in Sections XII.C and XII.A. Ex-1003, ¶189.

XIII. GROUND 8: CLAIMS 13, 28, AND 29 ARE RENDERED OBVIOUS BY *KNUTSSON* IN VIEW OF *JAIN*

A. Motivation to Combine *Knutsson* and *Jain*

As explained in Section III, to the extent it is argued that *Knutsson* does not disclose an SSID, *Jain* does, as explained for claim 6, Ground 7, discussed in Section XII.B. Ex-1003, ¶190. The further combination of *Woodard* in Section XII.A does not affect the combination of *Knutsson* and *Jain*, and a POSA would have been motivated to combine *Knutsson* and *Jain* for the reasons discussed in Section XII.A. *Id.*

B. [Claim 13] “The access control system of claim 8, wherein the application uses **Wi-Fi to communicate with the access device and the communication setting comprises a **network SSID**.”**

Claim 13 is identical to claim 6 aside from its dependency from claim 8. *Knutsson* in view of *Jain* renders obvious claim 13, as explained for claim 6 in Section XII.B. A POSA would have been motivated to combine *Jain* and *Knutsson*, as explained in Section XIII.A. Ex-1003, ¶191.

- C. **[Claim 28]** “The access control system of claim 26, wherein the first communication protocol comprises a **wireless LAN protocol**.”

Knutsson in view of *Jain* renders obvious claim 28, as explained for claim 17 in Section XII.C. A POSA would have been motivated to combine *Jain* and *Knutsson*, as discussed above for Section XIII.A. Ex-1003, ¶192.

- D. **[Claim 29]** The access control system of claim 28, wherein the wireless LAN protocol comprises **Wi-Fi**.

Knutsson in view of *Jain* renders obvious claim 29, as explained for claim 18 in Section XII.D. A POSA would have been motivated to combine *Jain* and *Knutsson*, as discussed above for Section XIII.A. Ex-1003, ¶193.

XIV. DISCRETIONARY DENIAL IS IMPROPER

Non-institution under § 314(a) would be improper because no factors articulated in *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 5-6 (PTAB Mar. 20, 2020), weigh in favor of non-institution. No effective trial date has been set in either *Liberty Access Technologies Licensing LLC v. ASSA ABLOY AB et al.*, 2:22-cv-00507 (E.D. Tex.) (“the -00507 case”) or *ASSA ABLOY Global Solutions, Inc. v. Liberty Access Technologies Licensing LLC*, 1:23-cv-00756 (N.D. Ill.) (“the -00756 case”). Ex-1011; Ex-1015. These cases are in their infancy. No invalidity contentions have been asserted and no *Markman* hearing date has been set. Petitioners filed counterclaims asserting invalidity in the -00756 case, but those counterclaims do not create a bar to institution. 35 U.S.C. § 315(a)(3); *Canfield*

Scientific, Inc. v. Melanoscan, LLC, IPR2017-02125, Paper 7 (P.T.A.B. Mar. 30, 2018). Petitioners intend to seek a stay of these cases pending this IPR, and there is a high likelihood that a stay will be granted in the co-pending case because there has been virtually no investment in the parallel proceeding. Moreover, as invalidity allegations and contentions have not been asserted, there are no overlap of issues with this Petition.

Further, this Petition's grounds include compelling merits, challenging all claims with only minor modifications of § 102(b) references.

Non-institution under § 325(d) would also be improper based on a weighing of the factors set forth in *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 (PTAB Dec. 15, 2017). The asserted combinations are materially different and not cumulative of the prior art involved during the examination of the challenged claims. During prosecution, **no** references were applied by the Office, and the claims were issued only a double patenting rejection, Ex-1002 at 102-06, before being allowed barely seven months after being filed. Ex-1001 at 1.

The prior art references presented in this Petition were never listed by the Patent Owner nor cited by any examiner with the exception of *Bröndrup* discussed below. None of the references were discussed or applied by the Examiner to reject any claims. The references are materially different from and not cumulative of the

earlier references, at least because they describe (1) a door lock with a processor able to communicate with a portable terminal to open it; (2) an application on the portable terminal; (3) a server that provides a communication identifier and reservation information to the application; and (4) checking the time and identifier to activate the door lock. Although a U.S. publication equivalent of *Bröndrup* is listed on the face of the patent, Ex-1001, (56), the Office did not apply *Bröndrup* to any of the claims, Ex-1002, and the Office did not consider *Bröndrup* in combination with any other reference listed herein. Indeed, *Bröndrup* is only cited herein for minor limitations in dependent claims 3 and 10. There is thus little to no overlap between the current arguments and any consideration given to the art during prosecution. *Becton*, Paper 8, 23. But, as explained in this Petition, the cited references teach these added limitations, making denial under § 325(d) improper.

Shortly before this Petition was filed, Unified Patents LLC (“Unified”) filed an *ex parte* reexamination (“EPR”) of the ’474 patent, challenging claims 1, 2, 5-9, 14-16, 19-20, 24, 26-27, 30, and 35. Ex-1006, at 1-2. Unified proposes the following rejections:

Proposed Rejections	Claims	Basis	References
1	8, 9, 14, 26, 27, 30, and 35	§ 102	Anticipated by <i>Nielsen</i>
2	8, 9, 14, 26, 27, 30, and 35	§ 103	Obvious over <i>Nielsen</i>
3	1, 2, 5-7, 15-16, 19-20, and 24	§ 103	Obvious over <i>Nielsen</i> in view of <i>Kung</i> and <i>Buckingham</i>
4	1, 8, 15, 16, 19, 26, 27, and 30	§ 103	Obvious over <i>Ullmann</i> in view of <i>Barnes</i>

Ex-1006, 35.

Discretionary denial of this Petition in view of Unified's EPR is improper for the following reasons:

(1) Liberty has asserted claims 1-36 against Petitioner ASSA ABLOY Global Solutions, Inc. ("AAGS") in the -00507 case. Ex-1007, 2-265. Unified's EPR challenges only 17 of the claims, whereas this Petition challenges every asserted claim.

(2) Unified has not been accused of infringement, but AAGS has. AAGS should be entitled to challenge the claims asserted against it. Further, the interest of judicial efficiency favors resolving every claim asserted against AAGS in this Petition.

(3) There is no overlap of references between this Petition and Unified's EPR. Each challenge contains different grounds with completely different references.

(4) Petitioners developed the present Petition independently and without any knowledge of Unified's EPR before it was filed.

(5) The claims challenged by this Petition, obvious as discussed above, are materially different than those challenged in Unified's EPR. For example, claims 3 and 10 include limitations not found in independent claims 1 and 8, respectively, that "the application notifies the user of proximity of the access device." These claims are asserted against AAGS, Ex-1007, 47-49, 102-104, and are not challenged in Unified's EPR. Claims 4, 11-13, 21-23, 25, 28, 29, 31-34, and 36 similarly contain material differences from the independent claims, that have been asserted against AAGS, and Unified's EPR does not challenge their validity.

Accordingly, discretionary denial of this Petition would be improper.

XV. MANDATORY NOTICES

A. Real Parties-in-Interest

The real parties-in-interest are ASSA ABLOY AB, ASSA ABLOY Mobile Services AB,⁵ ASSA ABLOY Global Solutions, Inc., and ASSA ABLOY Global Solutions AB, HID Global Corp., and Marriott International, Inc.

⁵ ASSA ABLOY Mobile Services AB was named as a party in the -00507 case, but this entity does not exist and did not exist at the time.

B. Related Matters

Unified Patents LLC filed a request for *ex parte* reexamination of the '474 patent on May 11, 2023, Reexamination No. 90/015231.

Patent Owner has asserted the '474 patent in litigation filed on August 18, 2022, *Liberty Access Technologies Licensing LLC v. Marriott International, Inc.*, 2:22-cv-00318 (E.D. Tex.).

Patent Owner has asserted the '474 patent in litigation filed on Dec. 30, 2022, *Liberty Access Technologies Licensing LLC v. ASSA ABLOY AB et al.*, 2:22-cv-00507 (E.D. Tex.).

Petitioner ASSA ABLOY Global Solutions, Inc. asserted non-infringement of the '474 patent in a declaratory judgment action filed on February 7, 2023, *ASSA ABLOY Global Solutions, Inc. v. Liberty Access Technologies Licensing LLC*, 1:23-cv-00756 (N.D. Ill.).

C. Lead and Back-Up Counsel, and Service Information

LEAD COUNSEL	BACK-UP COUNSEL
Lionel Lavenue (Reg. No. 46,859) lionel.lavenue@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer Street, Suite 800 Reston, VA 20190-6023 Tel: (571) 203-2750 Fax: (571) 203-2777	Kara A. Specht (Reg. No. 69,560) kara.specht@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 271 17th Street, NW, Suite 1400 Atlanta, GA 30363-6209 Tel: (404) 653-6400 Fax: (404) 653-6444 R. Maxwell Mauldin (Reg. No. 78,626)

	r.maxwell.mauldin@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 271 17th Street, NW, Suite 1400 Atlanta, GA 30363-6209 Tel: (404) 653-6400 Fax: (404) 653-6444
--	---

XVI. GROUNDS FOR STANDING

Petitioners certify the '474 patent is available for IPR, and Petitioners are not barred or estopped from requesting IPR challenging the patent claims on the grounds identified in this Petition.

XVII. CONCLUSION

Petitioners have established a reasonable likelihood of prevailing with respect to each of the challenged claims 1-36 of the '474 patent. Petitioners therefore request the Board institute *inter partes* review and cancel each of these claims as unpatentable.

The Office may charge any required fees for this proceeding to Deposit Account No. 06-0916.

Date: May 25, 2023

Respectfully Submitted,

/Lionel M. Lavenue/

Lionel M. Lavenue, Lead Counsel
Reg. No. 46,859

CERTIFICATION UNDER 37 C.F.R. § 42.24(d)

Pursuant to 37 C.F.R. § 42.24(a)(1)(i), the undersigned hereby certifies that the foregoing PETITION FOR *INTER PARTES* REVIEW contains 13,942 words, excluding the parts of this Petition that are exempted under 37 C.F.R. § 42.24(a), as measured by the word-processing system used to prepare this paper.

/Lionel M. Lavenue/

Lionel M. Lavenue, Lead Counsel

Reg. No. 46,859

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(a), the undersigned certifies that the foregoing **Petition for *Inter Partes* Review, the associated Power of Attorneys, and Exhibits 1001 through 1015** are being served on May 25, 2023, by FedEx Priority Overnight on the correspondence address of record indicated in the Patent Office's Patent Center system for U.S. Patent No. 11,373,474.

John Kasha
Kasha Law LLC
14532 Dufief Mill Road
North Potomac, MD 20878

A courtesy copy has been served on litigation counsel at:

Carey Matthew Rozier
Rozier Hardt McDonough PLLC
2590 Walnut St. Ste 10
Denver, CO 80205

Date: May 25, 2023

/Daniel E. Doku/
Daniel E. Doku
Litigation Legal Assistant

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP