

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
Filing Date: January 3, 2022
Issue Date: June 28, 2022

Case No. IPR2023-00817

DECLARATION OF BENJAMIN B. BEDERSON, PH.D.

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	QUALIFICATIONS	2
III.	MATERIALS CONSIDERED	13
IV.	LEGAL PRINCIPLES	14
V.	THE '474 PATENT	17
VI.	OVERVIEW OF PRIOR ART	18
A.	<i>Knutsson</i>	18
B.	<i>Woodard</i>	19
C.	<i>Bröndrup</i>	21
D.	<i>Jain</i>	21
E.	<i>Adams</i>	22
VII.	LEVEL OF ORDINARY SKILL IN THE ART	23
VIII.	CLAIM CONSTRUCTION	24
IX.	SUMMARY OF OPINIONS	25
X.	GROUND 1: CLAIMS 1-7 AND 15-25 ARE RENDERED OBVIOUS BY KNUTSSON IN VIEW OF WOODARD	32
A.	Motivation to Combine <i>Knutsson</i> and <i>Woodard</i>	32
B.	Claim 1	33
1.	[1p] “An access control system comprising:”	34
2.	[1A] “an access device comprising a communication module connected to a processor having control of a door lock;”	35

3.	[1B] “an application on a portable terminal; and”	38
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,”	41
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”	50
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.”	53
C.	[Claim 2] The access control system of claim 1, wherein the communication setting is specific to the access device.	56
D.	[Claim 3] The access control system of claim 2, wherein the application notifies the user of proximity to the access device.	57
E.	[Claim 4] The access control system of claim 1, wherein the communication module does not advertise that the communication module is present.....	58
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.....	59
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.....	61
H.	[Claim 7] The access control system of claim 1, wherein the reservation certificate comprises the communication setting.	63
I.	Claim 15	63

1.	[15p] “An access control system comprising:”	63
2.	[15A] “an access device comprising a communication module connected to a processor having control of a door lock;”	64
3.	[15B] “an application on a portable terminal; and”	64
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,”	64
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”	65
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.”	65
J.	[Claim 16] The access control system of claim 15, wherein the first communication protocol comprises a cellular protocol.....	69
K.	[Claim 17] The access control system of claim 15, wherein the first communication protocol comprises a wireless LAN protocol.....	70
L.	[Claim 18] The access control system of claim 17, wherein the wireless LAN protocol comprises Wi-Fi.	71
M.	[Claim 19] The access control system of claim 15, wherein the second communication protocol comprises a short-range wireless protocol.....	72

N.	[Claim 20] The access control system of claim 19, wherein the short-range wireless protocol comprises Bluetooth.	73
O.	[Claim 21] The access control system of claim 15, wherein the second communication protocol comprises a wireless LAN protocol.....	73
P.	[Claim 22] The access control system of claim 21, wherein the wireless LAN protocol comprises Wi-Fi.	73
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.	74
R.	[Claim 24] The access control system of claim 15, wherein the reservation certificate is encrypted.....	74
S.	[Claim 25] The access control system of claim 24, wherein the encrypted reservation certificate is decrypted by the access device.....	75
XI.	GROUND 2: CLAIMS 8-14 AND 26-36 ARE RENDERED OBVIOUS BY KNUTSSON.....	75
A.	Claim 8	75
1.	[8p] “An access control system comprising:”.....	75
2.	[8A] “an access device comprising a communication module connected to a processor having control of a door lock;”	75
3.	[8B] “an application on a portable terminal; and”	76
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,”	76

5.	[8D] “wherein the processor receives the reservation certificate from the application based on use by the application of the communications setting,”	76
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”	79
7.	[8F] “wherein the processor activates the door lock when the processor determines that the reservation certificate is current.”	81
B.	[Claim 9] The access control system of claim 8, wherein the communication setting is specific to the access device.	84
C.	[Claim 10] The access control system of claim 9, wherein the application notifies the user of proximity to the access device.	84
D.	[Claim 11] The access control system of claim 8, wherein the communication module does not advertise that the communication module is present.....	84
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.....	84
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.....	85
G.	[Claim 14] The access control system of claim 8, wherein the reservation certificate comprises the communication setting.	85
H.	Claim 26	85
1.	[26p] “An access control system comprising:”	85
2.	[26A] “an access device comprising a communication module connected to a processor having control of a door lock;”	85

3.	[26B] “an application on a portable terminal; and”	85
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,”	86
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,”	86
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”	86
7.	[26F] “wherein the processor activates the door lock when the processor determines that the reservation certificate is current.”	87
I.	[Claim 27] The access control system of claim 26, wherein the first communication protocol comprises a cellular protocol.....	87
J.	[Claim 28] The access control system of claim 26, wherein the first communication protocol comprises a wireless LAN protocol.....	87
K.	[Claim 29] The access control system of claim 28, wherein the wireless LAN protocol comprises Wi-Fi.	87
L.	[Claim 30] The access control system of claim 26, wherein the second communication protocol comprises a short-range wireless protocol.....	87
M.	[Claim 31] The access control system of claim 30, wherein the short-range wireless protocol comprises Bluetooth.	88

N.	[Claim 32] The access control system of claim 26, wherein the second communication protocol comprises a wireless LAN protocol.....	88
O.	[Claim 33] The access control system of claim 32, wherein the wireless LAN protocol comprises Wi-Fi.	88
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.	88
Q.	[Claim 35] The access control system of claim 26, wherein the reservation certificate is encrypted.....	88
R.	[Claim 36] The access control system of claim 35, wherein the encrypted reservation certificate is decrypted by the access device.....	89
XII.	GROUND 3: CLAIM 3 IS RENDERED OBVIOUS BY KNUTSSON IN VIEW OF WOODARD AND BRÖNDRUP	89
A.	Motivation to Combine <i>Knutsson</i> , <i>Woodard</i> , and <i>Bröndrup</i>	89
B.	[Claim 3] The access control system of claim 2, wherein the application notifies the user of proximity to the access device.	90
XIII.	GROUND 4: CLAIM 4 IS RENDERED OBVIOUS BY <i>KNUTSSON</i> IN VIEW OF <i>WOODARD</i> AND <i>ADAMS</i>	92
A.	Motivation to Combine <i>Knutsson</i> , <i>Woodard</i> , and <i>Adams</i>	92
B.	[Claim 4] The access control system of claim 1, wherein the communication module does not advertise that the communication module is present.....	95
XIV.	GROUND 5: CLAIM 10 IS RENDERED OBVIOUS BY <i>KNUTSSON</i> IN VIEW OF <i>BRÖNDRUP</i>	96
A.	Motivation to Combine <i>Knutsson</i> and <i>Bröndrup</i>	96

B.	[Claim 10] The access control system of claim 9, wherein the application notifies the user of proximity to the access device.	96
XV.	GROUND 6: CLAIM 11 IS RENDERED OBVIOUS BY <i>KNUTSSON</i> IN VIEW OF <i>ADAMS</i>	97
A.	Motivation to Combine <i>Knutsson</i> and <i>Adams</i>	97
B.	[Claim 11] “The access control system of claim 8, wherein the communication module does not advertise that the communication module is present.”	97
XVI.	GROUND 7: CLAIMS 6, 17, AND 18 ARE RENDERED OBVIOUS BY <i>KNUTSSON</i> IN VIEW OF <i>WOODARD</i> AND <i>JAIN</i>	98
A.	Motivation to Combine <i>Knutsson</i> , <i>Woodard</i> , and <i>Jain</i>	98
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.....	99
C.	[Claim 17] The access control system of claim 15, wherein the first communication protocol comprises a wireless LAN protocol.....	101
D.	[Claim 18] The access control system of claim 17, wherein the wireless LAN protocol comprises Wi-Fi.	103
XVII.	GROUND 8: CLAIMS 13, 28, and 29 ARE RENDERED OBVIOUS BY <i>KNUTSSON</i> IN VIEW OF <i>JAIN</i>	103
A.	Motivation to Combine <i>Knutsson</i> and <i>Jain</i>	103
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.....	104
C.	[Claim 28] The access control system of claim 26, wherein the first communication protocol comprises a wireless LAN protocol.....	104

D.	[Claim 29] The access control system of claim 28, wherein the wireless LAN protocol comprises Wi-Fi.	104
XVIII.	CONCLUSION	105

I. INTRODUCTION

1. My name is Benjamin B. Bederson, Ph.D. I am currently Professor Emeritus of Computer Science at the University of Maryland. I have been retained as an independent expert by ASSA ABLOY Global Solutions Inc. (“AAGS”) in this proceeding.

2. I have been asked to provide my opinion as to whether claims 1-36 of U.S. Patent No. 11,373,474 are patentable. This report sets forth my opinions and the bases of my opinions.

3. All of the opinions stated herein are based on my own personal knowledge and professional judgment and my analysis of the materials and information I considered in preparing this report. The materials I reviewed in connection with preparing this report are listed below. I make the following statements based on my own personal knowledge and, if called as a witness, I could and would testify to the following. I am being paid for my work in this litigation at my standard rate of \$600.00 per hour, plus reimbursement of reasonable expenses. My compensation does not depend on the outcome of this proceeding, and I have no financial interest in that outcome.

II. QUALIFICATIONS

4. My qualifications for forming the opinions set forth in this report are summarized here and are addressed more fully in my CV, which is attached hereto as Exhibit 1004 with specific publications attached as Appendices.

Appendix	Description
Appx. 1	A Miniaturized Active Vision System. <i>In Proceedings of Eleventh International Conference on Pattern Recognition</i> , IEEE Press, 58-61.
Appx. 2	Pocket PhotoMesa: A Zoomable Image Browser for PDAs. <i>In Proceedings of Mobile and Ubiquitous Multimedia (MUM 2004)</i> ACM Press, 19-24.
Appx. 3	SlideBar: Analysis of a Linear Input Device. <i>Journal of Behaviour and Information Technology</i> , London, Taylor & Francis, 23 (1), 1-9.
Appx. 4	Multi-Modal Text Entry and Selection on Mobile Devices, <i>Proceedings of Graphics Interface (GI 2010)</i> , 19-26.
Appx. 5	DateLens: A Fisheye Calendar Interface for PDAs, <i>Transactions on Computer-Human Interaction</i> , New York: ACM, 11 (1), 90-119.
Appx. 6	Understanding One Handed Use of Mobile Devices. Lumsden, Jo (Ed.), <i>Handbook of Research on User Interface Design and Evaluation for Mobile Technology</i> , Idea Group Reference, 86-101.
Appx. 7	Audio Augmented Reality: A Prototype Automated Tour Guide. In <i>Proceedings of Human Factors in Computing Systems (CHI 95)</i> New York: ACM Press, (Short Paper), 210-211.

5. Based on my education, research, and work experience, I am knowledgeable about the subject matter of the '474 patent and the related prior art. I am currently Professor Emeritus of Computer Science at the University of Maryland ("UMD"). From 2014 to 2018, I was the Associate Provost of Learning Initiatives and Executive Director of the Teaching and Learning Transformation

Center at the UMD. I am a member and previous director of the Human-Computer Interaction Lab ("HCIL"), the oldest and one of the best-known Human-Computer Interaction ("HCI") research groups in the country. I was also co-founder and Chief Scientist of Zumobi, Inc. from 2006 to 2014, a Seattle-based startup that is a publisher of content applications and advertising platforms for smartphones. I am also co-founder and co-director of the International Children's Digital Library ("ICDL"), a web site launched in 2002 that provides the world's largest collection of freely available online children's books from around the world with an interface aimed to make it easy for children and adults to search and read children's books online. I am also co-founder and prior Chief Technology Officer of Hazel Analytics, a data analytics company to improve food safety and better public health whose product sends alerts in warranted circumstances. Last year, I co-founded the J.S. Bryant School to launch in 2025. In addition, I have for more than 25 years consulted for numerous companies in the area of user interfaces, including EPAM, Hillcrest Labs, Lockheed Martin, Logitech, Microsoft, NASA Goddard Space Flight Center, the Palo Alto Research Center, and Sony.

6. For more than 30 years, I have studied, designed, and worked in the field of computer science and HCI. That includes teaching, research, entrepreneurship, and administration in HCI and the software and technology

underlying interactive computing systems. I have worked on the design and implementation of hardware and software systems including the use of capacitive, resistive, optical and IR among other sensors, and interactive applications on a range of devices, including embedded systems, controllers, smart phones, and PDAs for 2D and 3D interfaces.

7. In 1992, I completed my Ph.D. dissertation at New York University titled "A Miniature Space-Variant Active Vision System: Cortex-I" in which I built a custom small motor that aimed a custom camera along with a custom DSP-based computing system. Collectively, these worked together to create a miniature computer vision system that one could carry in one hand - dramatically smaller than other computer vision systems of the day. This system included the ability to generate a real-time video signal with the result of the image processing. Appx. 1.

8. In my dissertation work, I described a custom two degree of freedom motor that I designed and built called a "Spherical Pointing Motor". I was issued U.S. Patent #5,204,573 in 1993 for this work, which included this figure illustrating the motor. A photograph of the actual motor I built was included in Figure 4.1 of my dissertation.

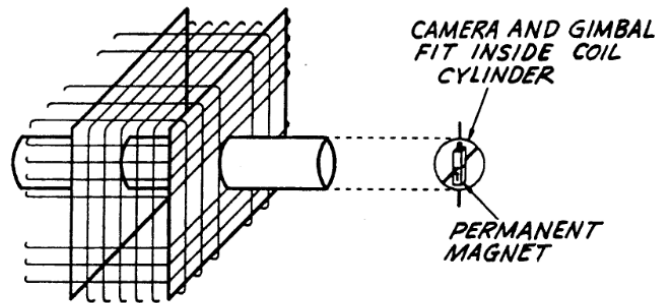
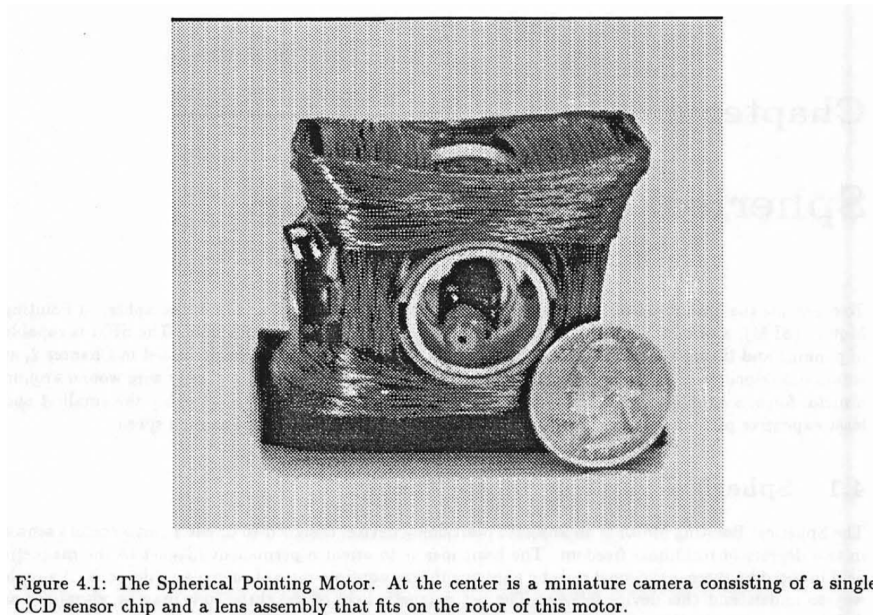


FIG 5



9. As described in my dissertation, I controlled the motor by generating a set of pulse width modulation signals for each of the three coils. I then calibrated those signals by using the camera in the motor to determine exactly where each set of signals ended up pointing the motor. Because the motor used an open loop control system, the device would oscillate in response to the input signals generated. I reduced this oscillating response by measuring its movement in response to the

control signals I generated and then creating complementary signals to dampen the oscillation. The following figure from my dissertation demonstrates the uncontrolled and controlled motor movement in response to the control system I built.

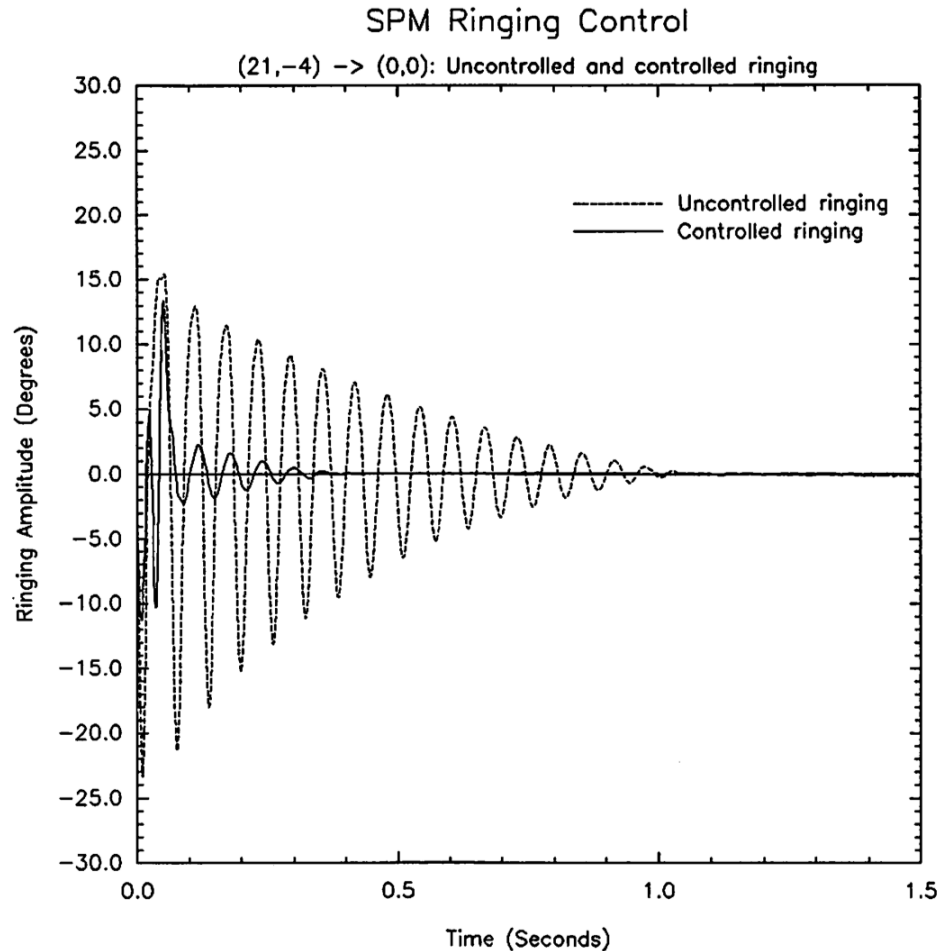


Figure 4.14: Measurement of two-step open-loop control strategy to reduce SPM ringing. Results are shown for the same movement of 21.4° with and without control. The motor currents are changed to hold the motor at the final position when the motor is expected to have zero velocity. Because the midpoint and timing are not exactly correct, the ringing is not completely eliminated.

10. In 1995, I built an “audio augmented reality” system for use in an art museum that identified and announced which piece of art a person was standing in front of. Appx. 7. This worked by installing infrared (IR) transmitters in the ceiling above each piece of art which was identified by an infrared (IR) receiver controlled by a microcontroller. As depicted in Figure 1 from that paper below, a person wearing the receiver walked around, the microcontroller they were carrying would identify the code from the transmitter they were standing under.

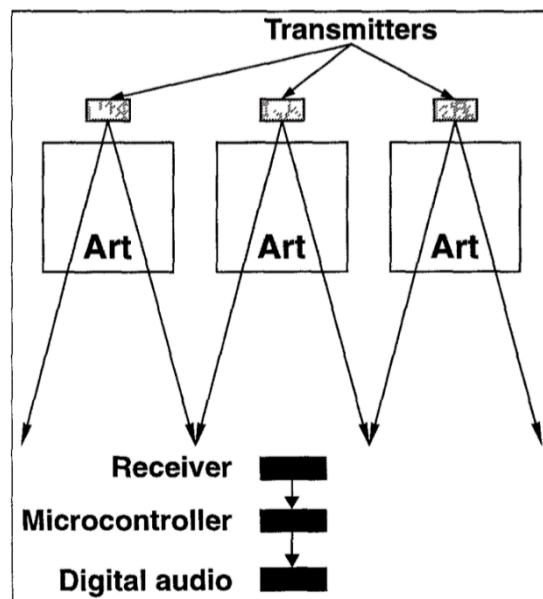


Figure 1: Schematic of automated tour guide prototype.

11. Starting in the mid-1990s and going through the 2000s, I worked on a range of "zoomable user interfaces" (ZUIs) that supported users in navigating large information spaces by zooming in and out of the information on the screen. I built several different ZUI systems over the years, including Pad++, Jazz, and Piccolo.

Starting in the early 2000s, I adapted that work to work on mobile devices including PDAs, tablets, and mobile phones. Appx. 2.

12. I was heavily involved in the research and development of mobile device applications during the early 2000s. For example, I envisioned, designed, and built DateLens in 2002-2004 to create a richer calendar for the Microsoft PocketPC platform as well as desktops as described in a 2004 paper. Appx. 5. One of its innovations was its design that enabled it to scale between small (mobile) and large (desktop) computers. It also had a special double-headed scroll bar that allowed a user to touch scroll and also control how much information was presented on the screen at a time. I started DateLens as a research project and eventually sold it commercially. DateLens displayed calendar data that came from the Microsoft PocketOutlook database and allowed modification and viewing of appointments. The research website from that time period that describes DateLens is still available at <http://www.cs.umd.edu/hcil/datelens/> which shows screenshots and a picture of me demonstrating DateLens to Bill Gates. The commercial website from that time period is also available at <http://www.windsorinterfaces.com/datelens.shtml>, which shows a number of news articles reviewing DateLens at that time.

13. That work led to my co-founding of Zumobi, where I was responsible for investigating new software platforms and developing new user interface designs

that provide efficient and engaging interfaces for mobile touchscreen platforms including the iPhone and Android-based devices. For example, I designed and implemented software called "Ziibii," a "river" of news for iPhone, software called "ZoomCanvas," a zoomable user interface for several iPhone apps, and iPhone apps including "Inside Xbox" for Microsoft and Snow Report for REI. All of these applications included touch-based zooming and scrolling.

14. My work has often integrated hardware and software systems as I explained above where I described my work on the spherical pointing motor of my dissertation and my work on audio augmented reality. Some other work of mine that involved the combination of hardware and software included the development of "SlideBar" in 2004, a linear input device used for absolute linear position control. Appx. 3. Another project from 2010 used input from an accelerometer, a foot pedal and voice to allow multi-modal text entry and selection on a mobile device. Appx. 4. And in 2007, I built a custom sensing device to understand how people grasped and used mobile devices with one hand, as illustrated in the figure below from a paper describing that work. Appx. 6.

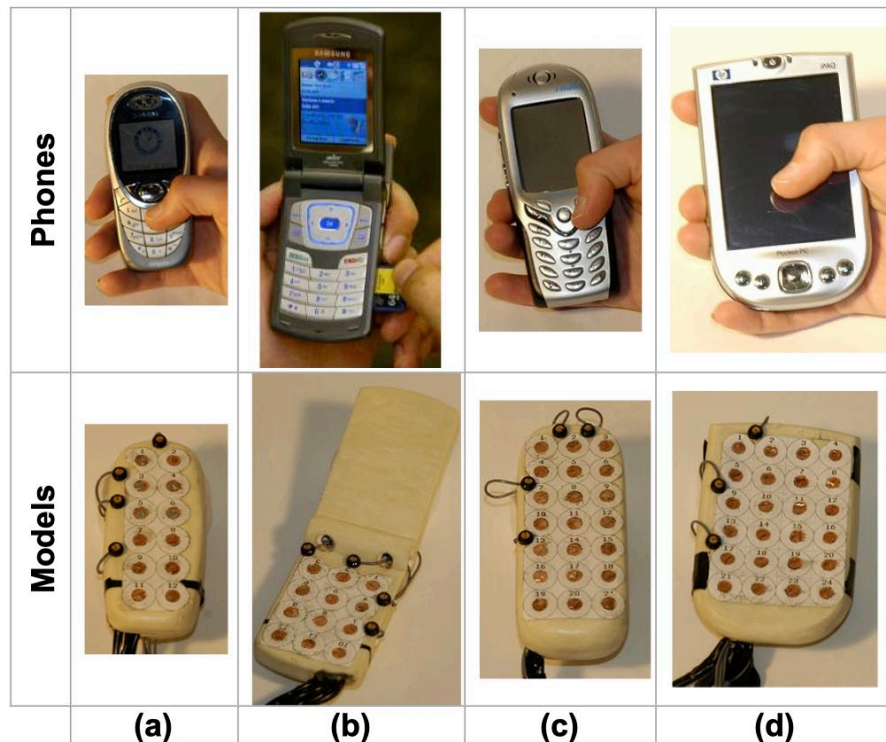


Figure 4. Devices we chose to represent a range of sizes and forms (top row) together with their study-ready models (bottom row): (a) SMALL, (b) FLIP, (c) LARGE, and (d) PDA.

15. At UMD, I have been focused primarily on the area of HCI, a field that relates to the development and understanding of computing systems to serve users' needs. Researchers and practitioners in this field are focused on making universally usable, useful, efficient, and appealing systems to support people in their wide range of activities. My approach is to balance the development of innovative technology that serves people's practical needs. Example systems following this approach that I have built include Cortex-I (1992 embedded computer vision system that sensed licensed plates with custom motor, camera, and controller), Audio Augmented Reality (1995 embedded system for sensing a user's location and playing audio

suited to that location), Fisheye Menus (2000 software for sensing movement within and selection of linear list of items in a menu), PhotoMesa (2001 software for end users to browse personal photos), DateLens (2002 software for end users to use their mobile devices to efficiently access their calendar information), SlideBar (2005 linear sensor to control scrolling), LaunchTile (2005 "home screen" software for mobile devices to allow users to navigate apps in a zoomable environment), SpaceTree (2001 software for end users to efficiently browse very large hierarchies), ICDL (2002 International Children's Digital Library), and StoryKit (a 2009 iPhone app for children to create stories).

16. My work has been published extensively in more than 160 technical publications, and I have given about 100 invited talks, including 9 keynote lectures. I have won a number of awards including the Brian Shackel Award for "outstanding contribution with international impact in the field of HCI" in 2007, and the Social Impact Award in 2010 from the Association for Computing Machinery's ("ACM") Special Interest Group on Computer Human Interaction ("SIGCHI"). ACM is the primary international professional community of computer scientists, and SIGCHI is the primary international professional HCI community. I have been honored by both professional organizations. I am an "ACM Distinguished Scientist," which "recognizes those ACM members with at least 15 years of professional experience

and 5 years of continuous Professional Membership who have achieved significant accomplishments or have made a significant impact on the computing field." I am a member of the "CHI Academy," which is described as follows: "The CHI Academy is an honorary group of individuals who have made substantial contributions to the field of HCI. These are the principal leaders of the field, whose efforts have shaped the disciplines and/or industry, and led the research and/or innovation in human-computer interaction." The criteria for election to the CHI Academy are: (1) cumulative contributions to the field; (2) impact on the field through development of new research directions and/or innovations; and (3) influence on the work of others. I have received two "Test of Time" awards from IEEE InfoVis for my 2001 and 2002 work on visualizing hierarchies, including those containing digital photos.¹

17. I have appeared on radio shows numerous times to discuss issues relating to user interface design and people's use and frustration with common technologies, web sites, and mobile devices. My work has been discussed and I have been quoted by mainstream media around the world over 120 times, including by the New York Times, the Wall Street Journal, the Washington Post, Newsweek, the

¹ <https://ieevis.org/year/2021/info/awards/test-of-time-awards>;
<https://ieevis.org/year/2022/info/awards/test-of-time-awards>.

Seattle Post Intelligencer, the Independent, Le Monde, NPR's All Things Considered, New Scientist Magazine, and MIT's Technology Review.

18. I have designed, programmed, and publicly deployed dozens of user-facing software products that have cumulatively had millions of users. My work is cited by several major companies, including Amazon, Apple, Facebook, Google, and Microsoft. I am a named inventor on 14 U.S. patents and 20 U.S. patent applications. The patents are generally directed to user interfaces and experience.

19. I received a B.S. degree in Computer Science with a minor in Electrical Engineering in 1986 from the Rensselaer Polytechnic Institute. I received M.S. and Ph.D. degrees in Computer Science in 1989 and 1992, both from New York University.

III. MATERIALS CONSIDERED

20. In forming my opinions, I have reviewed the following documents, and any other document cited in this declaration:

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-1004	Curriculum Vitae of Benjamin B. Bederson
Ex-1005	WO Publication No. 2008/076074 A1 to Knutsson et al. (“ <i>Knutsson</i> ”)
Ex-1008	U.S. Patent Publication No. 2009/0219133 A1 to Woodard et al. (“ <i>Woodard</i> ”)
Ex-1009	WO Publication No. 2001/063425 A1 to Bröndrup (“ <i>Bröndrup</i> ”)
Ex-1010	U.S. Patent Publication No. 2009/0070272 A1 to Jain (“ <i>Jain</i> ”)

Ex-1012	U.S. Patent Publication No. 2007/0053313 A1 to Adams et al.
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.

21. I have also relied on my education, experience, research, training, and knowledge in the relevant art, and my understanding of any applicable legal principles described in this declaration.

22. All of the opinions contained in this declaration are based on the documents I reviewed and my knowledge and professional judgment. My opinions have also been guided by my understanding of how a person of ordinary skill in the art would have understood the claims of the '474 patent at the time of the alleged invention. For purposes of this declaration, I have been asked to assume that the date of the alleged invention is the earliest claimed priority date: March 2, 2010.

23. I reserve the right to supplement and amend any of my opinions in this declaration based on documents, testimony, and other information that becomes available to me after the date of this declaration.

IV. LEGAL PRINCIPLES

24. It is my understanding that there are two ways that prior art references can render a patent claim unpatentable: anticipation and obviousness. Counsel has informed me that the petitioner has the burden in an *inter partes* review to show unpatentability by a preponderance of the evidence.

25. I also understand that there is a set process as follows: (a) the claims of a patent are properly construed, (b) then, you must compare the claim language to the prior art on a limitation-by-limitation basis. If the prior art reference contains all the elements of the claim language (explicitly or inherently), arranged as in the claims, then that is considered anticipation.

26. I understand that an invention is obvious when the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time of the invention to a person having ordinary skill in the art. For this reason, I have been asked to consider the level of ordinary skill in the field that someone would have had at the time of the claimed invention.

27. Counsel has also instructed me that in an obviousness determination, the factors to consider are (1) the scope and content of the prior art, (2) the differences between the prior art and the asserted claims, (3) the level of ordinary skill in the pertinent art, and (4) the existence of secondary considerations of nonobviousness. Secondary considerations include a long-felt need, commercial success, unexpected results, praise of the invention, licensing, copying, failure of others, and skepticism by experts.

28. Counsel has also instructed me that an obviousness inquiry may involve assessing the motivation of a person of ordinary skill to combine references. The prior art references themselves may provide a suggestion, motivation, or reason to combine, but other sources may also support a rationale for combining two or more prior art references.

29. It is also my understanding through counsel that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. It is further my understanding that a proper obviousness analysis focuses on what was known or obvious to a person of ordinary skill in the art, not just the patentee.

30. I have been informed that, in this proceeding, claim terms in the '474 patent must be given the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention in light of the patent specification.

31. I have been asked to assume that March 2, 2010, is the date of the purported invention, as that is the earliest date to which the '474 patent claims priority. I have not conducted a separate analysis to determine whether the challenged claims are entitled to this priority date, as I understand that the prior art

references discussed below qualify as prior art even if all claims are deemed to be entitled to the March 2, 2010, date.

V. THE '474 PATENT

32. The '474 patent describes a smart phone or terminal to active 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. The first independent claim, 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.

33. *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**

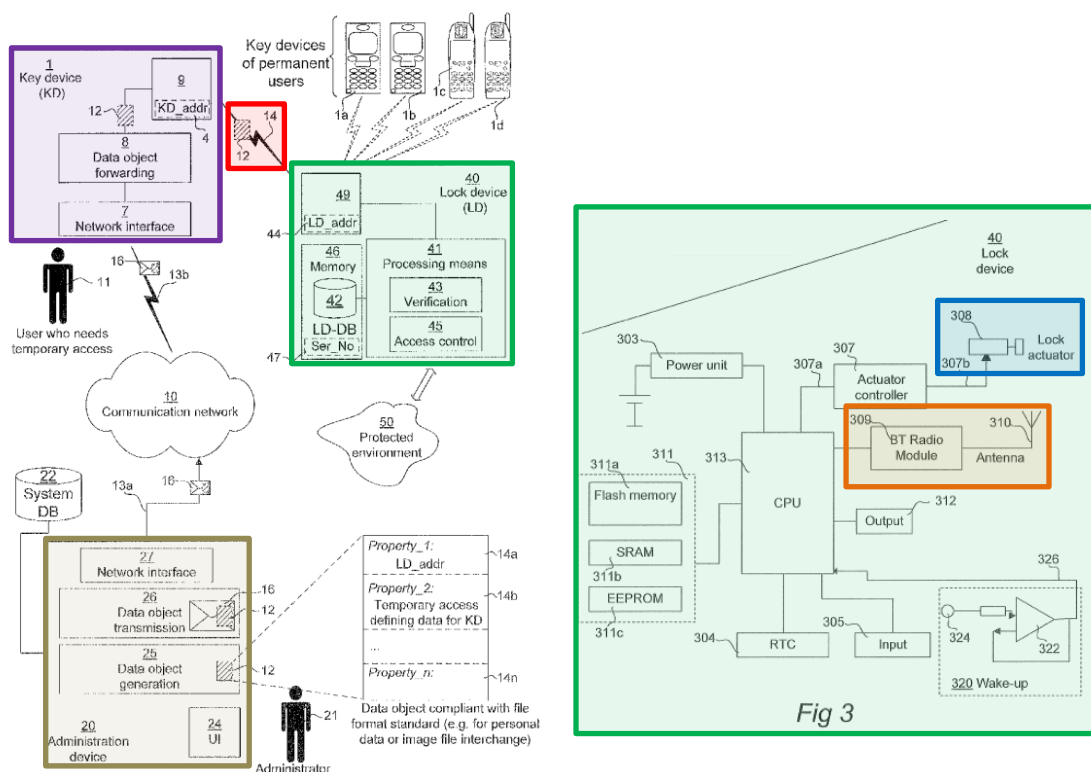
reservation certificate and communicates with the access device to unlock a door lock if the reservation certificate is current, like those claimed by the '474 patent.

VI. OVERVIEW OF PRIOR ART

A. *Knutsson*

34. WO Publication WO2008/076074 (Ex-1005, “*Knutsson*”), was published on June 26, 2008, and was filed as International Application No. PCT/SE2007/051042, filed on December 19, 2007. I have been asked to assume that *Knutsson* is therefore prior art to the '474 patent.

35. *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 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* says 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.*, 10:24-28. *Knutsson*’s “lock device 40 has a Bluetooth® radio module 309 with an antenna 310.” *Id.*, 17:18-19.



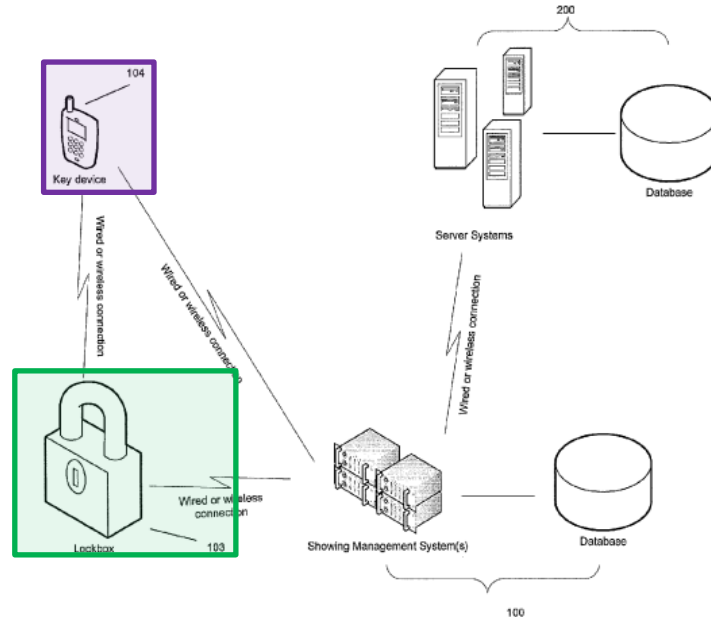
Id., FIGS. 1, 3 (annotated).

B. Woodard

36. U.S. Publication No. 2009/0219133 A1 to Woodard et al., (“*Woodard*”), was filed no later than February 28, 2008, and published no later than September 3, 2009. I have been asked to assume that *Woodard* is prior art.

37. *Woodard* discloses, “the showing management system 100 transmits the showing appointment data directly to an **electronic key device 104** that has been assigned to the showing agent who is scheduled to show the property to which the transmitted showing appointment data pertains to. In this embodiment, the

specification of the **electronic key device 104** needs to include at least, but is not limited to, a power source, an internal controller, an accurate timer which may be capable of synchronization with a timer server, and a storage medium for storing at least showing appointment data, the key device's own unique ID or the Showing Agent ID who uses the key device 104.” *Woodard*, [0054]. Then, “the logic inside the **electronic lockbox 103** compares the current date and time of the internal timer and the Showing Agent ID of the showing agent attempting to access **the lockbox 103** with the stored showing appointment data.” *Id.*, [0065].



Id., FIG. 5 (annotated).

C. Bröndrup

38. WO Publication No. 01/63425 to Bröndrup (“*Bröndrup*”), was filed no later than February 13, 2001, and published on August 30, 2001. I have been asked to assume *Bröndrup* is prior art.

39. *Bröndrup* discloses “[o]n receiving the appropriate key token from the wireless device in the mobile 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*, 7:30-33. *Bröndrup* discloses, by means of 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.

D. Jain

40. U.S. Publication No. 2009/0070272 A1 to Jain, (“*Jain*”), was filed no later than September 11, 2008, and published on March 12, 2009. I have been asked to assume *Jain* is prior art.

41. *Jain* discloses, “the host device may be a cellphone such that the card 400 may request network authentication prior to activation. For example, the card 400 may be distributed by a Wireless Network Operator (WNO) that requires a network authentication. In this example, a flag in memory may be set to ON

indicating that network authentication is required. If the flag is set to ON, a unique identity about the allowed network is 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, “the CPU 408 in response to at least insertion may request a special software plug-in to be downloaded to the host device and instantiated. This software plug-in 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.*

E. *Adams*

42. U.S. Publication No. 2007/0053313 A1 to Adams, (“*Adams*”), was filed no later than September 6, 2005, and published on March 8, 2007. I have been asked to assume *Adams* is prior art.

43. *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*, [0005]. As Adams explains, in the Non-Discoverable Mode, “a [Bluetooth] device is visible to other [Bluetooth] device and users that are familiar with its

Bluetooth® device address.” *Adams*, [0006]. *Adams* explains, “[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*, [0007].

VII. LEVEL OF ORDINARY SKILL IN THE ART

44. In rendering the opinions set forth in this declaration, I have been asked to consider the ’474 patent’s claims and the prior art through the eyes of a person of ordinary skill in the art (“POSA”). I considered factors such as the educational level and years of experience of those working in the pertinent art, the types of problems encountered in the art, the teachings of the prior art, patents and publications of other persons or companies, and the sophistication of the technology.

45. I have been instructed to assume a person of ordinary skill in the art is not a specific real individual, but rather a hypothetical individual having the qualities reflected by the factors discussed above.

46. Taking these factors into consideration, it is my opinion that 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 two to three years of academic or industry experience with wireless systems or

comparable experience. Additional education could substitute for professional experience and vice versa.

47. By March 2, 2010, as evidenced by my qualifications outlined in Section II, I was at least a person of ordinary skill in the art at the relevant time. In this declaration, and for all of my opinions herein, I have applied the knowledge of a person of ordinary skill in the art as of March 2, 2010.

48. In forming my opinions, I have also relied on my education and experience.

VIII. CLAIM CONSTRUCTION

49. I understand that in *inter partes* review, the U.S. Patent and Trademark Office construes terms according to their plain and ordinary meaning, in view of the specification, as would have been understood by a person of ordinary skill in the art. I understand that no terms have been proposed for construction in any case. Based on my review of the claims and my personal knowledge and experience, I have considered and applied the plain and ordinary meaning of all terms of the '474 patent as they would have been understood by one skilled in the art in view of the specification as of March 2, 2010.

IX. SUMMARY OF OPINIONS

50. In my opinion, claims 1-36 of the '474 patent are rendered obvious under the following grounds.

Ground	Reference(s)	Claims
1	<i>Knutsson, Woodard</i>	1-7, 15-25
2	<i>Knutsson</i>	8-14, 26-36
3	<i>Knutsson, Woodard, Bröndrup</i>	3
4	<i>Knutsson, Woodard, Adams</i>	4
5	<i>Knutsson, Bröndrup</i>	10
6	<i>Knutsson, Adams</i>	11
7	<i>Knutsson, Woodard, Jain</i>	6, 17, 18
8	<i>Knutsson, Jain</i>	13, 28, 29

51. The claims recite a phone or portable terminal to active 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. As shown below, the certificate includes a start time. *Id.*, 5:36-37. The '474 patent discloses, “the smart phone application [can] attempt communication with the EV charging system 4 (or other parking spot amenity system or access device 11, e.g., a

hotel room lock) and to provide the reservation certificate 5 to the charger 6 or device (11), thereby enabling it 32 for the interval of the reservation.” *Id.*, 8:50-55.

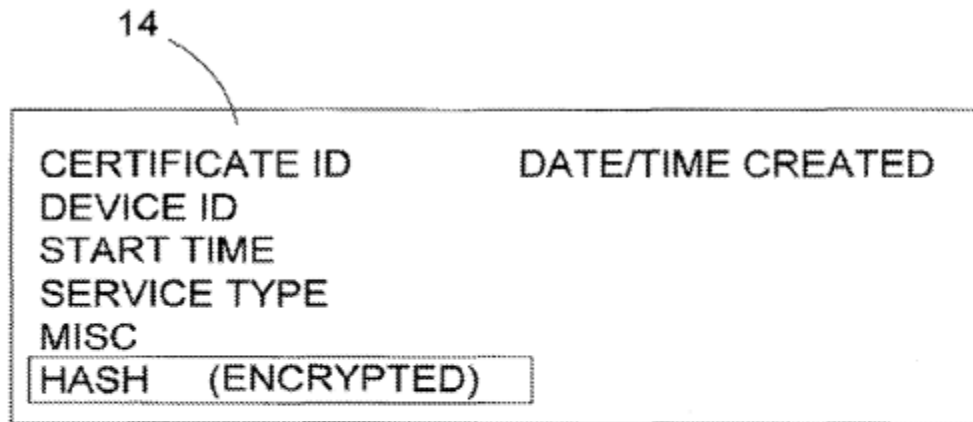


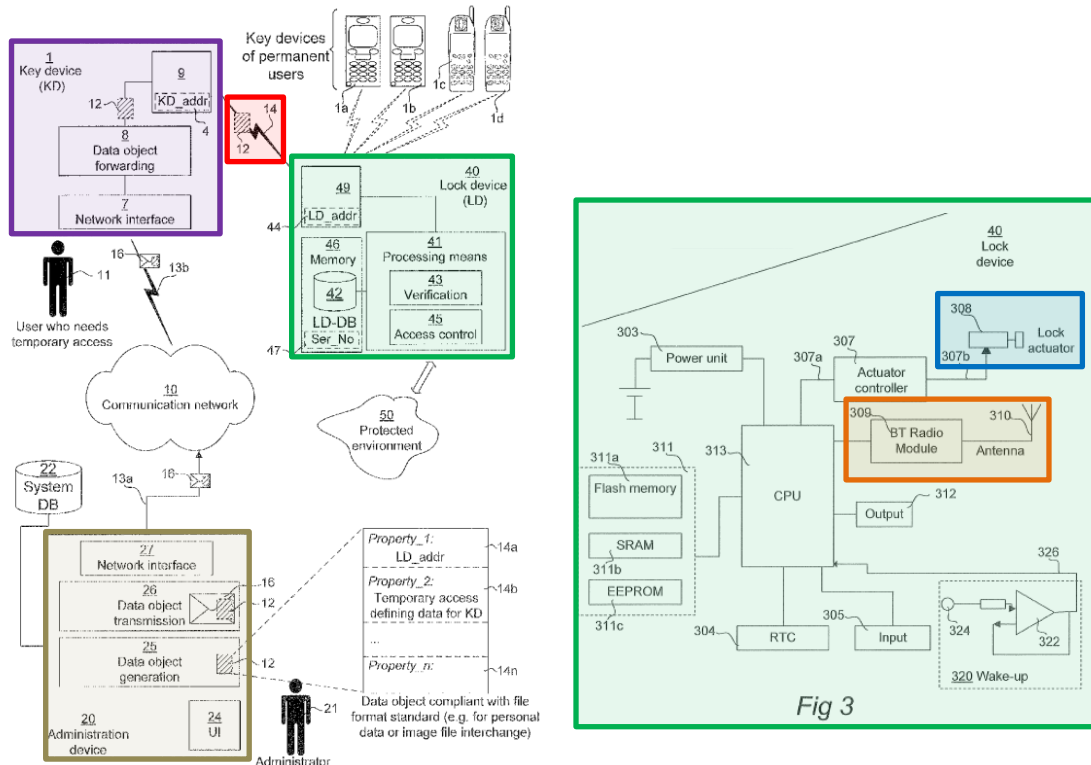
FIG. 2

Id., FIG. 2.

52. But access credentials or a reservation certificate used by a phone to unlock a door, was known before March 2, 2010, the earliest-claimed priority date of the '474 patent as discussed below.

53. *Knutsson* alone or in view of *Woodard* 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 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

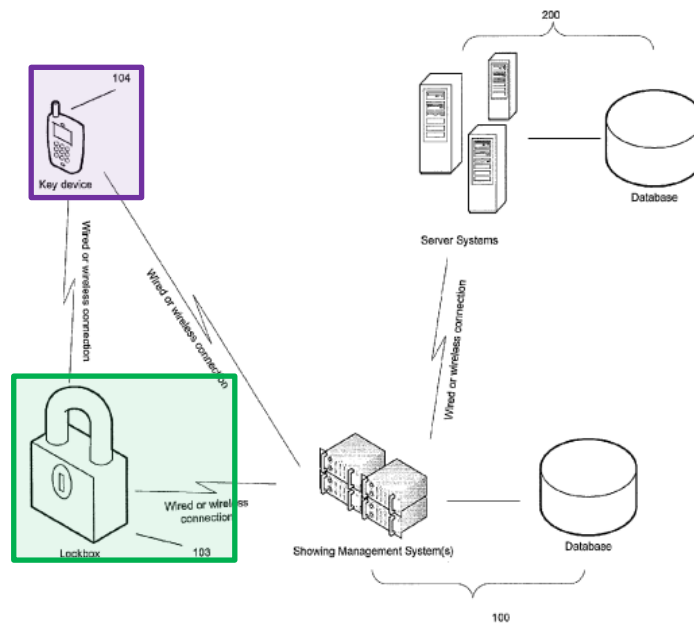
gain access. *Knutsson*, 10:13-21. *Knutsson* discloses that its “lock device 40 will be integrated with or coupled to a lock mechanism in the lockable door or garage port and in particular have a controllable lock actuator configured to unlock the lock mechanism upon detection and successful authorization of the key device 1.” *Id.*, 10:24-28. *Knutsson*’s “the lock device 40 has a Bluetooth® radio module 309 with an antenna 310.” *Id.*, 17:18-19.



Id., FIGS. 1, 3 (annotated).

54. 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 the mobile terminal application checking the time of the reservation certificate, but *Woodard* does. *Woodard* discloses, “the showing management system 100 transmits the showing appointment data directly to an **electronic key device 104** that has been assigned to the showing agent who is scheduled to show the property to which the transmitted showing appointment data pertains to. In this embodiment, the specification of the **electronic key device 104** needs to include at least, but is not limited to, a power source, an internal controller, an accurate timer which may be capable of synchronization with a timer server, and a storage medium for storing at least showing appointment data, the key device's own unique ID or the Showing Agent ID who uses the key device 104.” *Woodard*, [0054]. Then, “the logic inside the **electronic lockbox 103** compares the current date and time of the internal timer and the Showing Agent ID of the showing agent attempting to access **the lockbox 103** with the stored showing appointment data.” *Id.*, [0065].



Id., FIG. 5 (annotated).

55. Certain dependent claims in the '474 patent further require notification methods (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.

56. *Bröndrup* discloses “[o]n receiving the appropriate key token from the wireless device in the mobile 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*, 7:30-33. *Bröndrup* discloses, by means of 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.

57. 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 the communication module not advertising that it is present, *Adams* does.

58. *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*, [0005]. As *Adams* explains, in the Non-Discoverable Mode, “a [Bluetooth] device is visible to other [Bluetooth] device and users that are familiar with its Bluetooth® device address.” *Adams*, [0006]. *Adams* explains, “[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*, [0007].

59. 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 a network SSID or the first communication protocol is Wi-Fi, *Jain* does.

60. *Jain* discloses, “the host device may be a cellphone such that the card 400 may request network authentication prior to activation. For example, the card 400 may be distributed by a Wireless Network Operator (WNO) that requires a network authentication. In this example, a flag in memory may be set to ON indicating that network authentication is required. If the flag is set to ON, a unique identity about the allowed network is 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, “the CPU 408 in response to at least insertion may request a special software plug-in to be downloaded to the host device and instantiated. This software plug-in 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.” *Jain*, [0068].

61. Accordingly, because the challenged claims of the '474 patent were known in the art prior to its earliest priority date, it is my opinion that the challenged claims are unpatentable.

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

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

62. As explained in Section IX, 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*. 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.” *Id.*, [0010]. *Woodard* further discloses an access system similar to *Knutsson*'s, where the user “carries an electronic key device 104, which can be a PDA, a cell phone, or a custom device adapted to wirelessly communicate with the electronic lockbox 103” but further discloses *Woodard*'s key device 104 communicates with “the central computer system/database 200.” *Woodard*, [0003].

63. Based on my experience, 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.” *Id.*, [0013]. *Woodard* discloses that its key device 104 would be able to 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.”

Id., [0004]. Thus, in my opinion, 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 would be able to "track, store and centrally process [the] access data." *Id.*, [0004]. This would be a useful way to track each access and ensure that each access occurs occurring to the time that was reserved for that access. Further, it would ensure the central computer system/database 200 and the lock devices (*Knutsson*'s lock device 40 or *Woodard*'s lockbox 103) are working from a common time (i.e., that the two devices are synchronous).

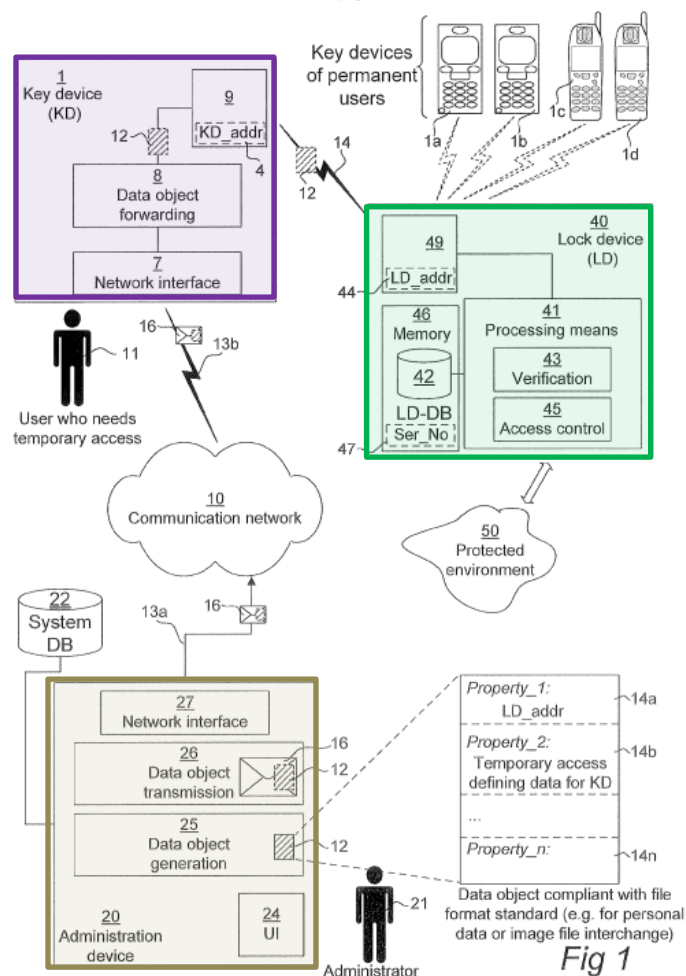
64. In my opinion, a POSA would have had a reasonable expectation of success combining *Woodard* and *Knutsson* because *Woodard* and *Knutsson* disclose similar key devices such as *Woodard*'s "electronic key device 104, which can be a PDA, [or] a cell phone," *id.*, [0003], and *Knutsson*'s key device that can be a PDA or a mobile phone, *Knutsson*, 5:1-2, to actuate access devices like *Woodard*'s lockbox 103, *Woodard*, [0048], or *Knutsson*'s lock device 40 to open a lock. *Knutsson*, 10:24-30.

B. Claim 1

65. *Knutsson* in view of *Woodard* renders obvious claim 1.

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

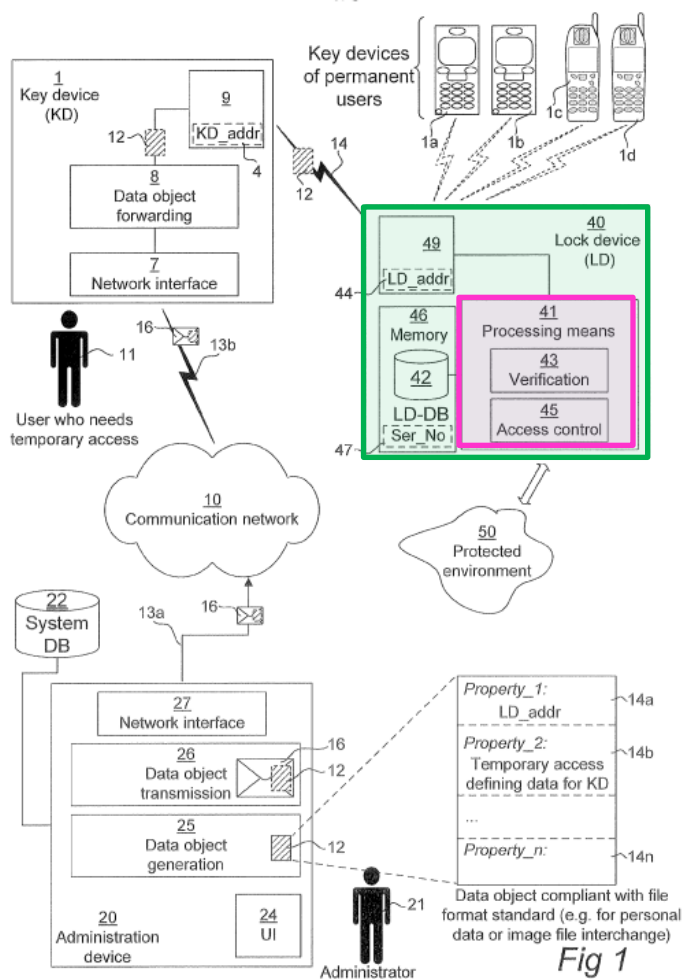
66. *Knutsson* renders obvious [1p] because *Knutsson* discloses “[a]n access control system ... to provide temporary access for a wireless key device to a lock device.” *Knutsson*, Abstract. *Knutsson* discloses, “Fig 1 is a schematic illustration of an access control system, including an administration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



Id., FIG. 1 (annotated).

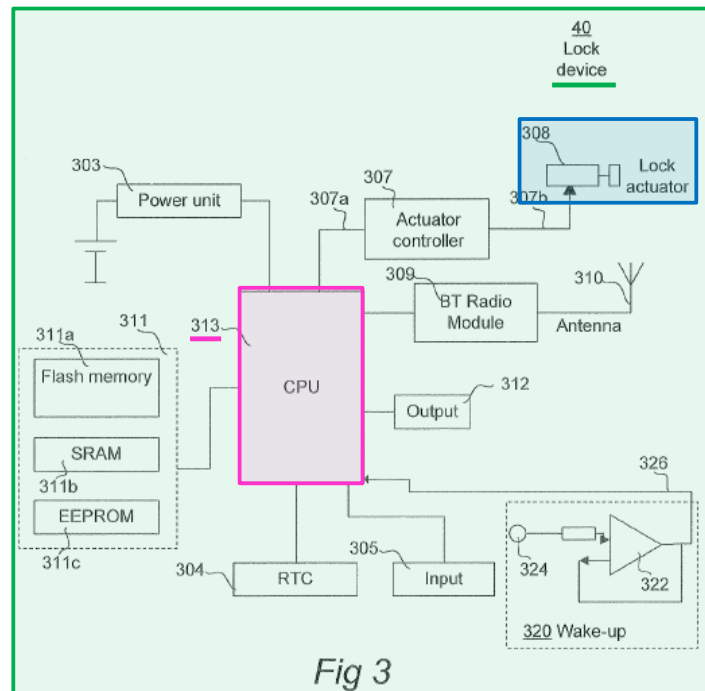
2. [1A] “an access device comprising a communication module connected to a processor having control of a door lock;”

67. *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.



Id., FIG. 1 (annotated).

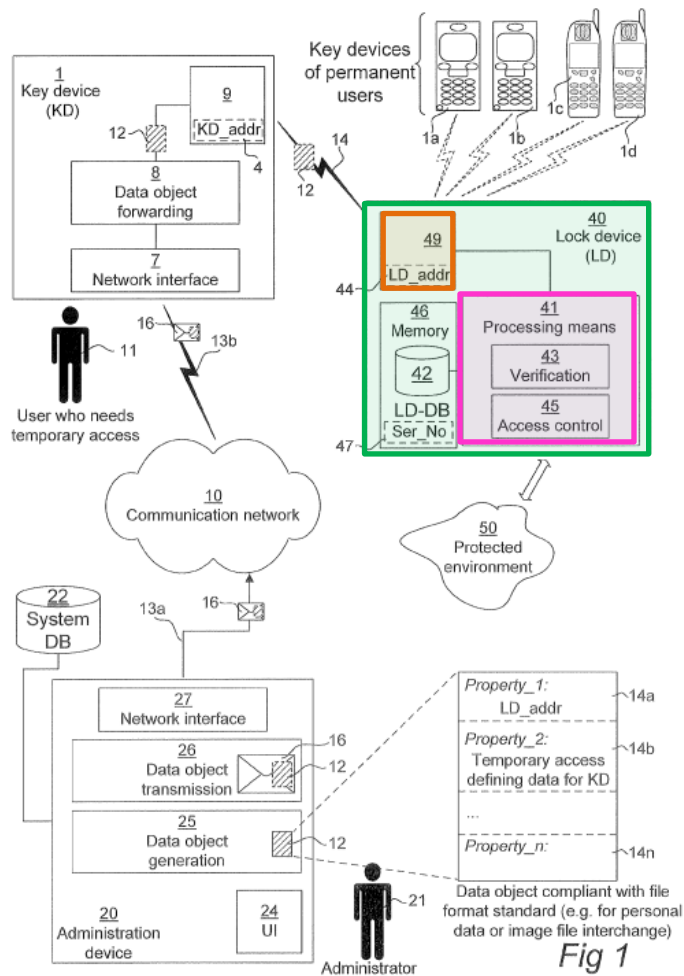
68. *Knutsson*’s “FIG. 3 is a schematic block diagram illustrating internal components and modules of a lock device.” *Id.*, 9:31-32.



Id., FIG. 3 (annotated).

69. *Knutsson*’s “CPU [313] may be identical to the aforementioned 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 is coupled to the lock actuator 308 and is adapted to provide 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, etc, and allow opening of the door, etc, to the protected environment.” *Id.*, 20:8-11 (emphasis added).

70. *Knutsson*'s communication means 49 corresponds to the claimed, "communication module." *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." *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. The Bluetooth® radio module 309 may be identical to the aforementioned 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.



Id., FIG. 1 (annotated).

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

71. *Knutsson* renders obvious [1B] because *Knutsson* discloses a key device such as a mobile terminal (portable terminal) that uses applications.

72. *Knutsson* discloses that “a mobile terminal is used as the wireless key device.” *Id.*, 5:15-16 (emphasis added). *Knutsson* discloses “mobile terminals are very often provided with standard utility software which includes a messaging

application and a contacts application. Therefore, such standard utility software in the mobile terminal will conveniently implement the required data interchange means of the wireless key device.” *Id.*, 5:16-20. *Knutsson* discloses “the mobile terminal” in FIG. 2 that includes “a graphical user interface 206 ... which may be used by a user of the mobile terminal to **control the terminal's functionality** and get access to any of the telecommunications services referred to above, or to **any other software application** executing in the mobile terminal.” *Id.*, 13:20-28 (emphasis added).

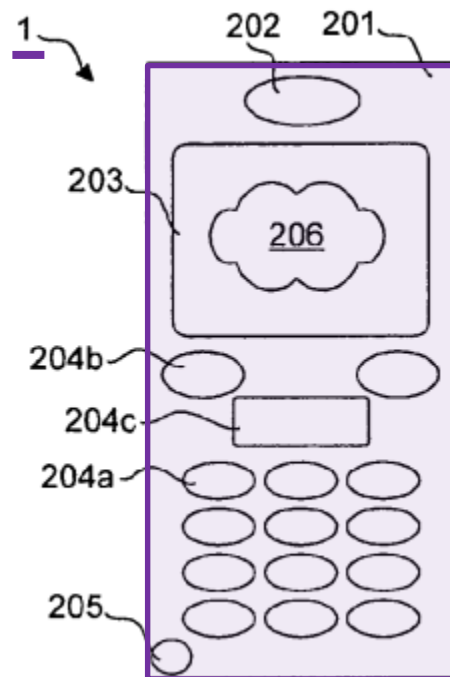
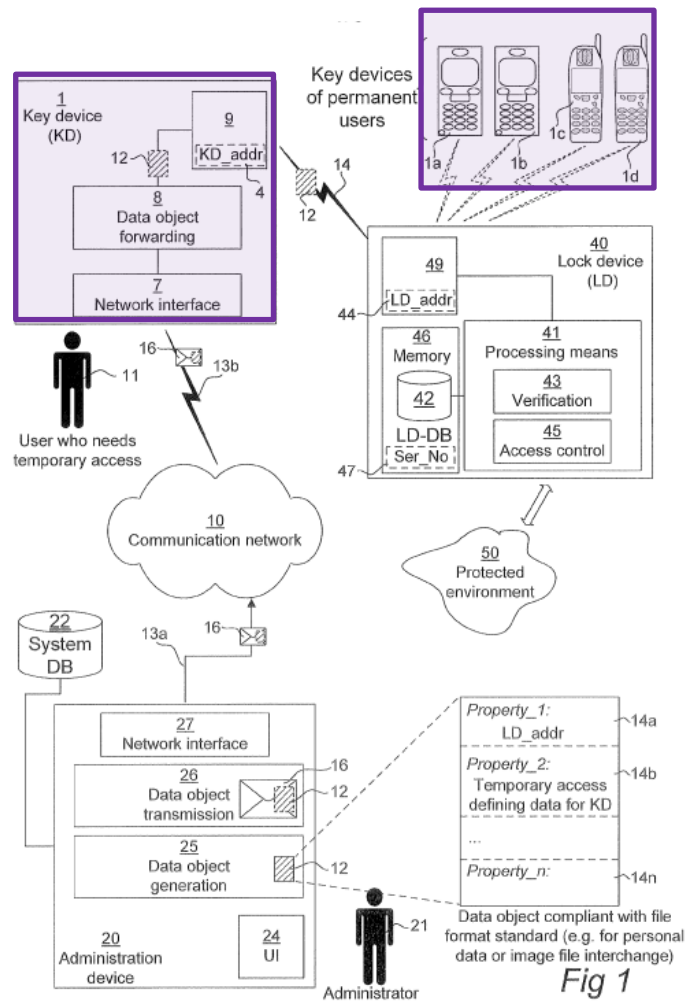


Fig 2

Id., FIG. 2 (annotated).



Id., FIG. 1 (annotated).

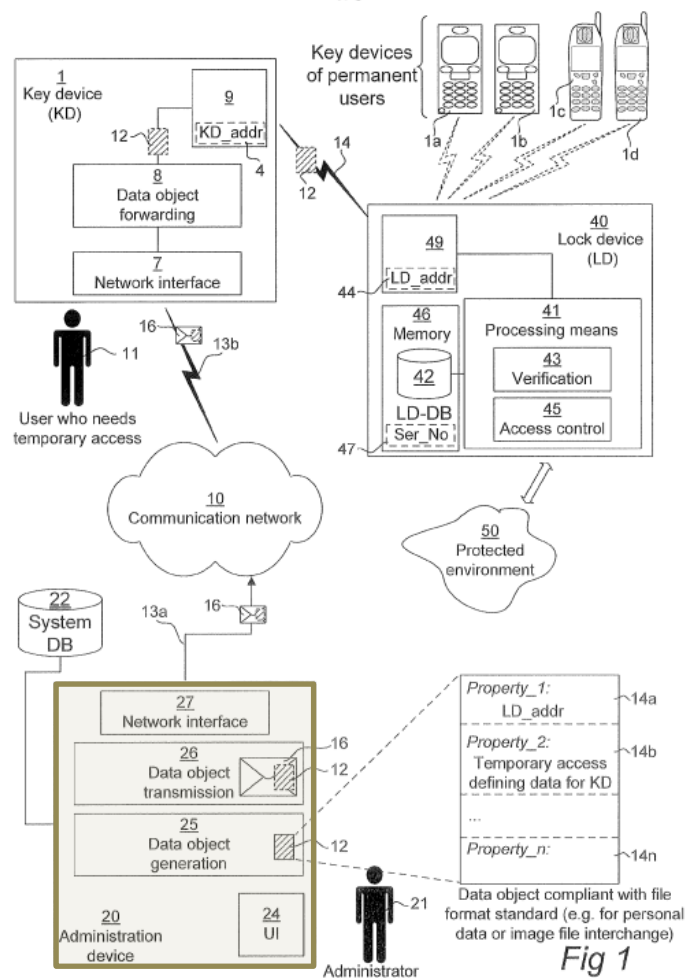
73. *Knutsson*’s key device is the claimed, “portable terminal.” *Knutsson* discloses, “the wireless key device is advantageously a mobile terminal, such as a mobile phone.” *Id.*, 5:1-2. *Knutsson*’s “key devices 1a-1d” are portrayed in Figure 1 as mobile phones. *Id.*, FIG. 1, 10:30. Further, *Knutsson* builds on a previous reference, WO Publication 2006/0986590 that, like *Knutsson*, discloses as using “high-end mobile phones” that handle, “their appropriate authentication via short-

range wireless data communication (Bluetooth communication) with the lock device.” *Id.*, 1:19-22, 2:26-29. *Knutsson*’s “mobile terminal” (portable terminal) includes “a graphical user interface 206 ... which may be used by a user of the mobile terminal to **control the terminal’s functionality** and get access to any of the telecommunications services referred to above, or to **any other software application** executing in the mobile terminal.” *Id.*, 13:25-28 (emphasis added). *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. *Id.*, 14:12-17, 14:20-23. *Knutsson*’s mobile terminal or key device’s functionality would be controlled through a software application, like the combined application, through graphical interface 206 so the user would control functions of the key device.

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,**”

74. *Knutsson* renders obvious [1C]. *Knutsson*’s administrative device 20 corresponds to the claimed “server,” because *Knutsson* discloses, “**the**

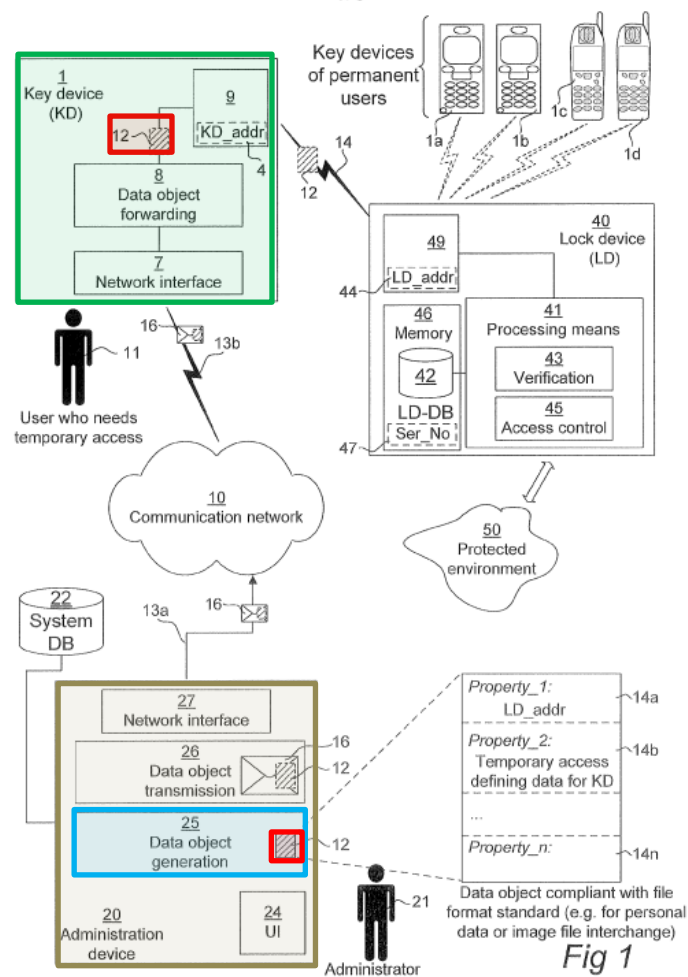
administration device may advantageously be a server computer or a mobile terminal.” *Knutsson*, 5:11-12. *Knutsson* displays administrative device 20 in FIG. 1.



Id., FIG. 1 (annotated).

75. *Knutsson* renders obvious the claimed, “a server to provide a communication setting to the application,” because *Knutsson* discloses, **the 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. *Knutsson* discloses the

digital message 16 to the key device 1 has attached, “the **data object 12** (vCard).” *Id.*, 13:7-9. Further, “[t]he **key device** also has data object forwarding functionality 8 capable of receiving the digital message 16,” *id.*, 13:31-34, which is accomplished through the key device’s “combined application.” *Id.*, 14:6-10. The path of data object 12 is shown below in FIG. 1.



Knutsson, FIG. 1 (annotated).

76. *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. 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.

77. *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. 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.

78. *Knutsson* renders obvious 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 (emphasis added). 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* teaches that “the communication identifier may ... be the unique **Bluetooth communication address**,” i.e., its Bluetooth ID. *Knutsson*, 3:30-33. And, as discussed above, the data object 12 would include this communication identifier, the Bluetooth communication address. Thus, *Knutsson*’s communication identifier of its lock device corresponds to the claimed “communication setting corresponding to the access device.”

79. *Knutsson*’s data object 12 corresponds to the claimed, “reservation certificate.” *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 (emphasis added). *Knutsson* discloses, “[i]n the disclosed embodiment of Figs 4a and 4b, the temporary access defining data assigned to the second vCard property 14b includes temporal data which defines one

or more time frames during which access is permitted for the key device 1 to the protected environment 50.” *Id.*, 12:21-24. Because the data object 12 discloses necessary data for temporary access, including the communication identifier and temporal data needed for a user to access a room for a time frame. In my opinion, a POSA would have also 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,” would be a reservation because *Knutsson*’s disclosure of temporary access to rooms with controllable access satisfies the definition of a “reservation.” This is confirmed by the ’474 patent’s disclosure of a reservation as allowed access “to any access device such as a hotel room lock or the like.” Ex-1001, 2:11-12.

80. *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. Further, “[t]he key device also has data object forwarding functionality 8 capable of receiving the digital message 16.” *Id.*, 13:31-34

81. *Knutsson* renders obvious the claimed, “the reservation certificate comprising an interval of a reservation” because it discloses its data object 12

(reservation certificate) also includes “temporal data which defines **one or more time frames** during which access is permitted for said key device to said protected environment. In one or more embodiments, such temporal data is specified in a calendar data format, for instance in the form of one of more dates and/or times which define **start and end points** for permitted temporary access.” *Id.*, 6:1-5, 11:32-12:1, FIG. 6 at 628, FIG. 5C at 538. Figures 4a-4b show the “temporal data.”

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

Id., FIGS. 4A-4B (annotated).

82. It is my experience that a POSA would have understood that *Knutsson*'s data object 12 including both a start time and an end time of a temporary access is

an “interval of a reservation” because an interval is defined by a starting point and an end point. By providing start and end times, an interval is presented by *Knutsson*’s key device (portable terminal). *Knutsson*, 12:21-26. In my opinion, a POSA would have understood that the duration of a temporary access defined by a start and end time is an interval. Indeed, the duration can be calculated by subtracting the start time from the end time, such that $\text{duration} = \text{end time} - \text{start time}$. This would have been obvious to a POSA because it is simple to calculate and useful because given any two of start time, end time, or duration, the third can be calculated using the simple, useful formula above. This is confirmed by *Knutsson*’s disclosure of “temporary” access because *Knutsson* is disclosing access for a set time, or an interval. *Knutsson*, Abstract. *Knutsson* confirms, 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.

83. *Knutsson*’s key device 1 receives data object 12, including a communication identifier and temporal data. *Knutsson*, 11:32-12:1, 12:21-26. In my opinion, a POSA would have found it obvious that *Knutsson*’s key device’s functionality would be controlled through a software application that would be able to receive data object 12, including a communication identifier and temporal data,

so that the application could be used to “control the terminal’s functionality,” including sending data object 12 to lock device 40 to unlock the door.

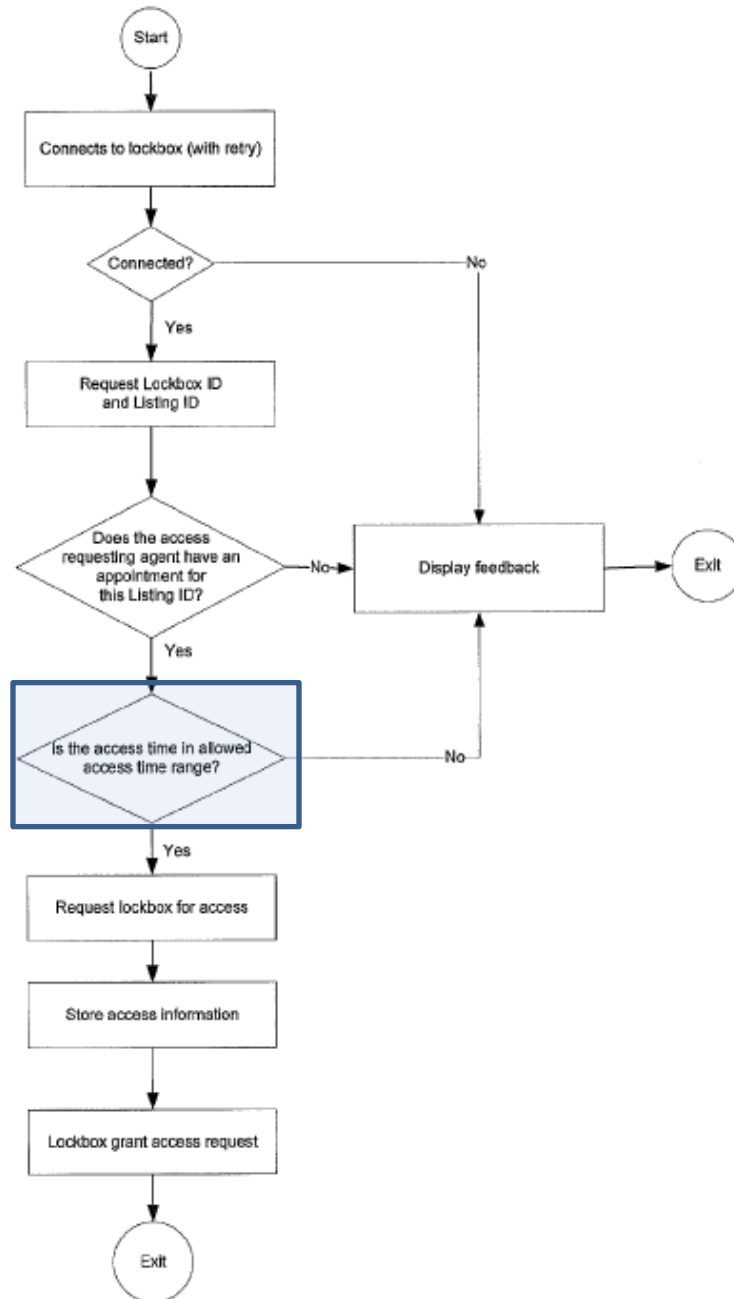
5. [1D] “wherein the application compares the interval of the reservation to a current time accessible to the application to determine if the reservation certificate is current and”

84. *Knutsson* in combination with *Woodard* renders obvious [1D]. *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. *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. *Id.*, 14:12-17, 14:20-23.

85. *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. *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] (emphasis added). 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.

86. 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, in my opinion, 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." *Woodard*, [0004], [0009]. A POSA would have found it obvious that *Knutsson*'s software application would be capable of the similar functions of analyzing and manipulating 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. 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 X.A.

87. In my opinion, 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.

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.”

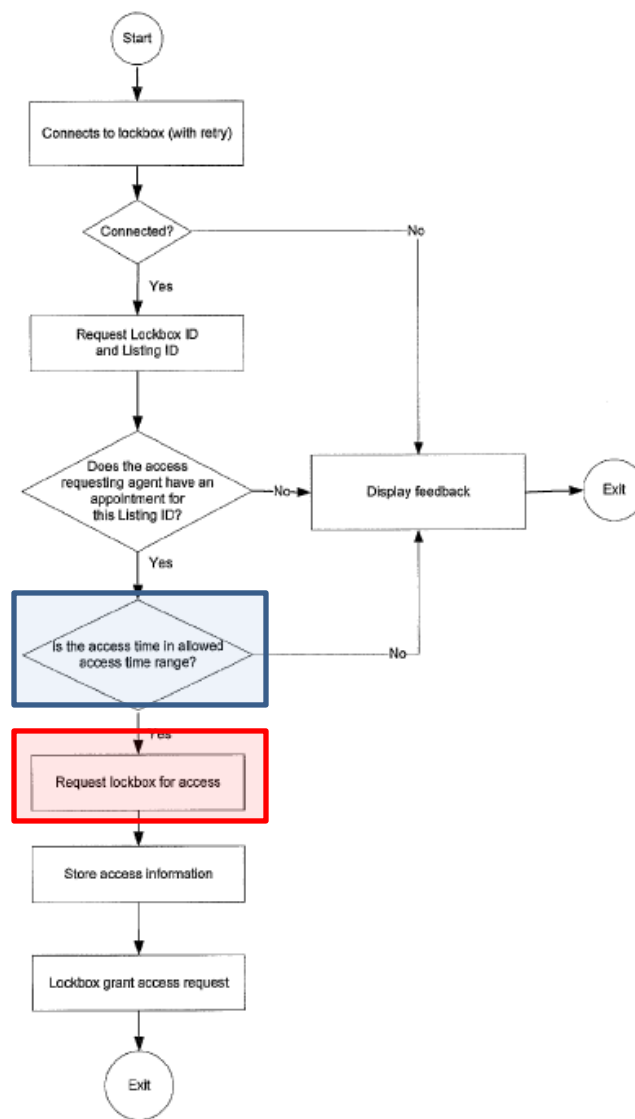
88. *Knutsson* in view of *Woodard* renders obvious [1E]. *Knutsson* renders obvious the claimed “application activates the door lock by communicating with the access device” because *Knutsson*'s key device is “capable of receiving the digital message 16 and forwarding the attached vCard data object 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.

89. *Knutsson* does not explicitly disclose that “communicating with the access device ... when the application determines that the reservation certificate is current,” but *Woodard* does. *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 request for access is sent. *Id.*, FIG. 10.

FIG. 10



Id., FIG. 10.

90. Based on *Woodard*'s disclosure that "actual access to the lockbox 103 is controlled by logic executed inside the electronic key device 104," in my opinion, 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. 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 X.B.5 for [1D], and that the data object 12 is forwarded to the lock device 40 which causes communication with the lock. *Knutsson*, 13:31-14:2. A POSA would have been motivated to combine *Knutsson* and *Woodard*, as discussed above in Sections X.B.5 and X.A.

91. Because the communication identifier (communication setting), which can be a Bluetooth address, is sent to the lock device 40 (access device), and the communication means is a short-range communication, such as Bluetooth, *Knutsson*, 14:18-23, it is my opinion that 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. In my opinion, a POSA would have found it obvious that *Knutsson*'s mobile terminal or key device's functionality would be controlled through a software application that would be able to communicate data object 12 to lock device 40, including the communication identifier, so that the application could be used to "control the terminal's functionality," and communicate with lock device 40 to allow unlocking of the door.

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

92. *Knutsson* in view of *Woodard* renders obvious claim 2. As explained in Section X.B.4 for claim [1C], *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 35 Fig 1) of the lock device 40." *Id.*, 11:32-12:1 (emphasis added). *Knutsson* discloses, "the communication identifier (Bluetooth® address) of the lock device's radio transceiver 49." *Id.*, 12:17-18. In my opinion, a POSA would have understood "a communication identifier ... of the lock device 40" corresponds to the claimed "communication setting is specific to the access device," because the LD_addr of the communication identifier 44 must align with the correspondence lock device in order for the lock device to verify, through verification means 43, that the received data object 12 is appropriate for "the desired

temporary access.” *Id.*, 12:17-18, 16:11-19. 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.

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

93. *Knutsson* in view of *Woodard* renders obvious claim 3. *Knutsson* discloses, “assuming that the lock device 40 is in sleep mode, the initial wake-up stage 610 is performed in steps 612, 614 and 616 by using the proximity sensor 324 to detect the presence of the user of key device 1 near the lock device 40 and in response generate the wake-up control signal 326 to the CPU 313.” *Knutsson*, 19:23-26. After the wake-up signal, *Knutsson*’s CPU 313 within its lock device “proceeds in step 630 to check whether the determined Bluetooth® address of the responding device matches one of afore-described authentication data records.” *Id.*, 20:4-6. If the Bluetooth address is forbidden, CPU 313 may take appropriate action in step 636 “such as generating an alarm signal or... for later reporting.” *Id.*, 20:17-19. In my

² I have been informed by counsel that “the user” in this claim lacks antecedent basis. For the purposes of this proceeding, I have been asked to treat “the user” under a plain and ordinary meaning as the administration-user and/or the guest-user.

opinion, a POSA would have found it obvious that the alarm signal or report would have notified a user of *Knutsson*'s control system including a user of the administration device 20 or a user of the key device 1. Indeed, in my opinion, a POSA would have found it obvious that an alarm or report's function is to provide notice.

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

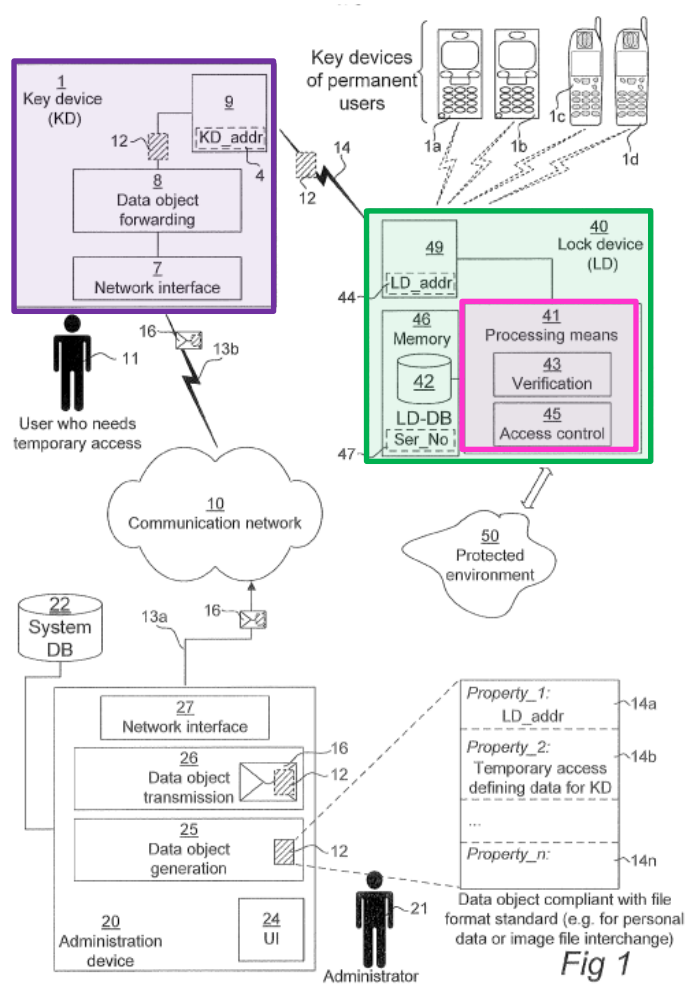
94. *Knutsson* in view of *Woodard* renders obvious claim 4. *Knutsson* discloses, “there may be an optional wake-up stage 518 ... [because] the lock device 40 is operable in a sleep mode and an operational mode. The purpose of the sleep mode is to keep as much as possible of the electronics in the lock device in a shut-off or disabled condition so as to minimize the power consumption during periods of inactivity.” *Knutsson*, 14:23-29. *Knutsson* discloses “the lock device 40 may be awoken[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.*, 14:31-35. *Knutsson* thus discloses its lock device 40 is in a sleep mode, and thus incapable of sending an advertisement signal, because “as much as possible of the electronics in the lock device” are off or disabled, excluding only 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. In my opinion, 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."

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.

95. *Knutsson* in view of *Woodard* renders obvious claim 5. *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 to receive the digital message from the administration device, temporarily save the

embedded data object in the **mobile terminal** and then have it forwarded to **the lock device** by way of Bluetooth® communication.” *Knutsson*, 5:20-23. *Knutsson* also discloses, “the **processing means** is configured to detect a communication identifier of the key device (such as its Bluetooth® address).” *Id.*, 7:26-27.



Id., FIG. 1 (annotated).

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.

96. *Knutsson* in view of *Woodard* renders obvious claim 6. As explained in Section X.F for claim 5, *Knutsson*'s software on key device 1 (application) communicates with its lock device 40 (access device) using Bluetooth and the communication setting comprises a network SSID. *Knutsson*, 5:20-23. *Knutsson* discloses the claimed, "uses Wi-Fi" because *Knutsson* discloses "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. A POSA would have understood that IEEE 802.11 is a Wi-Fi standard. 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]. In my opinion, a POSA would thus have understood Wi-Fi would be one of the short-range wireless communications used between *Knutsson*'s key device 1's application and lock device 40.

97. 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. *Knutsson* renders obvious the claimed “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 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. 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. Thus, in my opinion, a POSA would have found it obvious to use the SSID as part of the communication identifier in a Wi-Fi network. 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.

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

98. *Knutsson* in view of *Woodard* renders obvious claim 7. As explained in Section X.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 35 Fig 1) of the lock device 40.” *Knutsson*, 11:32-12:1 (emphasis added). Thus, *Knutsson* discloses the data object 12 (reservation certificate) includes a communication identifier (communication setting).

I. Claim 15

99. *Knutsson* in view of *Woodard* renders obvious claim 15.

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

100. [15p] is identical to [1p]. *Knutsson* renders obvious [15p] as explained for [1p] in Section X.B.1.

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

101. [15A] is identical to [1A]. *Knutsson* renders obvious [15A] as explained for [1A] in Section X.B.2.

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

102. [15B] is identical to [1B]. *Knutsson* renders obvious [15B] as explained for [1B] in Section X.B.3.

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,”

103. *Knutsson* renders obvious [15C]. As explained for [1C] in Section X.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.”

104. *Knutsson* also at least suggests that the reservation certificate is provided to the applicant “via the first communication protocol,” because *Knutsson* discloses, “[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.*, 4:4-8. *Knutsson* discloses, “communication network 10 is a mobile telecommunications network compliant with for instance GSM, UMTS, D-AMPS, CDMA2000, FOMA or TD- SCDMA.” *Id.*, 13:13-15. A POSA would have understood that any 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.

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”

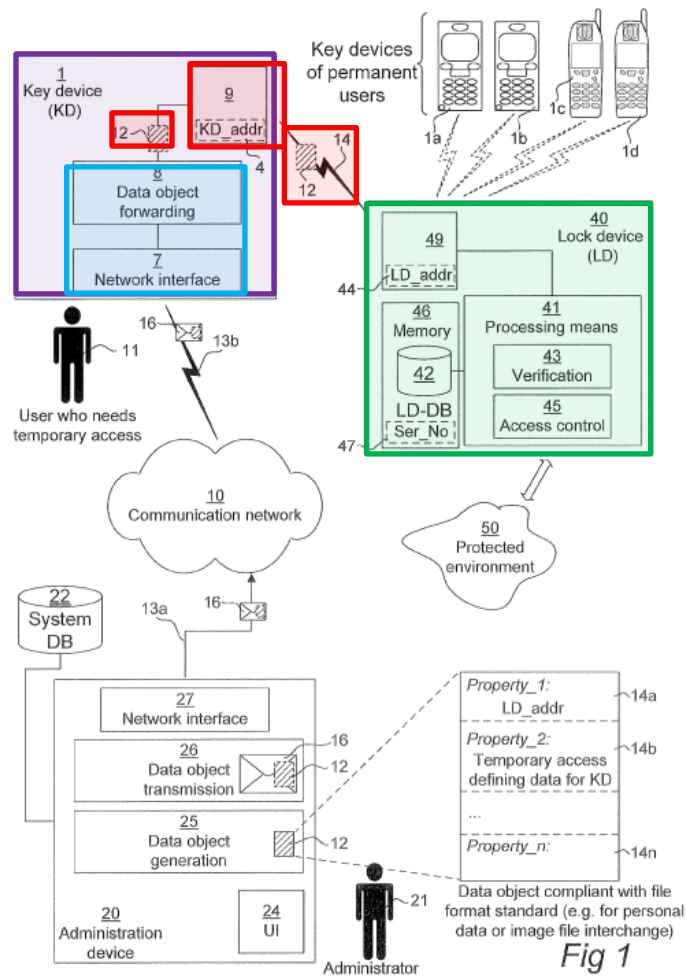
105. [15D] is identical to [1D]. *Knutsson* renders obvious [15D] as explained for [1D] in Section X.B.5.

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.”

106. *Knutsson* in view of *Woodard* renders obvious [15E]. As explained for claim [1E] in Section X.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.”

107. *Knutsson* also discloses, “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. 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.



Id., FIG. 1 (annotated).

108. The “short-range 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, 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 “GSM, UMTS, D-AMPS, CDMA2000, FOMA, or TD-SCDMA.” *Id.*, 13:12-15. Thus, in my opinion, a POSA

would have understood *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.

109. *Knutsson* discloses, “short-range wireless data communication means capable of short-range wireless data communication based on a communication identifier of said lock device.” *Id.*, 7:15-18. In my opinion, 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). *Id.*, 14:1-2. In my opinion, a POSA would have found it obvious that *Knutsson*'s mobile terminal having software applications uses *Knutsson*'s communication identifier because *Knutsson* discloses a “user interface 24” that selects or specifies the communication identifier. *Knutsson*, 11:1-6, 11:32-12:3. It is further my opinion that a POSA would have understood that *Knutsson*'s mobile terminal having software uses the *Knutsson*'s communication identifier because *Knutsson* discloses “lock device 40 detects the communication identifier ... of the key device 1.” *Id.*, 16:4-5.

110. The lock device 40 and the key device 1 communicate based on *Knutsson*'s disclosure that "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. *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. Because the communication identifier which can be a Bluetooth address (communication setting) is sent to the lock device 40 (access device), *id.*, 16:1-3, and the used communication means is a short-range communication like Bluetooth, in my opinion, a POSA would have found it obvious that *Knutsson*'s software on mobile terminal, the combined application, unlocks the door when it communicates the Bluetooth address through Bluetooth and when the current time is within the time slot of the data object 12.

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

111. *Knutsson* renders obvious claim 16. As explained for [15C] in Section X.I.4, *Knutsson* discloses, "[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.*, 4:4-8. *Knutsson* discloses, “communication network 10 is a mobile telecommunications network compliant with for instance GSM, UMTS, D-AMPS, CDMA2000, FOMA or TD-SCDMA.” *Id.*, 13:12-15. In my opinion, a POSA would have understood that any of the listed telecommunications networks are cellular protocols, consistent with *Knutsson*’s disclosure.

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

112. *Knutsson* in view of *Woodard* renders obvious claim 17. As explained for [15C] in Section X.I.4, *Knutsson* discloses, “[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.*, 4:4-8. *Knutsson* discloses 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 its devices communicate over “a wireless local area network (WLAN) standard.” *Id.*, 22:15-19.

113. A POSA would have understood *Knutsson* to at least suggest a “wireless LAN protocol” as the first communication protocol because *Knutsson*’s key device 1 communicates with communication network 10 to access “the Internet” through known communication methods such as through HomeRF, IEEE 802.11 (Wi-Fi), and WiMax. *Knutsson*, 22:18-19. Thus, a POSA would have understood that *Knutsson*’s disclosure of WLAN applies to 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.

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

114. *Knutsson* in view of *Woodard* renders obvious claim 18. As explained for [15C] in Section X.I.4, *Knutsson* discloses, “[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.*, 4:4-8. *Knutsson* discloses communications network 10 “comprise a wide-area data communication network, for instance being a part of the Internet.” *Id.*, 13:15-16.

115. A POSA would have understood *Knutsson* to disclose or at least suggest “Wi-Fi” because *Knutsson*’s key device 1 could communicate with communication network 10 through *Knutsson*’s disclosed WLAN to access “the Internet.” Indeed, *Knutsson* states that its key device 1 use short-range communication such as WLAN and 802.11, which is Wi-Fi. *Knutsson*, 22:18-19. Thus, 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.

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

116. *Knutsson* in view of *Woodard* renders obvious claim 19. *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.

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

117. *Knutsson* renders obvious claim 20. *Knutsson* discloses the “short-range wireless data communication means 9 to the lock device 40,” communicates through “Bluetooth®.” *Knutsson*, 13:31-14:2.

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

118. *Knutsson* renders obvious claim 21. *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**,” which corresponds to the claimed wireless LAN protocol. *Knutsson*, 13:31-34, 22:15-19, FIG. 1 (emphasis added).

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

119. *Knutsson* in view of *Woodard* renders obvious claim 22. *Knutsson* discloses the “short-range wireless data communication means 9 to the lock device 40, as seen at 14,” such as *Knutsson*’s disclosure of IEEE 802.11. *Knutsson*, 13:3-

34, 22:15-19. A POSA would have understood that IEEE 802.11 corresponds to Wi-Fi as explained for claim 6 in Section X.G.

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.

120. *Knutsson* renders obvious claim 23. *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 (emphasis added). *Knutsson* further 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 (emphasis added).

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

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

122. *Knutsson* renders obvious claim 24. *Knutsson* discloses, “all communication between key device and lock device may be encrypted in accordance

with an encryption algorithm.” *Knutsson*, 19:12-14. *Knutsson* similarly discloses, “enhanced security is obtained by configuring the administration device to encrypt the contents of the generated data object.” *Id.*, 6:13-15.

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

123. *Knutsson* 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.

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

A. Claim 8

124. *Knutsson* renders obvious claim 8.

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

125. [8p] is identical to [1p]. *Knutsson* renders obvious [8p] as explained for [1p] in Section X.B.1.

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

126. [8A] is identical to [1A]. *Knutsson* renders obvious [8A] as explained for [1A] in Section X.B.2.

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

127. [8B] is identical to [1B]. *Knutsson* renders obvious [8B] as explained for claim [1B] in Section X.B.3.

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,”**

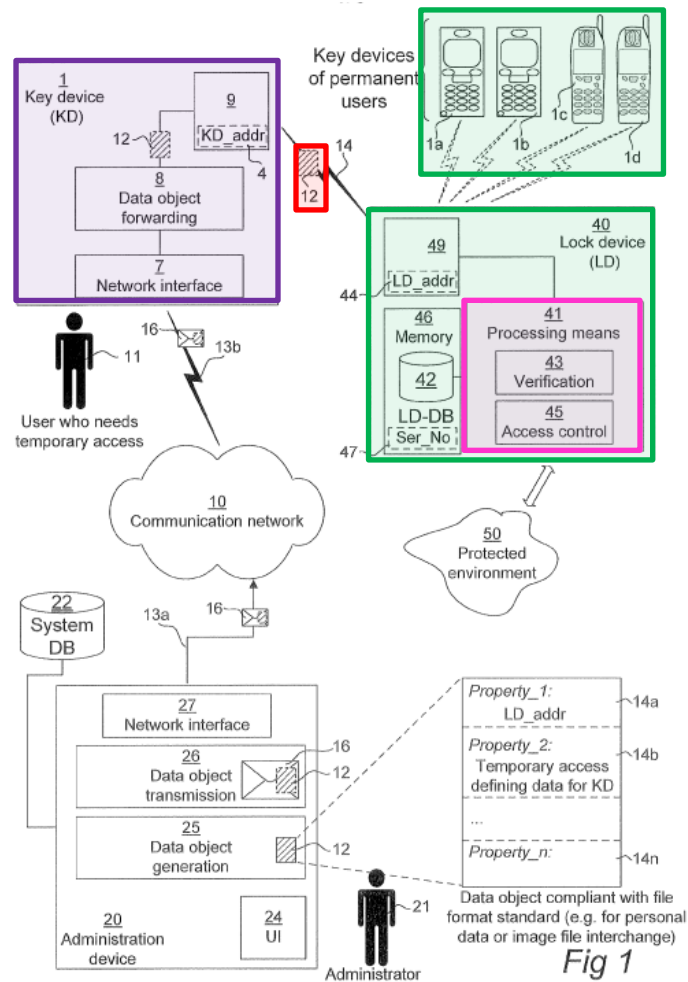
128. [8C] is substantially similar to [1C]. *Knutsson* renders obvious claim [8C] as explained for [1C] in Section X.B.4.

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

129. *Knutsson* renders obvious claim [8D]. As discussed above in Section X.B.3, *Knutsson*’s key device is the claimed “portable terminal” and includes “a graphical user interface 206 ... which may be used by a user of the mobile terminal to **control the terminal’s functionality** and get access to any of the telecommunications services referred to above, or to **any other software application** executing in the mobile terminal.” *Knutsson*, 13:20-28 (emphasis added). *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 of sending the vCard 12 to lock device 40. *Knutsson*, 14:12-17, 14:20-23.

130. *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.*, 16:6-8, 17:11-13, 20:8-11.



Id., FIG. 1 (annotated).

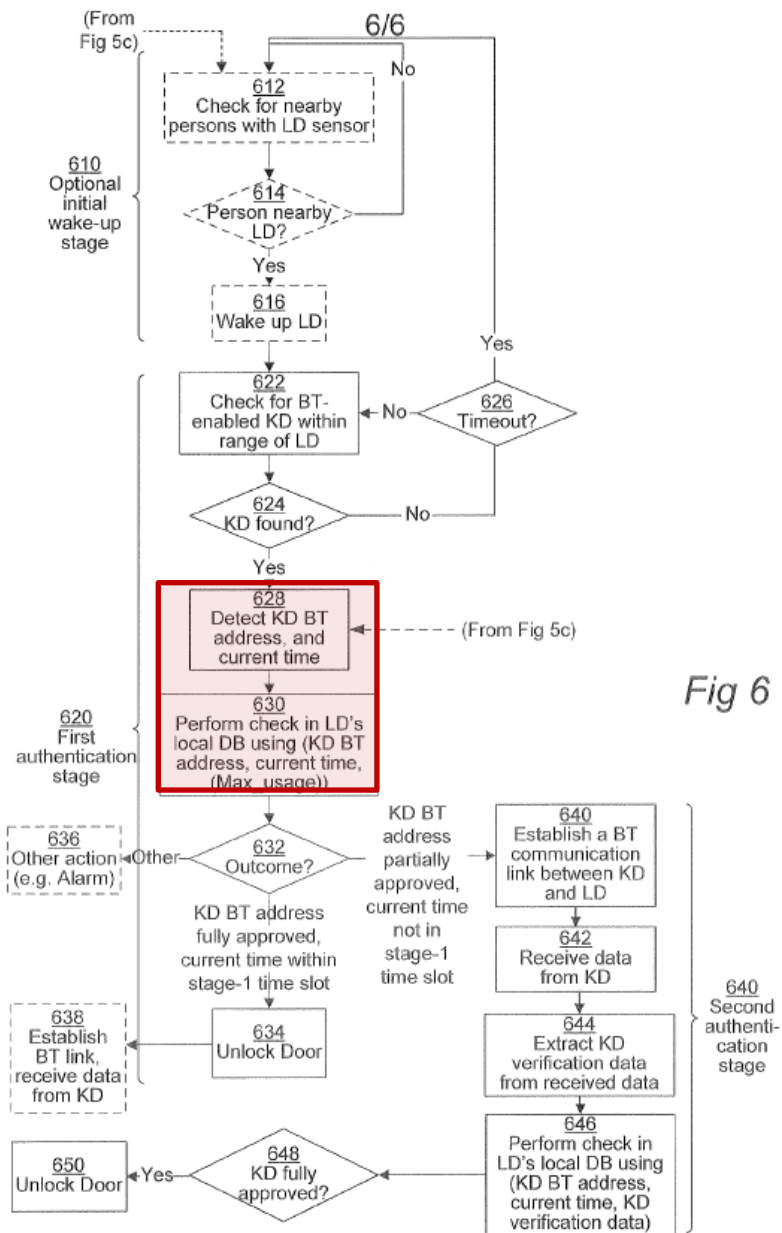
131. *Knutsson* discloses the claimed “processor receives the reservation certificate from the application.” *Knutsson*’s software application is capable of receiving a user command to “Send by Bluetooth®” to “cause the key device 1 to attempt to establish short-range data communication 14 with the lock 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 X.B.4, *Knutsson*’s data object 12 comprises a Bluetooth address.

132. Because the communication identifier that, as described above, can be a Bluetooth address (communication setting), is sent to the lock device 40 (access device), and the communication means is a short-range communication, like Bluetooth, initiated by the user command through the software application on key device 1, in my opinion, 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.

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”

133. *Knutsson* renders obvious [1D]. *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. *Knutsson* also discloses, “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.*, 6:4-6.



Id., FIG. 6 (annotated).

134. *Knutsson*'s **stage 1 authentication** determines "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.” *Id.*, 18:1-3. A structure that the lock device 40 uses to store authentication data is shown as LD-DB42:

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

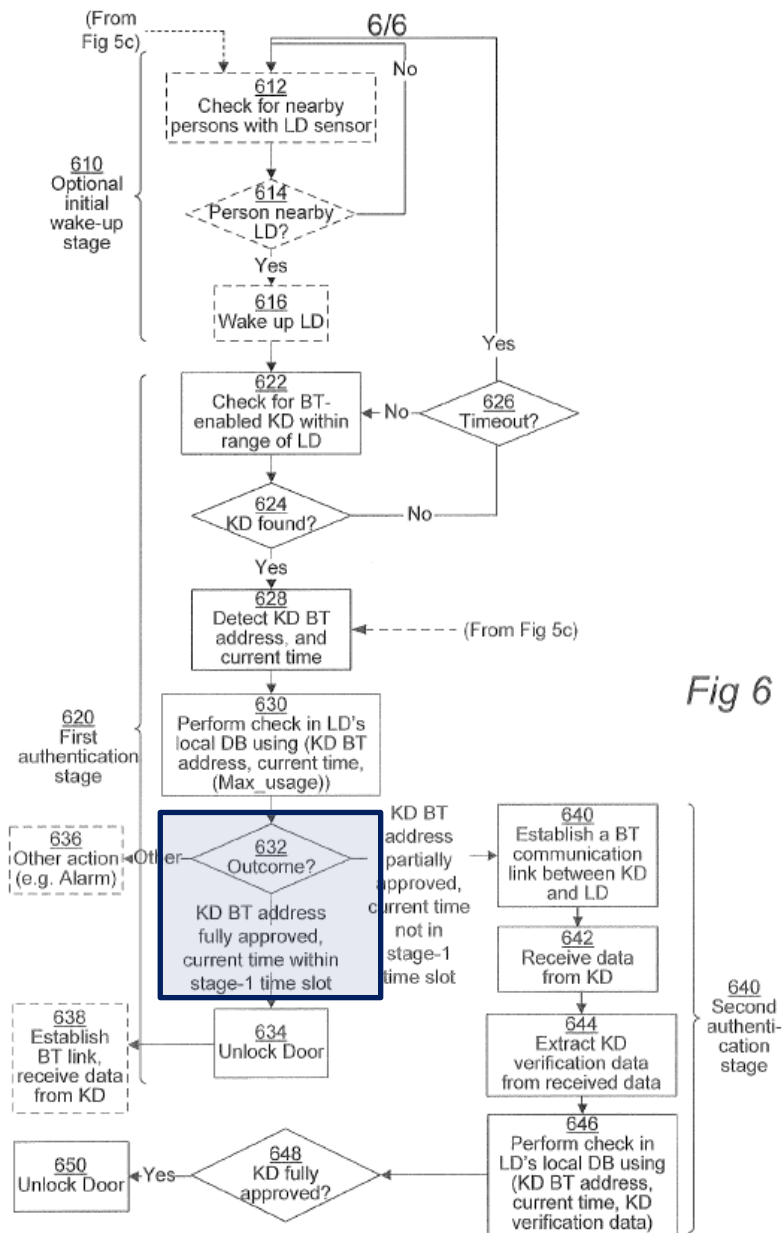
Id., Table 1 at 18 (annotated).

135. A POSA would have understood that *Knutsson*’s time slot, starting at a start point and ending at an end point, corresponds to the claimed, “interval” because an interval is set forth by start and end points as discussed above in Section X.B.3.

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

136. *Knutsson* renders obvious [8F]. *Knutsson* discloses that “using the proximity sensor 324 to detect the presence of the user of key device 1 near the lock device 40 and in response generate the wake-up control signal 326 to the CPU 313.” *Knutsson*, 19:23-26. As discussed above, the CPU 313 of the lock device “check[s] whether the current time falls within any stage-1 time slot defined for that

Bluetooth® address.” *Id.*, 20:5-7. And, “[i]f the outcome of these checks is fully positive, as checked in [step 632](#), the CPU 313 proceeds to step 634 and generates the control signal 307a to the actuator controller 307. As described above, this will cause unlocking of the lock, etc, and allow opening of the door, etc, to the protected environment.” *Id.*, 20:7-11. FIG. 6, including step 632 is shown below.



Id., FIG. 6 (annotated).

137. *Knutsson* further 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.” *Id.*, 18:1-4. The authorization leads to the unlocking of the lock. *Id.*, 20:7-11.

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

138. 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 X.C.

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

139. 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 X.D.

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

140. 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 X.E.

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.

141. 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 X.F.

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.

142. 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 X.G.

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

143. 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 X.H.

H. Claim 26

144. *Knutsson* renders obvious claim 26.

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

145. [26p] is identical to [1p]. *Knutsson* renders obvious [26p] as explained for [1p] in Section X.B.1

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

146. [26A] is identical to [1A]. *Knutsson* renders obvious [26A] as explained for [1A] in Section X.B.2.

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

147. [26B] is identical to [1B]. *Knutsson* renders obvious [26B] as explained for [1B] in Section X.B.3.

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,”**

148. [26C] is identical to [15C]. *Knutsson* renders obvious [26C] as explained for [15C] in Section X.I.4.

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,”**

149. [26C] is substantially similar to [8D]. *Knutsson* renders obvious [26C] as explained for [8D] in Section XI.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 X.I.6.

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”**

150. [26E] is identical to [8E]. *Knutsson* renders obvious [26E] as explained for [8E] in Section XI.A.6.

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

151. [26F] is identical to [8F]. *Knutsson* renders obvious [26F] as explained for [8F] in Section XI.A.7.

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

152. 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 X.J.

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

153. 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 X.K.

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

154. Claim 29 is identical to claim 18, aside from its dependency from claim 26. *Knutsson* renders obvious claim 29 as explained for claim 18 in Section X.L.

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

155. 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 X.M.

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

156. 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 X.N.

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

157. 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 X.O.

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

158. 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 X.P.

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.

159. 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 X.Q.

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

160. 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 X.R.

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

161. 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 X.S.

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

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

162. As explained in Section IX, claim 3 requires the application of the mobile terminal to notify the user of the proximity of the lock.

163. *Knutsson* at least suggests a proximity notification, as explained for claim 3 in Ground 1, Section X.D. To the extent that it is argued that *Knutsson* does not disclose this element, *Bröndrup* does. In my experience 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*, 2:10-14. 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.” *Id.*, 3:10-14. Besides maintaining a complete record, a POSA would have been further motivated to implement *Bröndrup* so that

Knutsson's key device 1 would be capable of "without having to make a check-in at the reception desk of [the] hotel." *Id.*, 11:17-20.

164. In my opinion, 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, communicates through Bluetooth to lock device 40 when the mobile terminal draws near. *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," *id.*, 6:4-6, and *Knutsson*'s key device that can be a PDA or a mobile phone, *Knutsson*, 5:1-2, and *Woodard*'s "electronic key device 104, which can be a PDA, a cell phone." *Woodard*, [0003], to actuate access devices like *Bröndrup*'s wireless door lock (9, 32), *Bröndrup*, Abstract, or *Knutsson*'s lock device 40 to open a lock, *Knutsson*, 10:24-30, or access devices like *Woodard*'s lockbox 103, *Woodard*, [0048].

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

165. *Knutsson* in view of *Woodard* and *Bröndrup* renders obvious claim 3. *Knutsson* at least suggests a proximity notification, as explained for claim 3 in

Ground 1, Section X.D. To the extent it is argued *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*, 7:30-33. *Bröndrup* discloses, by means of 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. Thus, in my opinion, a POSA would have found it obvious that the notification would be sent to a user of the hotel reservation system as well as a user of the mobile phone when the mobile terminal is near the door lock. In my experience, a POSA would have further understood that *Bröndrup*’s short range wireless device 25 of the mobile wireless terminal 1 communicates to the door lock 32 through Bluetooth renders obvious the claimed “proximity to the access device” because the Bluetooth communication is necessarily near to the door lock 32. As discussed above in Section XII.A, it is also my opinion that a POSA would have been motivated to combine *Knutsson*, *Woodard*, and *Bröndrup*.

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

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

166. As explained in Section IX, claim 4 requires that the communication module does not advertise that the communication module is present.

167. *Knutsson* renders obvious a communication module being non-operational and thus not sending signals (advertising) its presence, as explained for claim 4 in Ground 1, Section X.E. To the extent that it is argued that *Knutsson* does not disclose this element, *Adams* does. In my opinion, 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*, [0007]. Further, 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. Likewise, it is my opinion that 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]. The similar goals of controlling access in *Adams*, *Woodard*, and *Knutsson* are achieved through *Adams*' non-discoverable mode by preventing unauthorized access. Additionally, in my opinion, 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 access of an infiltrator to *Knutsson*'s protected environment.

168. In my experience, a POSA would have had reasonable expectations of success of 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]. *Adams* discloses a non-discoverable mode on a device 102 that "is a [Bluetooth] device" and has a button where "device 102 may become discoverable once the button is depressed and may become non-discoverable once the button is released." *Adams*, [0045]. *Adams* discloses the Non-Discoverable Mode is available on conventional devices 102 and 104 such as "wireless computerized devices, for example... handheld computers, cellular telephones." *Id.*, [0019]. *Knutsson* likewise discloses key and lock devices that use Bluetooth® to communicate with each other through their

Bluetooth® transceivers. *Knutsson*, 12:3-4, 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. Thus, *Adams*, *Woodard*, and *Knutsson* disclose devices that work in an access control system with similar communications technology. Because *Knutsson*'s key and lock devices communicate through Bluetooth® and employ Bluetooth® transceivers, it my opinion that 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. Further, in my opinion, a POSA would have been successful in implementing *Adams*'s "Non-Discoverable Mode" because *Knutsson*'s lock device operates based on receiving a Bluetooth® address. *Adams* explains "[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*, [0006]. Thus, although *Knutsson*'s lock device is in Non-Discoverable Mode, *Knutsson*'s key device would be able to 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.

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

169. *Knutsson* in view of *Adams* renders obvious claim 4. To the extent it is argued *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. As *Adams* explains, in the Non-Discoverable Mode, “a [Bluetooth] device is visible to other [Bluetooth] device 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). A POSA would have been motivated to combine *Knutsson* and *Adams* as discussed above in Section XIII.A.

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

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

170. As explained in Section IX, claim 10 requires the application notify the user of proximity of the access device.

171. *Knutsson* at least suggests a proximity notification, as explained for claim 3 in Ground 1, Section X.D. To the extent *Knutsson* does not disclose the notification limitation, *Bröndrup* does. In my experience a POSA would have been motivated to combine *Knutsson* and *Bröndrup* as disclosed in Section XII.A. The further combination of *Woodard* in Section XII.A does not affect the combination of *Knutsson* and *Bröndrup*, and in my experience a POSA would have been motivated to combine *Knutsson* and *Bröndrup* for the same reasons discussed above in Section XII.A.

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

172. 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 XI.B. In my experience a POSA would have been motivated to combine *Knutsson* and *Bröndrup* as explained in Sections XIII.A and XII.A.

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

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

173. As explained in Section IX, claim 11 requires that the communication module does not advertise that the communication module is present.

174. *Knutsson* renders obvious the communication not advertising itself, as explained for claim 4 in Ground 1, Section X.E. To the extent it is argued *Knutsson* does not disclose the notification limitation, *Adams* does as explained for claim 4 in Ground 4, Section XIII.B. A POSA would have been motivated to combine *Knutsson* and *Adams* as disclosed in Section XIII.A. The further combination of *Woodard* in Section XIII.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 XIII.A.

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

175. 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 XIII.B. A POSA would have been motivated to combine *Knutsson* and *Adams* as explained in Sections XIII.A and XV.A.

XVI. GROUND 7: CLAIMS 6, 17, AND 18 ARE RENDERED OBVIOUS BY KNOTSSON IN VIEW OF WOODARD AND JAIN

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

176. As explained in Section IX, claim 6 requires the communication setting to comprise a SSID.

177. As explained for claim 6 in Ground 1, Section X.G, *Knutsson* at least suggests an SSID. To the extent *Knutsson* does not expressly disclose this limitation, in my experience 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]. 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. Because *Knutsson* describes that its system is implemented on a IEEE 802.11 (Wi-Fi) system, *Knutsson*, 22:15-19, it is my experience that a POSA would have looked to *Jain* to implement the Wi-Fi system including modifying *Knutsson*'s communication identifier to be a SSID identifier. 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. In my opinion, a POSA also would have found the substitution of *Jain*'s SSID identifier for a Wi-Fi network for *Knutsson*'s

communication identifier that can be a Bluetooth address would yield predictable results when implementing *Knutsson*'s Wi-Fi system.

178. In my opinion, a POSA would have had a reasonable expectation of implementing *Jain*'s SSID within *Knutsson* because *Jain* and *Knutsson* disclose similar key devices such as *Jain*'s host device that includes "a cellphone, a smart-phone," *Jain*, [0018], and *Knutsson*'s key device that can be a PDA or a mobile phone, *Knutsson*, 5:1-2, to actuate access devices like *Jain*'s computer that can be a POS 114 and can be used for "physical access control," *Jain*, [0030], or *Knutsson*'s lock device 40 to open a lock. *Knutsson*, 10:24-30. A POSA would have been motivated to combine *Woodard* with *Knutsson* and *Jain* for the same reasons discussed in Ground 1, Sections X.A, X.B.5.

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.

179. As explained for claim 6 in Ground 1, Section X.G, *Knutsson* renders obvious the application using Wi-Fi to communicate with the access device and an SSID.

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

181. *Jain* discloses, “the host device may be a cellphone such that the card 400 may request network authentication prior to activation. For example, the card 400 may be distributed by a Wireless Network Operator (WNO) that requires a network authentication. In this example, a flag in memory may be set to ON indicating that network authentication is required. If the flag is set to ON, a unique identity about the allowed network is 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, “the CPU 408 in response to at least insertion may request a special software plug-in to be downloaded to the host device and instantiated. This software plug-in 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.*, [0068].

182. Further, it is my opinion that a POSA would have been motivated to combine *Jain* and the *Knutsson-Woodard* combination for the reasons explained in Section XVI.A.

183. In my experience 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.” *Id.*, [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]. *Jain*, like *Knutsson* and *Woodard*, also 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.

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

184. *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.”

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

186. 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].

187. In my opinion, a POSA would have found it obvious that *Jain*’s use of Wi-Fi between its mobile device 110 and financial institution 106 could be implemented between *Knutsson*’s key device 1 and administrative device 20. 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. In my opinion, 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 predictable use of one of a limited number of communication technologies. Thus, a POSA would have found claim 17 obvious over *Knutsson* in view of *Jain* and *Woodard* as further explained in Section XVI.A.

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

188. *Knutsson* in view of *Jain* and *Woodard* renders obvious claim 18 as explained for claim 17 in Section XVI.C.

189. Because *Jain* discloses that “the financial institutions 106 may wirelessly communicate with the transaction card 112f using, for example, WiFi technology.” *Jain*, [0069]. In my experience a POSA would have been motivated to combine *Jain* and the *Knutsson-Woodard* combination as discussed for claim 17 in Sections XVI.A and XVI.C.

XVII.GROUND 8: CLAIMS 13, 28, and 29 ARE RENDERED OBVIOUS BY KNUTSSON IN VIEW OF JAIN

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

190. As explained in Section IX, claim 13 requires the communication setting to comprise a SSID, which *Knutsson* does not expressly disclose. *Knutsson* renders obvious the SSID, as explained for claim 6 in Ground 1, discussed in Section

X.G. 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 XVI.B. The further combination of *Woodard* in Section XVI.A does not affect the combination of *Knutsson* and *Jain*, and in my experience a POSA would have been motivated to combine *Knutsson* and *Jain* for the same reasons discussed above in Section XVI.A.

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.

191. 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 XVI.B. In my experience a POSA would have been motivated to combine *Jain* and *Knutsson* as explained in Section XVII.A.

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

192. *Knutsson* in view of *Jain* renders obvious claim 28 as explained for claim 17 in Section XVI.C. In my experience a POSA would have been motivated to combine *Jain* and *Knutsson* as discussed above for Section XVII.A.

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

193. *Knutsson* in view of *Jain* renders obvious claim 29 as explained for claim 18 in Section XVI.D. In my experience a POSA would have been motivated to combine *Jain* and *Knutsson* as discussed above for Section XVII.A.

XVIII. CONCLUSION

194. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed this 25th day of May 2023, in Windsor, MA.

Respectfully submitted