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. 9,373,205
Filing Date: January 23, 2015
Issue Date: June 21, 2016

_____

Case No. IPR2023-00815

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 '205 PATENT 17

VI. OVERVIEW OF PRIOR ART 18

A. *Knutsson* 18

B. *Elfström* 19

C. *Woodard* 20

D. *DeBry* 22

E. *Micali* 23

VII. LEVEL OF ORDINARY SKILL IN THE ART 23

VIII. CLAIM CONSTRUCTION 24

IX. SUMMARY OF OPINIONS 25

A. The *Knutsson* Grounds (Grounds 1-3) 26

B. The *Elfström* Grounds (Grounds 4-6) 30

X. GROUND 1: CLAIMS 1-6, 8-10, 13-18, AND 20-22 ARE RENDERED OBVIOUS BY *KNUTSSON* 33

A. Claim 1 33

1. [1p] "An access device for use in an access control system, the access device comprising:" 33

2. [1A] “a processor (16) having control of a door lock (11); and” 34

3. [1B] “a communication module (17) connected to the processor, the processor is configured to receive a reservation certificate (5) presented by a portable terminal (4) through the communication module;” 37

4. [1C] “wherein, when a current reservation certificate that comprises an interval of a reservation is presented by the portable terminal,” 42

5. [1D] “the processor is configured to compare the interval of the reservation of the current reservation certificate to a current time accessible to the processor, determine the current time is within the interval of the reservation, and” 45

6. [1E] “activate the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation.” 48

B. Claim 2 50

1. [2A] The access device of claim 1 wherein the processor is configured to determine the current time is within the interval of the reservation by determining if the current time is within a start time of the interval of the reservation of the current reservation certificate and a predetermined duration and 50

2. [2B] is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the predetermined duration. 51

C. [Claim 3] The access device of claim 2 wherein the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation from the start time up to the predetermined duration that is all day.....53

D. [Claim 4] The access device of claim 1 wherein the interval of the reservation of the current reservation certificate comprises a start time and a duration and the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the duration.....56

E. [Claim 6] The access device of claim 1 wherein the interval of the reservation of the current reservation certificate comprises a start time and an end time. 57

F. [Claim 5] The access device of claim 6 wherein the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the end time. 60

G. Claim 8 60

1. [8A] The access device of claim 1 further comprising: a memory to which the processor has access, the memory is configured to comprise a symmetric key: 60

2. [8B] wherein at least a portion of the current reservation certificate is encrypted by a server of the access system configured to use the symmetric key and the processor is configured to verify that the current reservation certificate is genuine by decrypting the portion with the symmetric key. 64

H. [Claim 9] The access device of claim 1 wherein the processor is configured to verify that the current reservation certificate is genuine. 67

I. [Claim 10] The access device of claim 1 further comprising: an identification to which the processor has access, the identification corresponding to one of the access device and the door lock, wherein the processor is configured to determine that the current reservation certificate comprises data representative of the identification. 68

J. Claim 13 71

1. [13p] “A method for use by an access device in an access control system, the method comprising:” 71

2. [13A] “accepting, by a processor” 71

3. [13B] “through a communication module, a reservation certificate… presented with a portable terminal;.....71

4. [13C] “a reservation certificate that comprises an interval of a reservation” 72

5. [13D] “determining, by the processor, that the reservation certificate presented by the portable terminal is current by comparing the interval of the reservation to a current time accessible to the processor and determining that the current time is within the interval of the reservation; and activating, by the processor on the basis of the reservation certificate being current,” 72

6. [13E] “activating… a door lock to allow the portable terminal to unlock the door lock during the interval of the reservation.” 73

K. [Claim 14] The method of claim 13 wherein determining that the current time is within the interval of the reservation comprises determining that the current time is within a start time of the interval of the reservation and a predetermined duration and wherein the certificate is current from the start time up to the predetermined duration. 73

L. [Claim 15] The method of claim 14 wherein the predetermined duration is all day. 74

M. [Claim 16] The method of claim 13 wherein the interval of the reservation of the reservation certificate further comprises a start time and a duration and the reservation certificate is current from the start time up to the duration. 74

N. [Claim 18] The method of claim 13 wherein the interval of the reservation comprises a start time and an end time. 74

O. [Claim 17] The method of claim 18 wherein the reservation certificate is current from the start time up to the end time. 74

P. [Claim 20] The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a symmetric key stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the resrvation certificate is genuine on the basis of decrypting the portion with the symmetric key, and the c) activating is on the further basis of the reservation certificate being genuine. 74

Q. [Claim 21] The method of claim 13 wherein the b) determining by the processor is further that the reservation certificate is genuine, and the c) activating is on the further basis of the reservation certificate being genuine. 75

R. [Claim 22] The method of claim 13 wherein the processor has access to an identification, the identification corresponding to one of the access device and the door lock, wherein the b) determining by the processor is further that the reservation certificate comprises data representative of the identification, and the c) activating is on the further basis of the reservation certificate comprising data representative of the identification. 76

XI. GROUND 2: CLAIMS 7, 11, 19, AND 23 ARE RENDERED OBVIOUS BY *KNUTSSON* IN VIEW OF *DEBRY* 76

A. Motivation to Combine *Knutsson* and *DeBry* 76

B. Claim 7 79

1. [7A] The access device of claim 1 further comprising: a memory to which the processor has access, the memory is configured to comprise a public key for a server of the access system configured to issue the current reservation certificate;.....79

2. [7B] wherein at least a portion of the current reservation certificate is encrypted by the server using a private key and the processor is configured to verify that the current

reservation certificate is genuine by decrypting the portion with the public ey. 84

C. Claim 11 85

1. [11A] The access device of claim 1 further comprising: a memory to which the processor has access, the memory is configured to comprise a private key of the access device; 85

2. [11B] wherein at least a portion of the current reservation certificate is encrypted by a server of the access system configured to use a corresponding public key for the access device and the processor is configured to decrypt the portion with the private key. 89

D. [Claim 19] The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a private key for which the corresponding public key is stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the public key, and the c) activating is on the further basis of the reservation certificate being genuine....90

E. [Claim 23] The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a public key for which the corresponding private key is stored in a memory accessible to the processor, the method further comprising the step of: d) decrypting the portion, by the processor, with the private key....90

XII. GROUND 3: CLAIMS 12, 24 ARE RENDERED OBVIOUS BY *KNUTSSON* IN VIEW OF *WOODARD*....91

A. Motivation to Combine *Knutsson* and *Woodard*....91

B. [Claim 12] The access device of claim 1 wherein the processor has access to a server of the access system through the communication module and the processor is configured to

report to the server that the door lock was activated on the basis of the reservation certificate. 93

C. [Claim 24] The method of claim 13 wherein the processor has access to a server through the communication module, the method further comprising the step of: d) reporting to the server that the door lock was activated on the basis of the reservation certificate. 95

XIII. GROUND 4: CLAIMS 1-6, 9-10, 12-18, 21-22, AND 24 ARE UNPATENTABLE OVER *ELFSTRÖM* IN VIEW OF *WOODARD* 95

A. Motivation to Combine *Elfström* and *Woodard* 95

B. Claim 1 97

1. [1p] "An access device for use in an access control system, the access device comprising:" 97

2. [1A] "a processor (16) having control of a door lock (11);" 98

3. [1B] "a communication module (17) connected to the processor, the processor is configured to receive a reservation certificate (5) presented by a portable terminal (4) through the communication module;" 100

4. [1C] "wherein, when a current reservation certificate that comprises an interval of a reservation is presented by the portable terminal," 102

5. [1D] "the processor is configured to compare the interval of the reservation of the current reservation certificate to a current time accessible to the processor, determine the current time is within the interval of the reservation, and" 102

6. [1E] "activate the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation." 105

C. Claim 2 108

1. [2A] The access device of claim 1 wherein the processor is configured to determine the current time is within the interval of the reservation by determining if the current time is within a start time of the interval of the reservation of the current reservation certificate and a predetermined duration and 108

2. [2B] is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the predetermined duration. 109

D. [Claim 3] The access device of claim 2 wherein the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation from the start time up to the predetermined duration that is all day.....111

E. [Claim 4] The access device of claim 1 wherein the interval of the reservation of the current reservation certificate comprises a start time and a duration and the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the duration.....113

F. [Claim 6] The access device of claim 1 wherein the interval of the reservation of the current reservation certificate comprises a start time and an end time. 114

G. [Claim 5] The access device of claim 6 wherein the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the end time. 114

H. [Claim 9] The access device of claim 1 wherein the processor is configured to verify that the current reservation certificate is genuine. 115

I. [Claim 10] The access device of claim 1 further comprising: an identification to which the processor has access, the identification corresponding to one of the access device and the door lock, wherein the processor is configured to determine that

the current reservation certificate comprises data representative of the identification. 116

J. [Claim 12] The access device of claim 1 wherein the processor has access to a server of the access system through the communication module and the processor is configured to report to the server that the door lock was activated on the basis of the reservation certificate. 116

K. Claim 13 119

1. [13p] "A method for use by an access device in an access control system, the method comprising:" 119

2. [13A] "accepting, by a processor" 120

3. [13B] "through a communication module, a reservation certificate… presented with a portable terminal;" 120

4. [13C] "a reservation certificate that comprises an interval of a reservation" 120

5. [13D] "determining, by the processor, that the reservation certificate presented by the portable terminal is current by comparing the interval of the reservation to a current time accessible to the processor and determining that the current time is within the interval of the reservation; and activating, by the processor on the basis of the reservation certificate being current" 120

6. [13E] "activating… a door lock to allow the portable terminal to unlock the door lock during the interval of the reservation." 121

L. [Claim 14] The method of claim 13 wherein determining that the current time is within the interval of the reservation comprises determining that the current time is within a start time of the interval of the reservation and a predetermined duration and wherein the certificate is current from the start time up to the predetermined duration. 121

M. [Claim 15] The method of claim 14 wherein the predetermined duration is all day. 122

N. [Claim 16] The method of claim 13 wherein the interval of the reservation of the reservation certificate further comprises a start time and a duration and the reservation certificate is current from the start time up to the duration. 122

O. [Claim 17] The method of claim 18 wherein the reservation certificate is current from the start time up to the end time. 122

P. [Claim 18] The method of claim 13 wherein the interval of the reservation comprises a start time and an end time. 123

Q. [Claim 21] The method of claim 13 wherein the b) determining by the processor is further that the reservation certificate is genuine, and the c) activating is on the further basis of the reservation certificate being genuine. 123

R. [Claim 22] The method of claim 13 wherein the processor has access to an identification, the identification corresponding to one of the access device and the door lock, wherein the b) determining by the processor is further that the reservation certificate comprises data representative of the identification, and the c) activating is on the further basis of the reservation certificate comprising data representative of the identification. 124

S. [Claim 24] The method of claim 13 wherein the processor has access to a server through the communication module, the method further comprising the step of: d) reporting to the server that the door lock was activated on the basis of the reservation certificate. 125

XIV. GROUND 5: CLAIMS 7, 8, 11, 19, 20, AND 23 ARE UNPATENTABLE OVER *ELFSTRÖM* IN VIEW OF *WOODARD* AND *DEBRY* 126

A. Motivation to Combine *Elfström*, *Woodard*, and *DeBry* 126

B. Claim 7 128

1. [7A] The access device of claim 1 further comprising: a memory to which the processor has access, the memory is configured to comprise a public key for a server of the access system configured to issue the current reservation certificate;.....128

2. [7B] wherein at least a portion of the current reservation certificate is encrypted by the server using a private key and the processor is configured to verify that the current reservation certificate is genuine by decrypting the portion with the public key. 130

C. Claim 8 131

1. [8A] The access device of claim 1 further comprising: a memory to which the processor has access, the memory is configured to comprise a symmetric key: 131

2. [8B] wherein at least a portion of the current reservation certificate is encrypted by a server of the access system configured to use the symmetric key and the processor is configured to verify that the current reservation certificate is genuine by decrypting the portion with the symmetric key. 133

D. Claim 11 135

1. [11A] The access device of claim 1 further comprising: a memory to which the processor has access, the memory is configured to comprise a private key of the access device; 135

2. [11B] wherein at least a portion of the current reservation certificate is encrypted by a server of the access system configured to use a corresponding public key for the access device and the processor is configured to decrypt the portion with the private key. 136

E. [Claim 19] The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a

private key for which the corresponding public key is stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the public key, and the c) activating is on the further basis of the reservation certificate being genuine.....137

F. [Claim 20] The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a symmetric key stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the symmetric key, and the c) activating is on the further basis of the reservation certificate being genuine. 138

G. [Claim 23] The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a public key for which the corresponding private key is stored in a memory accessible to the processor, the method further comprising the step of: d) decrypting the portion, by the processor, with the private key.....139

XV. GROUND 6: CLAIMS 3 AND 15 ARE RENDERED OBVIOUS BY *ELFSTRÖM* IN VIEW OF *WOODARD* AND *MICALI* 139

A. Motivation to Combine *Elfström*, *Woodard*, and *Micali* 139

B. [Claim 3] The access device of claim 2 wherein the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation from the start time up to the predetermined duration that i all day. 140

C. [Claim 15] The method of claim 14 wherein the predetermined duration is all day. 143

XVI. CONCLUSION.....143

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 1-24 of U.S. Patent No. 9,373,205 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 the 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. *In Proceedings of Eleventh International Conference on Pattern Recognition*, IEEE Press, 58-61.
Appx. 2	Pocket PhotoMesa: A Zoomable Image Browser for PDAs. *In Proceedings of Mobile and Ubiquitous Multimedia (MUM 2004)* ACM Press, 19-24.
Appx. 3	SlideBar: Analysis of a Linear Input Device. *Journal of Behaviour and Information Technology*, London, Taylor & Francis, 23 (1), 1-9.
Appx. 4	Multi-Modal Text Entry and Selection on Mobile Devices, *Proceedings of* Graphics Interface (GI 2010), 19-26.
Appx. 5	DateLens: A Fisheye Calendar Interface for PDAs, *Transactions on Computer-Human Interaction*, New York: ACM, 11 (1), 90-119.
Appx. 6	Understanding One Handed Use of Mobile Devices. Lumsden, Jo (Ed.), *Handbook of Research on User Interface Design and Evaluation for Mobile Technology*, Idea Group Reference, 86-101.
Appx. 7	Audio Augmented Reality: A Prototype Automated Tour Guide. In Proceedings of Human Factors in Computing Systems (CHI 95) 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 ’205 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 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. Last year, I cofounded the J.S. Bryant School to open its doors in 2025. I was also cofounder 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 cofounder 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 cofounder and prior Chief Technology Officer of Hazel Analytics, a data analytics company that aims to improve food safety and better public health, whose product sends alerts in warranted circumstances. In addition, I have, for more than twenty-five 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 thirty 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 No. 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.

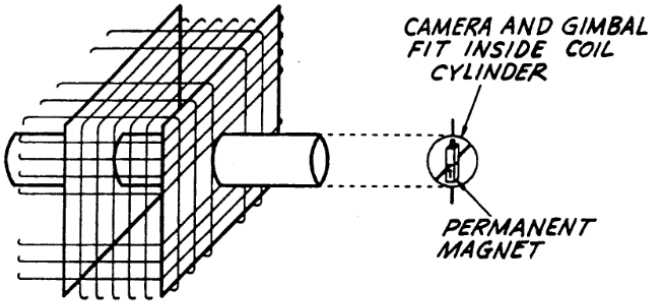


FIG 5

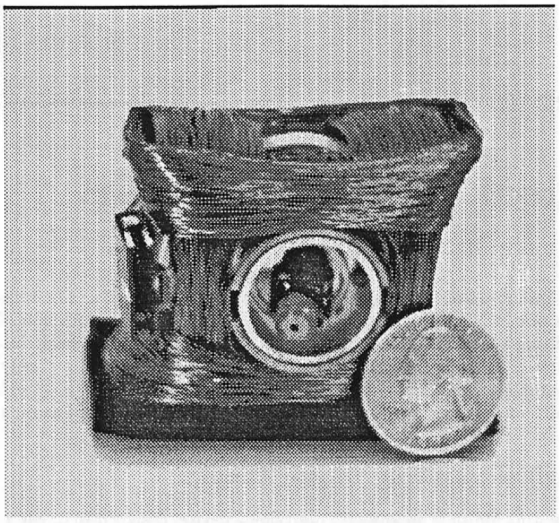


Figure 4.1: The Spherical Pointing Motor. At the center is a miniature camera consisting of a single CCD sensor chip and a lens assembly that fits on the rotor of this motor.

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 to 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.

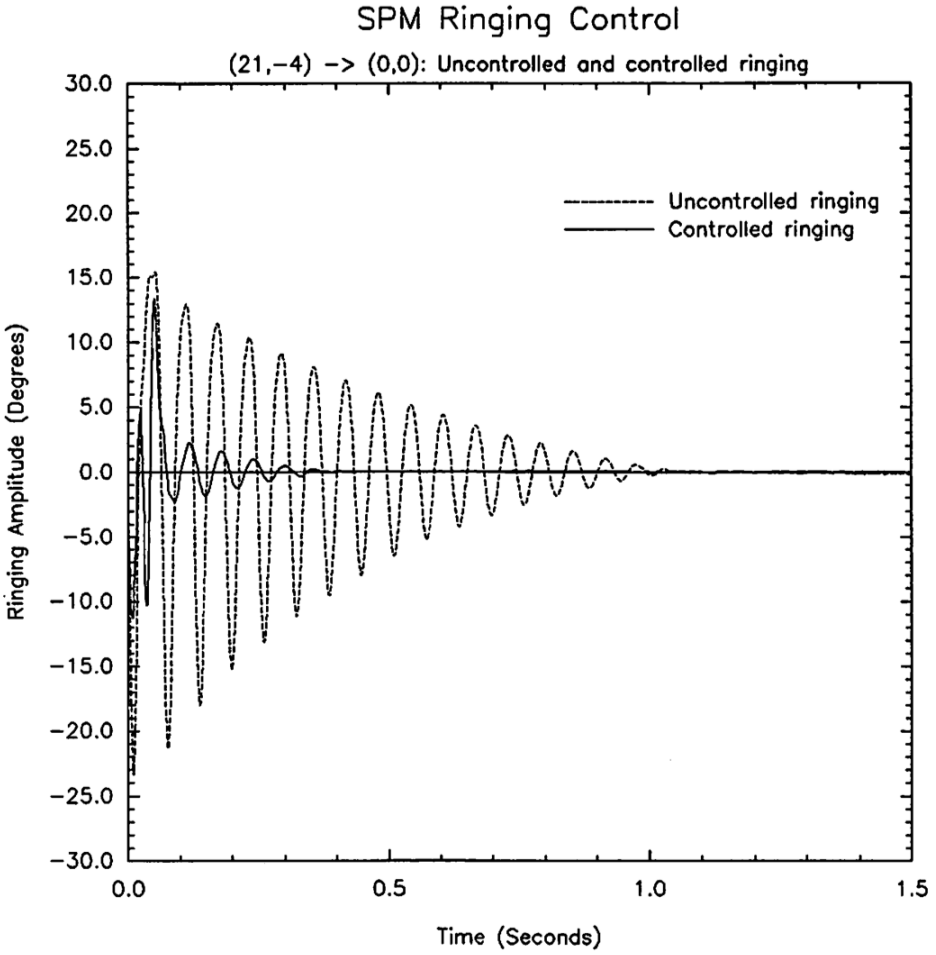


Figure 4.14: Measurement of two-step open-loop control strategy to reduce SPM ringing. Results are shown for the same movement of 21.4° with and without control. The motor currents are changed to hold the motor at the final position when the motor is expected to have zero velocity. Because the midpoint 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, when a person wearing the receiver walked around, the microcontroller they were carrying would identify the code from the transmitter they were standing under.

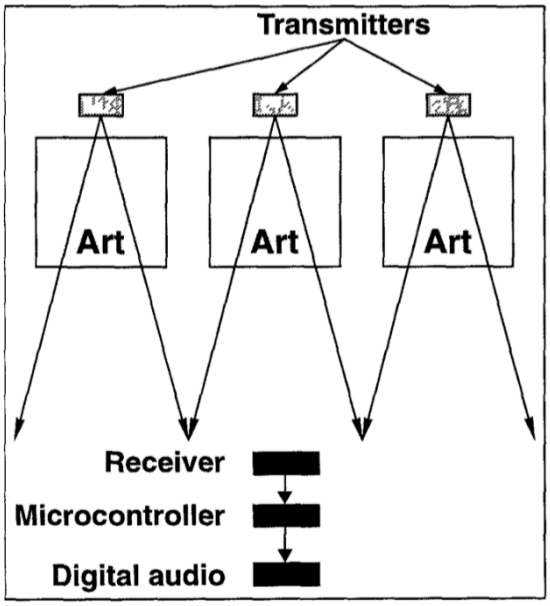


Figure 1: Schematic of automated tour guide prototype.

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 for 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 cofounding 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.

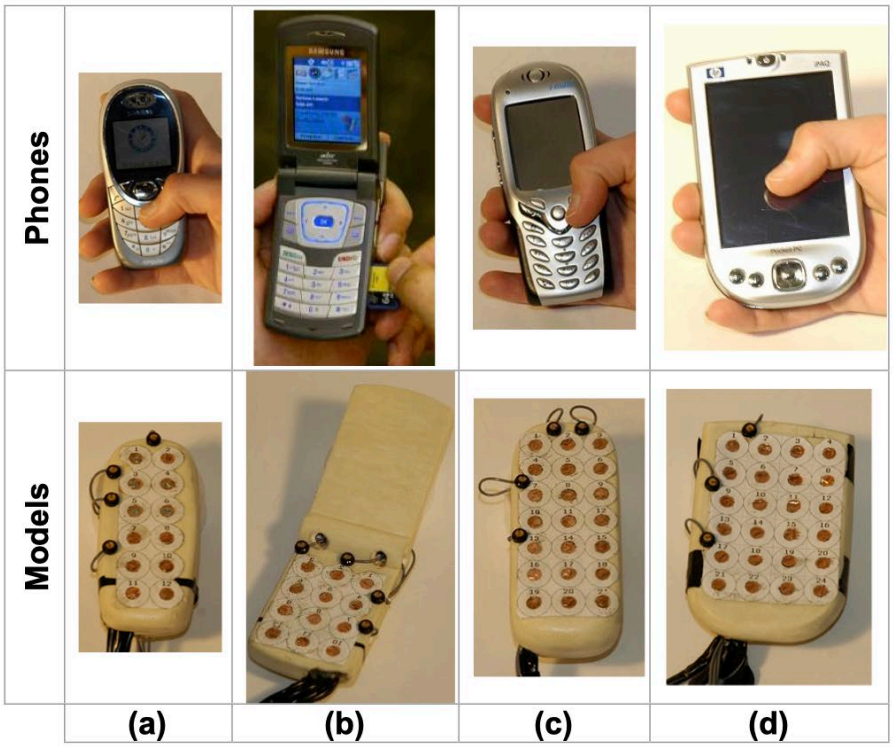


Figure 4. Devices we chose to represent a range of sizes and forms (top row) together with their study-ready models (bottom row): (a) SMALL, (b) FLIP, (c) LARGE, and (d) PDA.

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 a 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://ieeevis.org/year/2021/info/awards/test-of-time-awards; https://ieeevis.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. 9,373,205 ("the '205 patent")
Ex-1002	Prosecution File History of U.S. Patent No. 9,373,205
Ex-1004	Curriculum Vitae of Benjamin B. Bederson
Ex-1005	WO 2008/076074 A1 to Knutsson et al. ("*Knutsson*")
Ex-1006	U.S. Patent No. 8,730,004 B2 to Elfström et al. ("*Elfström*")
Ex-1007	U.S. Patent No. 6,385,728 B1 to DeBry ("*DeBry*")
Ex-1008	U.S. Patent Publication No. 2009/0219133 A1 to Woodard et al. ("*Woodard*")
Ex-1009	U.S. Patent No. 7,353,396 B2 to Micali et al. ("*Micali*")

Ex-1010	Reexamination File History of U.S. Patent No. 9,373,205
Ex-1011	U.S. Patent No. 8,412,837 B1 to Emigh et al.
Ex-1012	U.S. Patent No. 5,794,207 A to Walker et al.
Ex-1014	U.S. Patent Publication No. 2010/0293011 A1 to Lebreton 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 ’205 patent at the time of the alleged invention. For the 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 ’205 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 ’205 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 '205 PATENT

32. The '205 patent describes a smart phone or terminal to activate a door lock using a web site or server, and that a door lock receives a reservation certificate presented by the terminal through a communication module. Ex-1001, Abstract. The first independent claim, claim 1 of the '205 patent, is listed below:

	Claim Limitation
1p	An access device for use in an access control system, the access device comprising:
1A	**a processor (16) having control of a door lock (11); and**[2]
1B	**a communication module (17) connected to the processor, the processor is configured to receive a reservation certificate (5) presented by a portable terminal (4) through the communication module;**
1C	**wherein, when a current reservation certificate that comprises an interval of a reservation is presented by the portable terminal,**
1D	**the processor is configured to compare the interval of the reservation of the current reservation certificate to a current time accessible to the processor, determine the current time is within the interval of the reservation, and**
1E	**activate the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation.**

[2] All colors have been added herein unless otherwise noted.

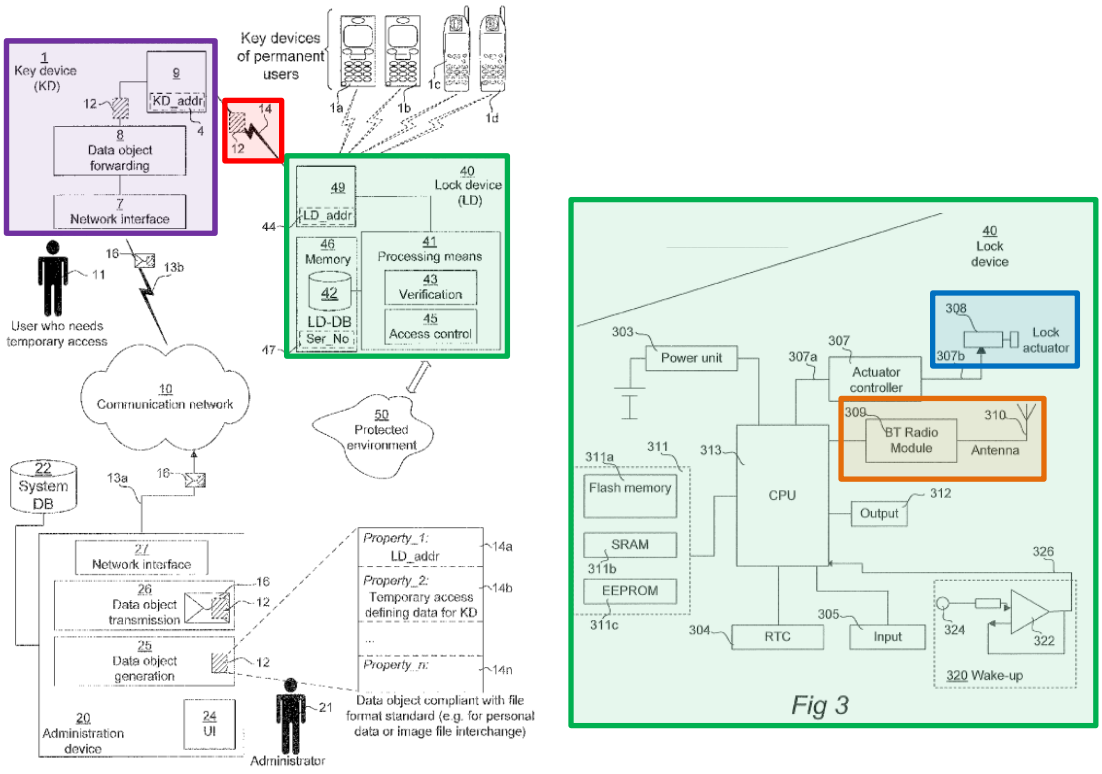
33. *Knutsson* and *Elfström* each disclose processors with communication modules configured to receive a reservation certification from a PDA or mobile phone, determine whether the reservation certificate is current, and activate the door lock if it is, like those claimed by the '205 patent.

VI. OVERVIEW OF PRIOR ART

A. *Knutsson*

34. Counsel has informed me WO Publication WO2008/076074 (Ex-1005, "*Knutsson*"), published on June 26, 2008, and filed as International Application No. PCT/SE2007/051042, filed on December 19, 2007, is prior art.

35. *Knutsson* discloses "[a]n access control system uses an existing file format standard, e.g. for personal data interchange (PDI) or image file interchange, for novel access control purposes to provide temporary access" and this applies "for a wireless key device to a lock device." *Knutsson*, Abstract. *Knutsson* discloses its "lock device 40 will be integrated with or coupled to a lock mechanism in the lockable door or garage port and in particular have a controllable lock actuator configured to unlock the lock mechanism upon detection and successful authorization of the key device 1." *Id.*, 10:24-30. Further, *Knutsson* discloses its "lock device 40 has a Bluetooth® radio module 309 with an antenna 310." *Id.*, 17:18-19.



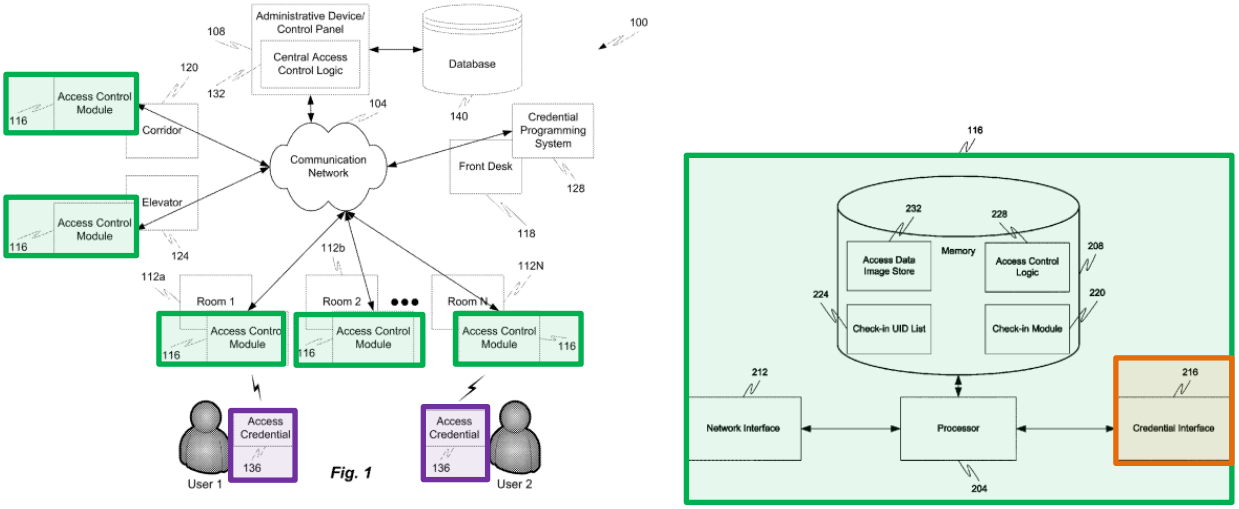
Id., FIGS. 1, 3 (annotated).

B. *Elfström*

36. Counsel has informed me U.S. Patent No. 8,730,004 B2 to Elfström et al., ("*Elfström*"), filed no later than January 29, 2010, is prior art.

37. *Elfström* discloses, "[t]o facilitate such security policies, the access control modules 116 may be adapted to communicate with access credentials 136 carried by users or guests of the multi-room facility via contactless and/or contact-based communication protocols." *Elfström*, 4:58-62. *Elfström* discloses, "[c]onnected to the communication interface 216 is a controller or processor 204."

Id., 5:60-61. *Elfström* discloses, "[t]he processor 204 is enabled to communicate with the access control device … includ[ing], without limitation, an electronic lock, a magnetic lock, or an electric strike for a door." *Id.*, 6:9-16. *Elfström* discloses, "the access data encoded on the credential 136 may include … stay duration (identifying either a departure date or an expiration date for the access data)." *Id.*, 12:29-36.



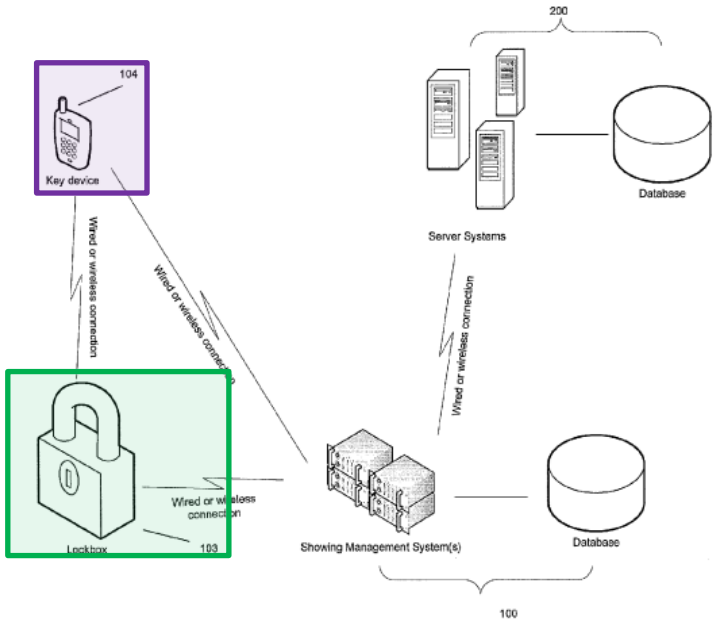
Id., FIGS. 1, 2 (annotated).

C. *Woodard*

38. Counsel has informed me that U.S. Publication No. 2009/0219133 A1 to Woodard et al., ("*Woodard*"), filed no later than February 28, 2008, and published no later than September 3, 2009, is prior art.

39. *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).

D. *DeBry*

40. Counsel has informed me that U.S. Patent No. 6,385,728 B1 to DeBry ("*DeBry*"), filed no later than November 26, 1997, and issued on May 7, 2002, is prior art.

41. *DeBry* discloses, "[p]ublic key cryptography is based on two keys, a private key and a public key, that work together …. Messages encrypted with a person's public key can only be decrypted with that person's private key." *DeBry*, 2:36-44. *DeBry* discloses two different systems of decryption. *DeBry* discloses a first system where "the message is first encrypted by the sender using the sender's private key, and decrypted by the recipient using the sender's public key." *DeBry*, 3:16-19. *DeBry* also discloses a second system where "[i]n a public key system, it is possible to communicate privately without transmitting any secret key." *Id.*, 2:46-49. *DeBry* discloses, "[a]nyone desiring to communicate in private with a recipient merely encrypts the message under the recipient's public key. Only the recipient, who retains the secret decrypting key, is able to decipher the transmitted message." *Id.*, 2:49-53.

E. *Micali*

42. Counsel has informed me that U.S. Patent No. 7,353,396 B2 to Micali et al., ("*Micali*"), filed no later than April 8, 2003, and issued on April 1, 2008, is prior art.

43. *Micali* discloses, "controlling physical access through a digital certificate validation process that works with standard certificate formats (e.g., X.509v3) and that enables a certifying authority (CA) to prove the validity status of each certificate C at any time interval (e.g., every day, hour, or minute) starting with C's issue date, D_1." *Micali*, 15:57-62.

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 '205 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 POSA at the time of the purported invention would have had a Bachelor of Science degree in Computer Science or an equivalent field, with at least two years of academic or industry experience with wireless systems or comparable experience. Additional education could substitute for professional experience and vice versa.

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 ’205 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 1-24 of the '205 patent are rendered obvious under the following grounds:

Ground	Reference(s)	Claims
1	*Knutsson*	1-6, 8-10, 13-18, 20-22
2	*Knutsson*, *DeBry*	7, 11, 19, 23
3	*Knutsson*, *Woodard*	12, 24
4	*Elfström*, *Woodard*	1-6, 9-14, 16-18, 21-22, 24
5	*Elfström*, *Woodard*, *DeBry*	7, 8, 11, 19, 20, 23
6	*Elfström*, *Woodard*, *Micali*	3, 15

51. The claims recite a phone or portable terminal to activate a door lock using a web site or server, and that a door lock receives a reservation certificate presented by the terminal through a communication module. Ex-1001, Abstract. As shown below, the certificate includes a start time. *Id.*, 5:14-15. The '205 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.*, 8:19-25.

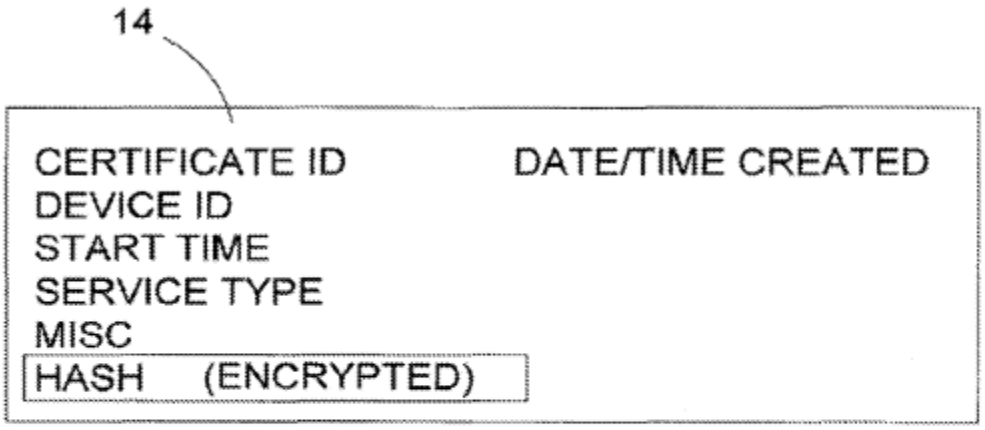


FIG. 2

Id., FIG. 2.

52. Access credentials or a reservation certificate used by a phone to unlock a door were known before March 2, 2010, the earliest-claimed priority date of the '205 patent, as discussed below.

A. The *Knutsson* Grounds (Grounds 1-3)

53. *Knutsson* discloses or renders obvious all limitations of the independent claims and many of the dependent claims of the '205 patent (**Ground 1**). *Knutsson* discloses, "[a]n access control system uses an existing file format standard, e.g. for personal data interchange (PDI) or image file interchange, for novel access control

purposes to provide temporary access for a wireless key device to a lock device." *Knutsson*, Abstract. *Knutsson* discloses that its "lock device 40 will be integrated with or coupled to a lock mechanism in the lockable door or garage port and in particular have a controllable lock actuator configured to unlock the lock mechanism upon detection and successful authorization of the key device 1." *Id.*, 10:24-30. To accomplish this, *Knutsson*'s "lock device 40 has a Bluetooth® radio module 309 with an antenna 310." *Id.*, 17:18-19.

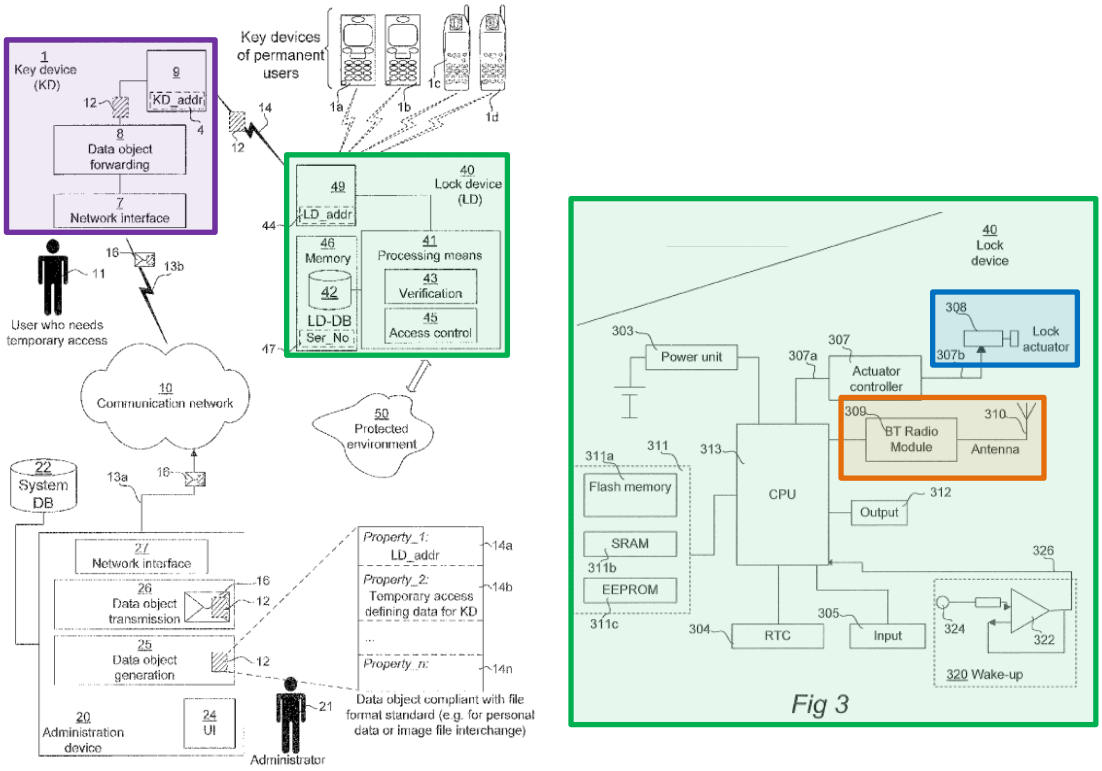


Fig 3

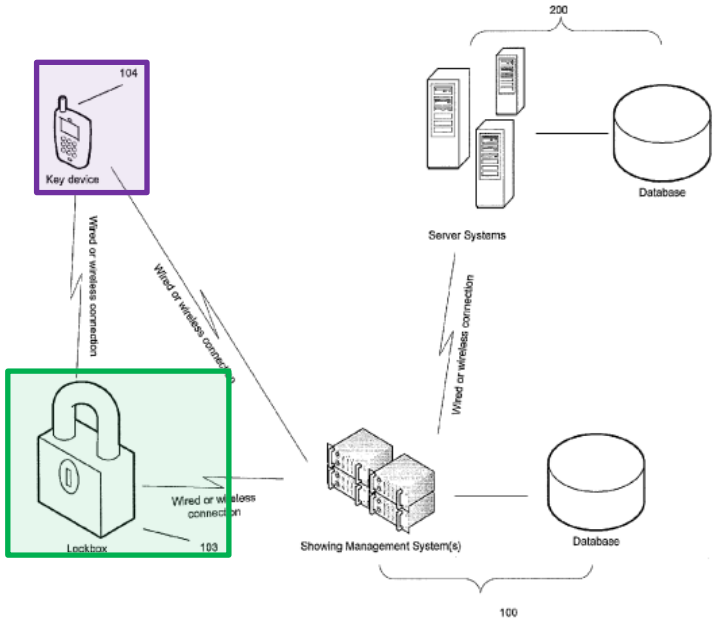
Id., FIGS. 1, 3 (annotated).

54. Certain dependent claims in the ’205 patent further require encryption methods (claims 7, 11, 19, and 23, **Ground 2**). Although *Knutsson* discloses use of encryption, it does not expressly disclose particular encryption methods with public-private key pairs, but *DeBry* does.

55. *DeBry* discloses, “[p]ublic key cryptography is based on two keys, a private key and a public key, that work together …. Messages encrypted with a person’s public key can only be decrypted with that person’s private key.” *DeBry*, 2:36-44. *DeBry* discloses, “the message is first encrypted by the sender using the sender’s private key, and decrypted by the recipient using the sender’s public key.” *Id.*, 3:16-19. *DeBry* also discloses, “[i]n a public key system, it is possible to communicate privately without transmitting any secret key.” *Id.*, 2:46-49. *DeBry* discloses, “[a]nyone desiring to communicate in private with a recipient merely encrypts the message under the recipient’s public key. Only the recipient, who retains the secret decrypting key, is able to decipher the transmitted message.” *Id.*, 2:49-53.

56. Certain dependent claims in the ’205 patent further require the processor to report to the server that the door lock was activated on the basis of the reservation certificate (claims 12 and 24, **Ground 3**). *Knutsson* does not expressly disclose reporting activation to the server, but *Woodard* does.

57. *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).

B. The *Elfström* Grounds (Grounds 4-6)

58. *Elfström*, like *Knutsson*, discloses the majority of features of the '205 patent's claims. *Elfström* discloses "[t]o facilitate such security policies, the access control modules 116 may be adapted to communicate with access credentials 136 carried by users or guests of the multi-room facility via contactless and/or contact-based communication protocols." *Elfström*, 4:58-62. Access control module 116 includes "processor 204 [that] controls and determines how the access control module 116 behaves when a credential 136 is presented." *Id.*, 5:66-6:1. "Connected to the communication interface 216 is a controller or processor 204." *Id.*, 5:60-61. *Elfström* discloses "[t]he processor 204 is enabled to communicate with the access

control device … includ[ing], without limitation, an electronic lock, a magnetic lock, or an electric strike for a door." *Id.*, 6:9-16. *Elfström* discloses "the access data encoded on the credential 136 may include … stay duration (identifying either a departure date or an expiration date for the access data)." *Id.*, 12:29-36.

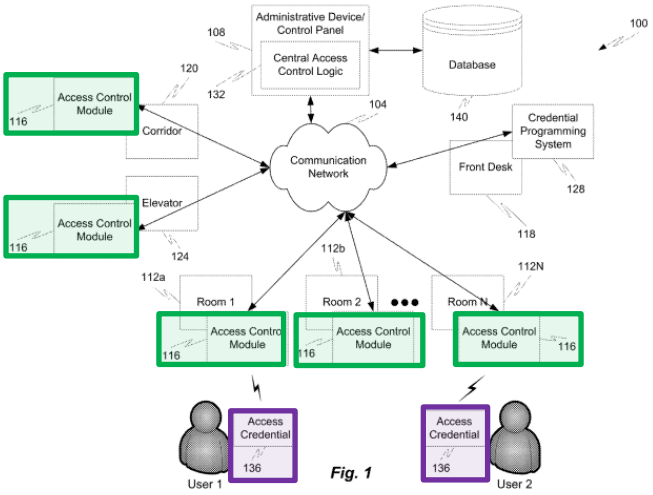
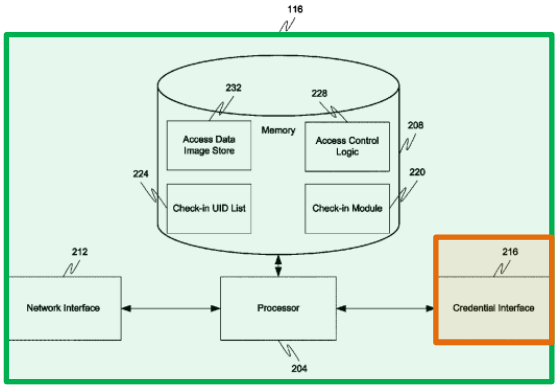


Fig. 1



Id., FIGS. 1, 2 (annotated).

59. For the independent claims of the '205 patent (**Ground 4**), *Elfström* does not expressly disclose the reservation timing limitations, like comparing the interval of the reservation of the current reservation certificate to a current time accessible to the processor, determining that the current time is within the interval of the reservation, and activating the door lock during the reservation interval. But *Woodard* does.

60. Addressing these limitations, *Woodard* discloses "automatically controlling access to an electronic lockbox utilizing showing appointment data maintained by a central showing management system." *Woodard*, [0010]. And, *Woodard* discloses "provid[ing] automatic access control to an electronic real estate lockbox utilizing showing appointment data maintained by a showing management system, whereby the showing appointment data is transmitted directly to the electronic lockbox and/or an electronic key device." *Id.*, [0012]. As part of the automatic access, *Woodard* discloses "[t]he electronic lockbox 103 will open only when the actual access time is within the scheduled showing appointment time." *Id.*, [0048].

61. Similar to the *Knutsson* Grounds, certain dependent claims in the '205 patent further require encryption methods (claims 7, 8, 11, 19, 20, and 23, **Ground 5**). *Elfström* does not expressly disclose particular encryption methods, but *DeBry* does, as explained for the *Knutsson* Grounds above. *DeBry* discloses "symmetric cryptography" and "public key cryptography" that includes "two keys, a private key and a public key, that work together." *DeBry*, 1:62-2:10, 2:27-53.

62. Certain dependent claims in the '205 patent further require the reservation certificate to be valid for an interval of a predetermined duration that is all day (claims 3 and 15, **Ground 6**). To the extent it is argued that the

Elfström-Woodard combination does not expressly disclose a duration interval that is all day, *Micali* does. *Micali* discloses "controlling physical access through a digital certificate validation process that works with standard certificate formats (e.g., X.509v3) and that enables a certifying authority (CA) to prove the validity status of each certificate C at any time interval (e.g., every day, hour, or minute) starting with C's issue date, D_1." *Micali*, 15:57-62. *Micali* provides a specific example where "every morning—e.g., at midnight—a wireless user may receive a 20-byte proof of the validity of his certificate for the remainder of the day." *Id.*, 18:17-19.

63. Accordingly, because the challenged claims of the '205 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 1-6, 8-10, 13-18, AND 20-22 ARE RENDERED OBVIOUS BY *KNUTSSON*

A. Claim 1

64. *Knutsson* renders obvious claim 1.

1. [1p] "An access device for use in an access control system, the access device comprising:"

65. *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.

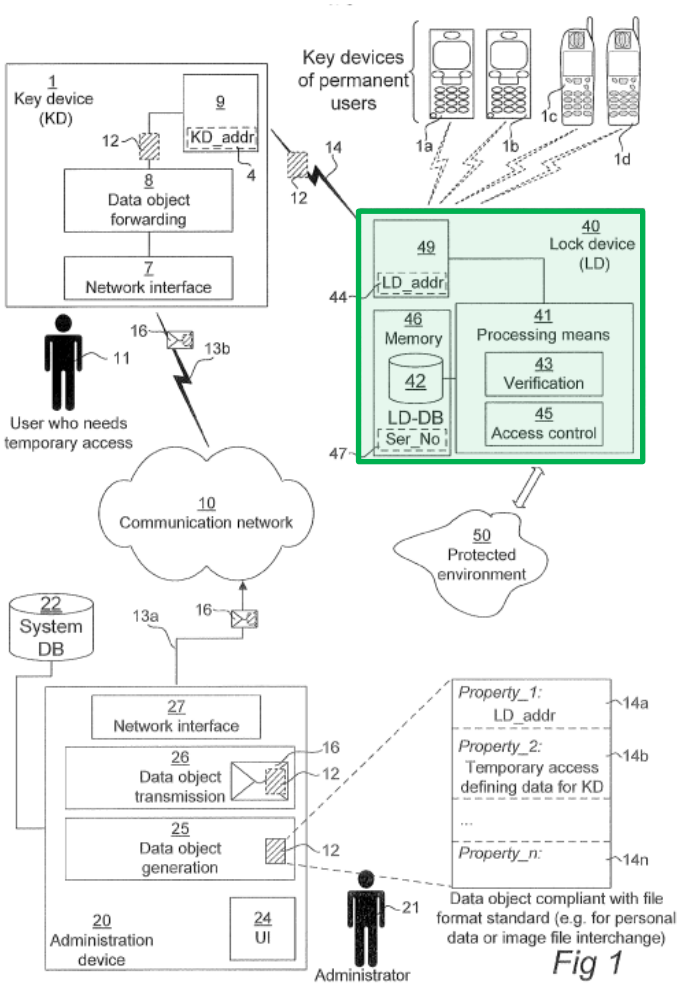


Fig 1

Id., FIG. 1 (annotated).

2. [1A] "a processor (16) having control of a door lock (11); and"

66. *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*, 16:6-8, 17:11-13, 20:7-11. "CPU" is a commonly used term meaning

"central processing unit," which is a processor executing various application programs and an Operating System.

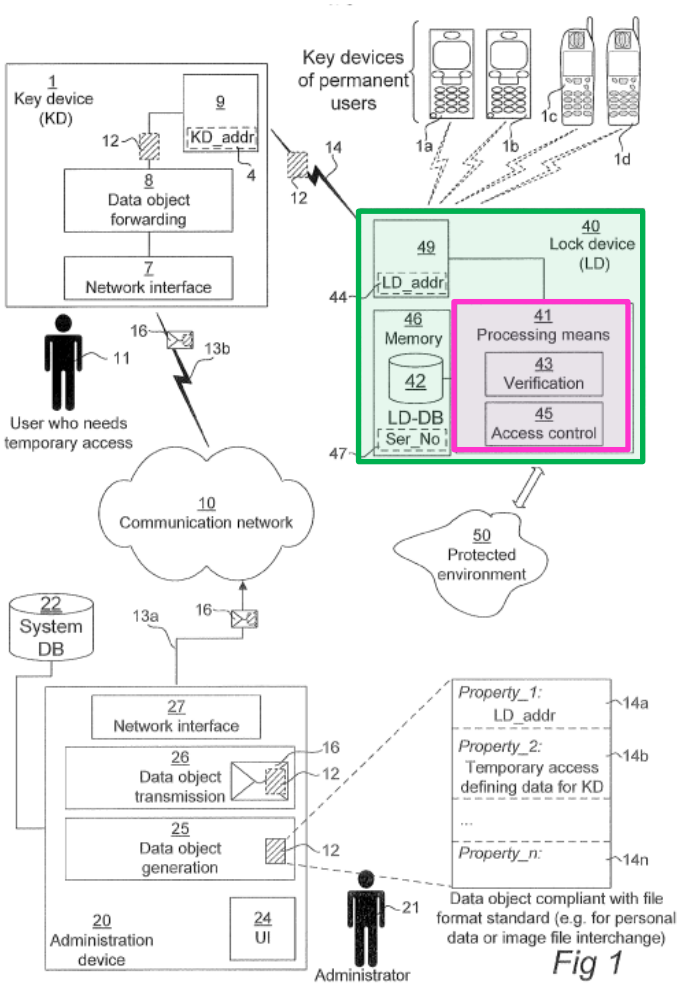
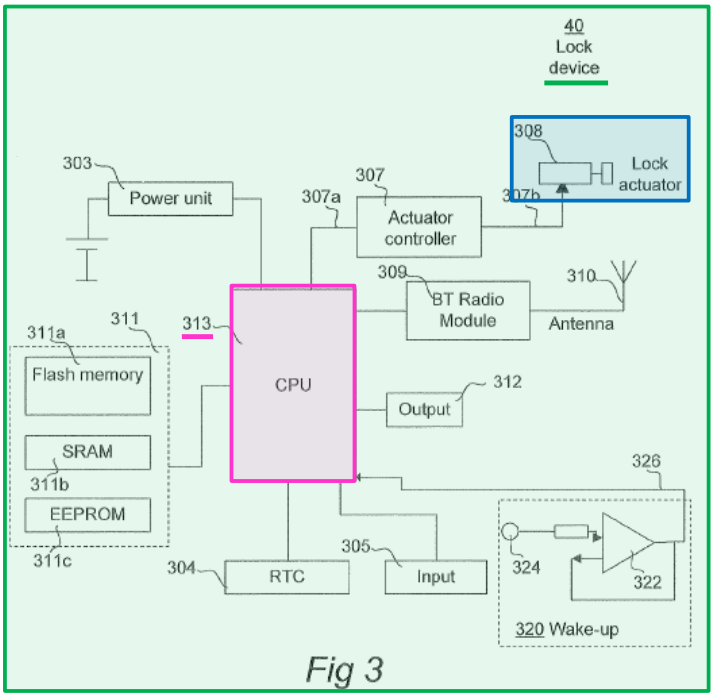


Fig 1

Id., FIG. 1 (annotated).

67. *Knutsson*'s "Fig 3 is a schematic block diagram illustrating internal components and modules of a lock device." *Id.*, 9:31-32.



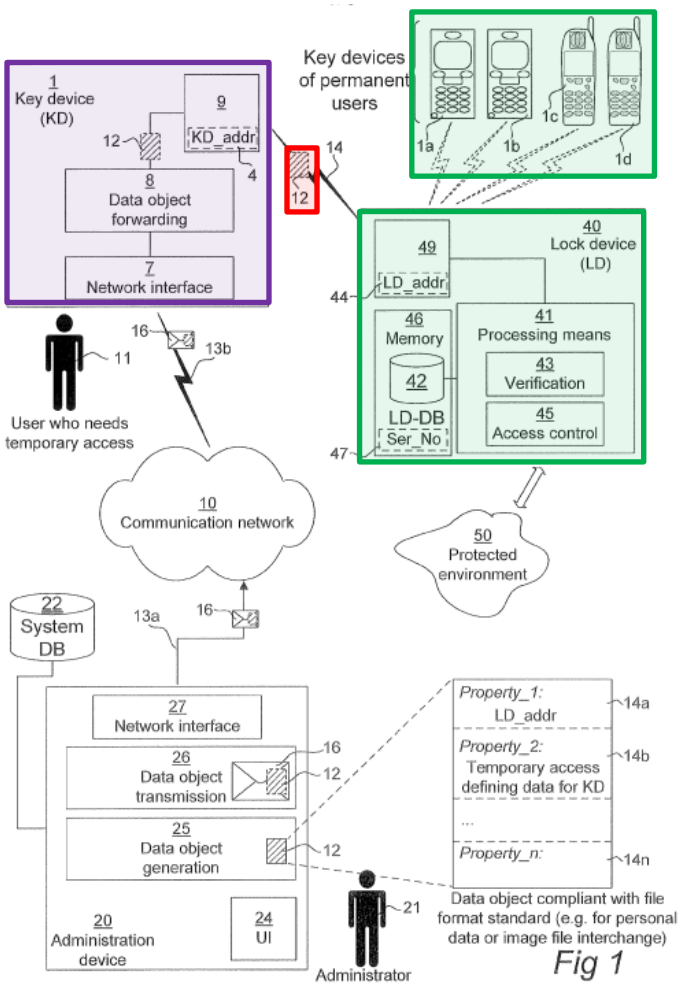
Id., FIG. 3 (annotated).

68. *Knutsson*'s "CPU [313] may be identical to the aforementioned processing means 41" as discussed above and shown with reference to FIG. 1. *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 when "CPU 313 … generates the control signal 307a to the actuator controller 307 … **this will cause unlocking of the lock**, etc, and allow opening of the door, etc, to the protected environment." *Id.*, 20:7-11.

3. [1B] "a communication module (17) connected to the processor, the processor is configured to receive a reservation certificate (5) presented by a portable terminal (4) through the communication module;"

69. *Knutsson* renders obvious [1B] because *Knutsson* discloses a key device such as a mobile phone (portable terminal) that sends access defining data in the form of a vCard data object (reservation certificate) to the lock device's short-range wireless data communications means, such as a Bluetooth radio module (communication module) coupled to its CPU 313 (processor).

70. *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. A data object 12 is created and assigned the temporary access data. *Id.*, 11:32-33. *Knutsson* discloses "[t]he key device [] 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. FIG. 1 is shown below.



Id., FIG. 1 (annotated).

71. *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.*, 4:32-5:4. *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 that it references and discusses, WO Publication 2006/098690, that, like *Knutsson*, discloses 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.

72. *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** …. This necessary data includes a communication identifier ('LD_addr' in 35 Fig 1) of the lock device 40." *Id.*, 11:32-12:1 (emphases 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. The structure of data object 12 is shown below in FIGS. 4a-4b, showing temporary access data that it includes.

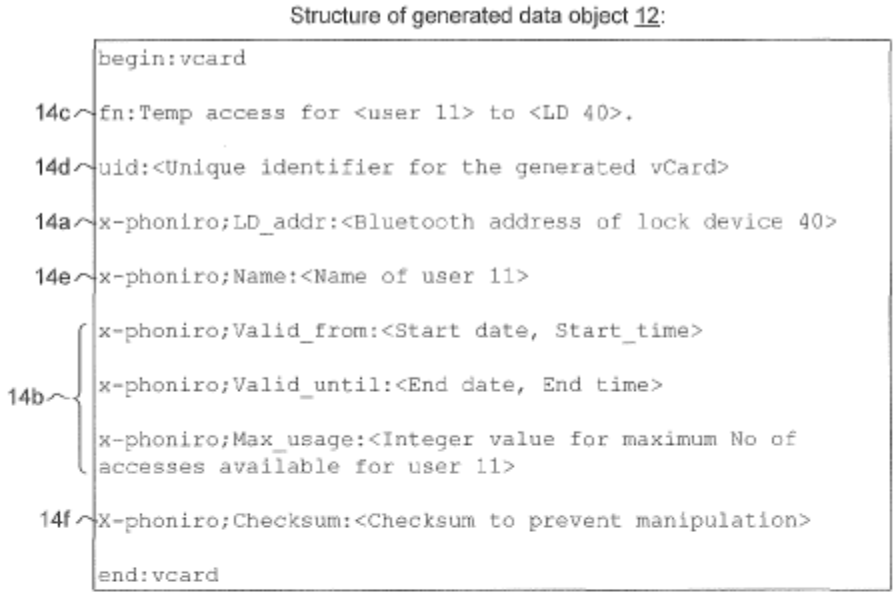


Fig 4a

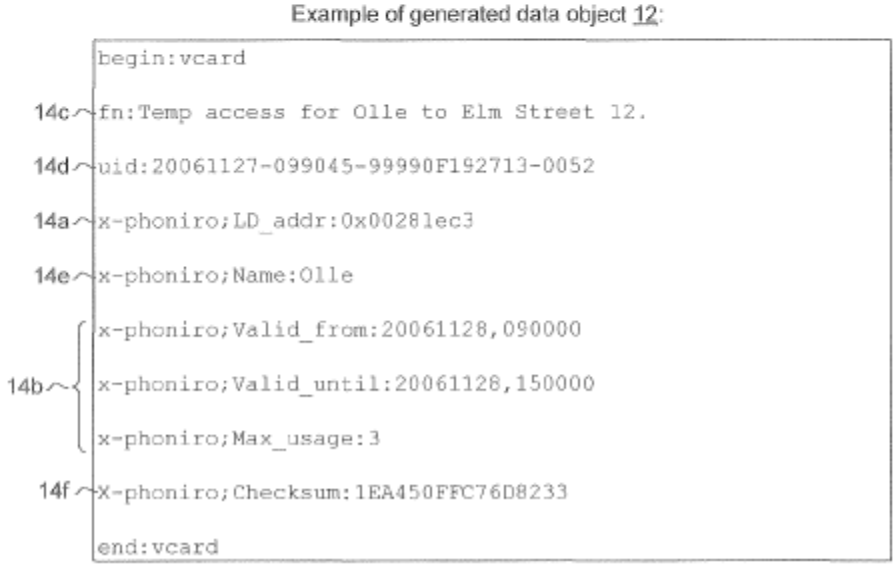
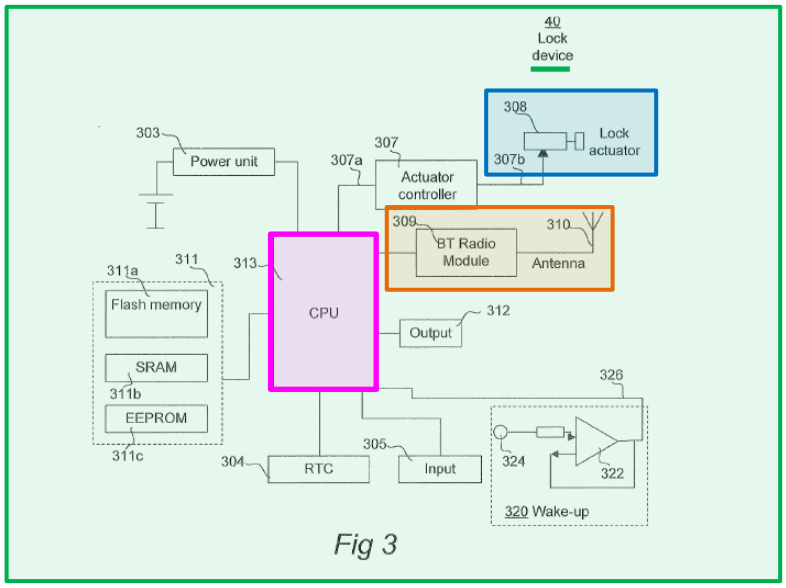


Fig 4b

Id., FIGS. 4A-4B.

73. For another limitation of [1B], *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 its "lock device 40 has short-range wireless data communication means 49 in the form of a Bluetooth® transceiver." *Id.*, 12:3-7. *Knutsson* provides further explanation, disclosing its "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. As shown below, CPU 313 is connected to the Bluetooth® radio module 309.



Id., FIG. 3 (annotated).

74. Using the above-discussed communications and communications means, *Knutsson* discloses "**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, FIGS. 1, 5C.

4. [1C] "wherein, when a current reservation certificate that comprises an interval of a reservation is presented by the portable terminal,"

75. *Knutsson* renders obvious [1C] because *Knutsson*'s data object 12 (reservation certificate) 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 [or] more dates and/or times which define start and end points for permitted temporary access." *Knutsson*, 6:1-6, 11:32-12:1, FIG. 6 at block 628, FIG. 5 at block 538.

76. Figures 4a-4b show that "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.

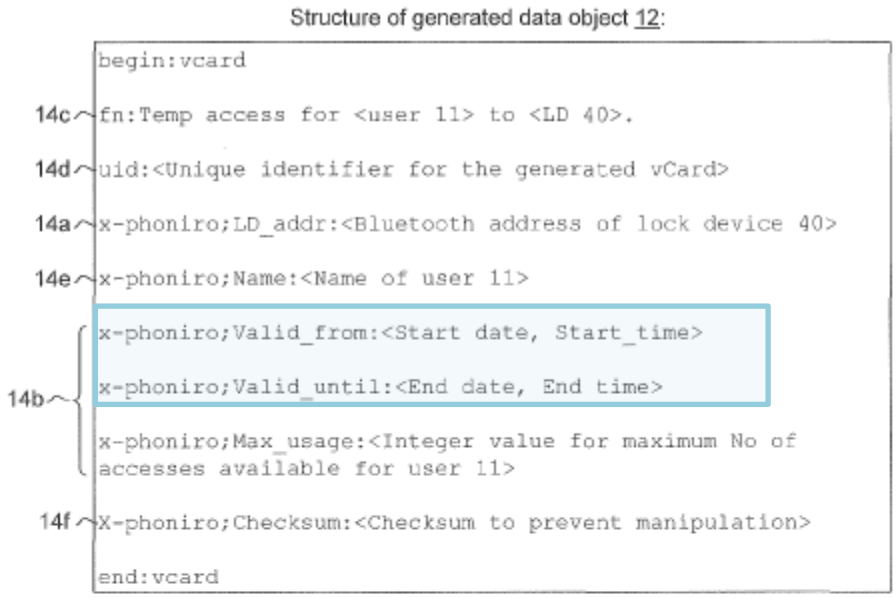


Fig 4a



Fig 4b

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

77. Based on my experience, 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). *Id.*, 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. Using similar language, *Knutsson* refers to this period as a "time-slot." *Id.*, 20:7, 20:12-15. The duration can be calculated by subtracting the start time from the end time, such that duration = end time - start time. This would have been obvious to a POSA because given any two of start time, end time, or duration, the third can be calculated using the simple, useful formula above. This is confirmed by *Knutsson*'s disclosure of "temporary" access, because *Knutsson* is disclosing access for a set time, time slot, or an interval. *Id.*, Abstract. *Knutsson* further confirms this by explaining that the lock device including CPU 313 determines whether the current time, which CPU 313 has access to, falls within the "stage-1 time slot," (*id.*, 17:21-22, 20:4-7), where the time slot corresponds to the claimed "interval." *Knutsson* even provides examples of time slots including "00-24," as in from 0000 to 2400 using military time, which would be 12:00 AM to 12:00 AM in 12-hour time, "2005-03-24: 19-22," as in March 24, 2005, from 1900 to 2200 (7:00 PM to 10:00 PM), and "Mon-Fri: 07-15," as in Monday through Friday, 0700 through 1500 (7:00 AM to 3:00 PM). *Knutsson*, Table 1, 18:16-19:16.

78. It is my further opinion that a POSA would have understood that *Knutsson*'s "temporary access" for a user of a wireless key device to "a room, apartment, commercial or public premises … with a controllable physical access interface in the form of a lockable door," satisfies the ordinary meaning of a "reservation." *Id.*, 10:18-24. The '205 patent discloses that a reservation allows control of "any access device such as a hotel room lock or the like," Ex-1001, 1:64-2:1, thus confirming that *Knutsson*'s disclosure of controlling a lockable door for a temporary amount of time or time slot corresponds to the claimed "reservation."

5. [1D] "the processor is configured to compare the interval of the reservation of the current reservation certificate to a current time accessible to the processor, determine the current time is within the interval of the reservation, and"

79. *Knutsson* renders obvious [1D] because *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, 20:2-3), 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 blocks 628-630.

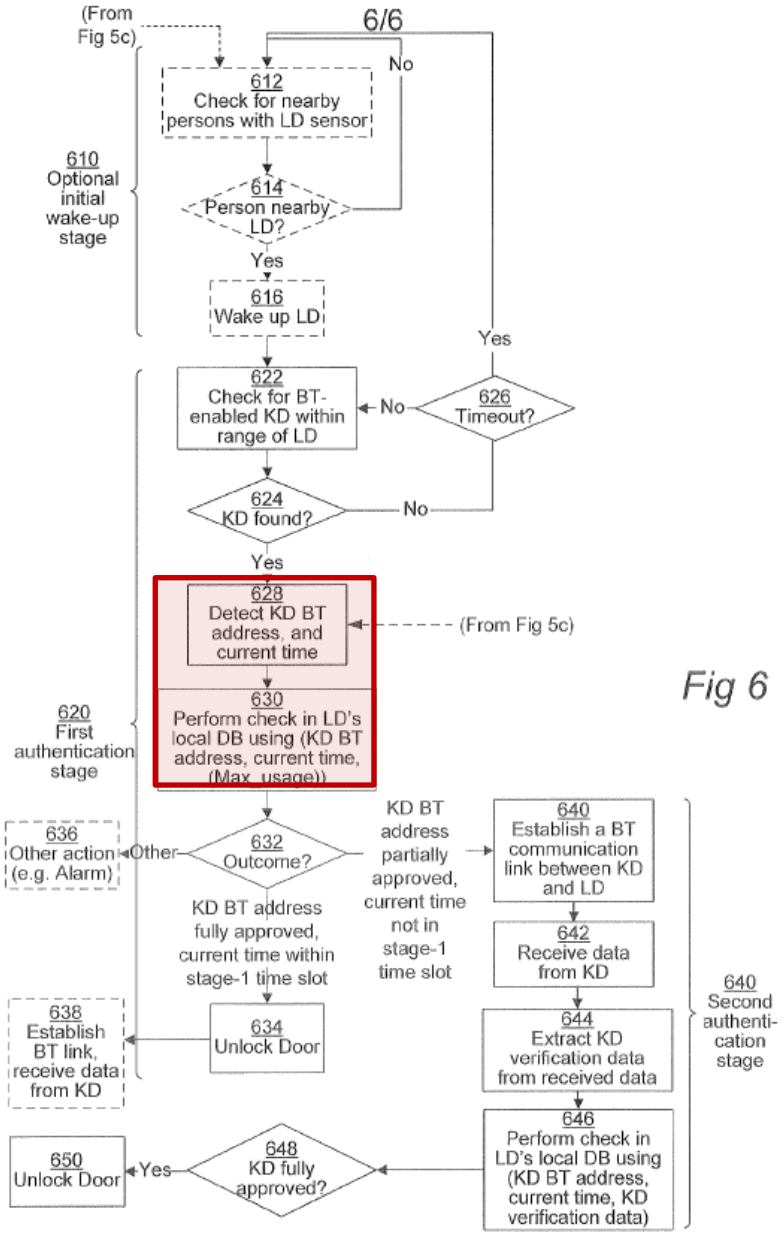


Fig 6

Id., FIG. 6 (annotated).

80. *Knutsson*'s stage-1 authentication step includes determining 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." *Id.*, 18:1-4. As shown in FIG. 6, step 630 includes performing a check using the current time and then granting authorization in step 632. *Id.*, FIG. 6 at blocks 632-634. Authorization therefore corresponds to determining the current time is in the time slot (interval) of the allowed temporary access (reservation). A structure that the lock device 40 uses to store authentication data is shown as a table of information, shown below.

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).

Thus, *Knutsson* discloses its object 12, including temporal data, would be used from the start time until the end time for temporary access, if that time slot included the "current time," (*id.*, 20:4-7), and thus the object 12 would be current during the time slot.

6. [1E] "activate the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation."

81. *Knutsson* renders obvious [1E] because *Knutsson*'s "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), "[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.

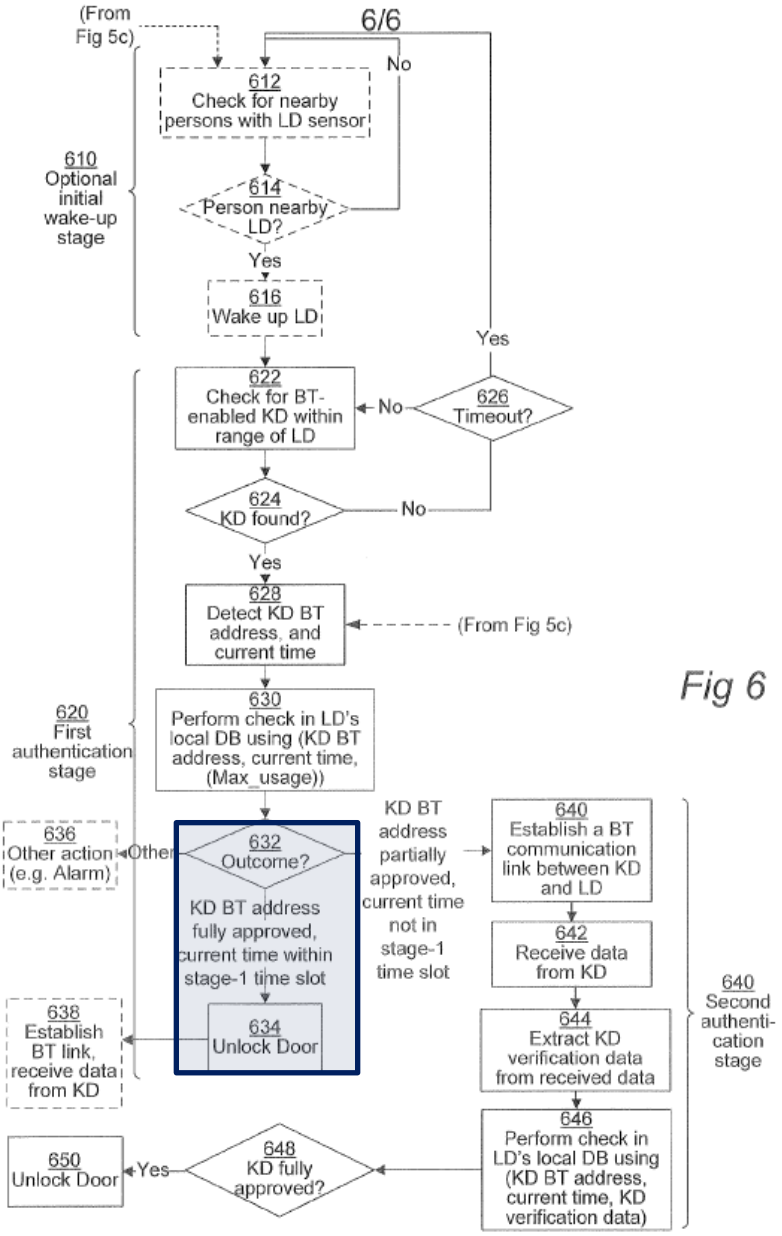


Fig 6

Id., FIG. 6 (annotated).

82. As explained in Section X.A.5 for [1D], *Knutsson* discloses, "the CPU 313 … [checks] whether the current time falls within any stage-1 time slot defined for that Bluetooth® address" and, upon determining that the current time falls within

a stage-1 time slot, actuates the lock mechanism (unlocks the door lock). *Id.*, 20:4-7, FIG. 6 at blocks 628-630.

B. Claim 2

1. [2A] The access device of claim 1 wherein the processor is configured to determine the current time is within the interval of the reservation by determining if the current time is within a start time of the interval of the reservation of the current reservation certificate and a predetermined duration and

83. *Knutsson* renders obvious [2A].

84. As explained in Sections X.A.5-6 for [1D-1E], *Knutsson* discloses, "the CPU 313 … [checks] whether the current time falls within any stage-1 time slot defined for that Bluetooth® address." *Knutsson*, 20:4-7, FIG. 6 at blocks 628-630. *Knutsson*'s temporal data may be "one [or] more dates and/or times which define start point ('Valid_from') and end point ('Valid_to') for the temporary access permitted." *Id.*, 12:24-26.

85. As explained in Section X.A.4 for [1C], based on my experience, a POSA would have understood that *Knutsson*'s disclosure of object 12 including both a start time and an end time of a temporary access renders obvious the claimed "interval" because an interval is defined by a starting point and an end point. Similarly, in my view, a POSA would have understood *Knutsson*'s disclosure of the object 12 including both a start time and an end time of a temporary access as

disclosing a "predetermined duration," because a POSA would have understood that a duration can be calculated by subtracting the start time from the end time. By providing start and end times, a duration is presented by *Knutsson*'s key device (portable terminal). This is confirmed by *Knutsson*'s disclosure of "temporary" access (*id.*, Abstract), because *Knutsson* is disclosing access for a set time, or a duration. *Knutsson* further confirms this by explaining that the lock device including CPU 313 determines "whether the current time falls within any stage-1 time slot," where a time slot is the claimed "predetermined duration." *Knutsson*, 20:4-7. Thus, *Knutsson* discloses its object 12 would be used from its disclosed start time to the end time, also an end of the duration, as compared to the "current time," (*Knutsson*, 20:4-7), and thus the object 12 would be current during the time slot.

2. [2B] is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the predetermined duration.

86. *Knutsson* renders obvious [2B].

87. As explained in Section X.A.5-X.A.6 for [1D-1E], *Knutsson* discloses, "the CPU 313 … [checks] whether the current time falls within any stage-1 time slot defined for that Bluetooth® address." *Knutsson*, 20:4-7, FIG. 6 at blocks 628-630. Based on my experience, a POSA would have understood that *Knutsson*'s processor uses a start time until the end time (predetermined duration) for granting temporary

access because *Knutsson*'s "stage-1 time slot" begins at the start time and ends at the end time. *Id.*

88. *Knutsson*'s temporal data may be "one [or] more dates and/or times which define start point ('Valid_from') and end point ('Valid_to') for the temporary access permitted." *Id.*, 12:24-26. If the outcome of checks of blocks 628-630 "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" that "will cause unlocking of the lock, etc, and allow opening of the door, etc, to the protected environment." *Id.*, 20:7-11. Thus, unlocking would happen when the current time falls within the time slot defined by the start and end points, as shown below.

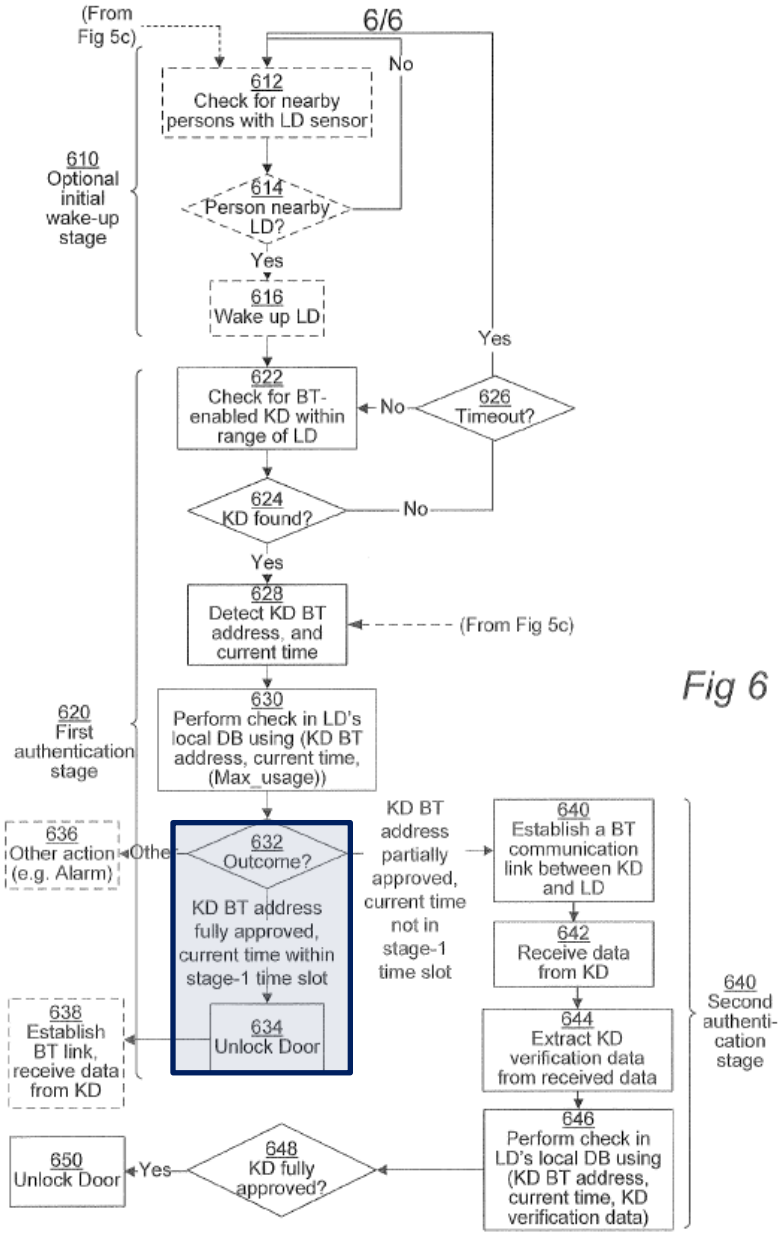


Fig 6

Id., FIG. 6 (annotated).

C. [Claim 3] The access device of claim 2 wherein the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation from the start time up to the predetermined duration that is all day.

89. *Knutsson* renders obvious claim 3.

90. As explained in Section X.B for claim 2, *Knutsson*'s temporal data may be "one [or] more dates and/or times which define start point ('Valid_from') and end point ('Valid_to') for the temporary access permitted." *Knutsson*, 12:24-26. It is my experience that a POSA would have found it obvious that *Knutsson*'s one date includes where the time slot defined by the start point and end point is the length of "a day," because a single date corresponds to a day. *Knutsson* even provides examples of stage-1 or stage-2 authentication of "during working days" or "any time (00-24)." *Id.*, 18:16-19:1. In my opinion, the example of (00-24) corresponds to all day, and a POSA would have found it obvious to set a time of all day based on the hours 00-24 covering all 24 hours of a day. *Knutsson* further provides an example of a stage-2 authentication, in Table 1 of "00-24," which would be all day.

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).

Knutsson's temporal data may be "one [or] more dates and/or times which define start point ('Valid_from') and end point ('Valid_to') for the temporary access permitted." *Id.*, 12:24-26. If the outcome of checks of blocks 628-630 "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" that "will cause unlocking of the lock, etc, and allow opening of the door, etc, to the protected environment." *Id.*, 20:7-11.

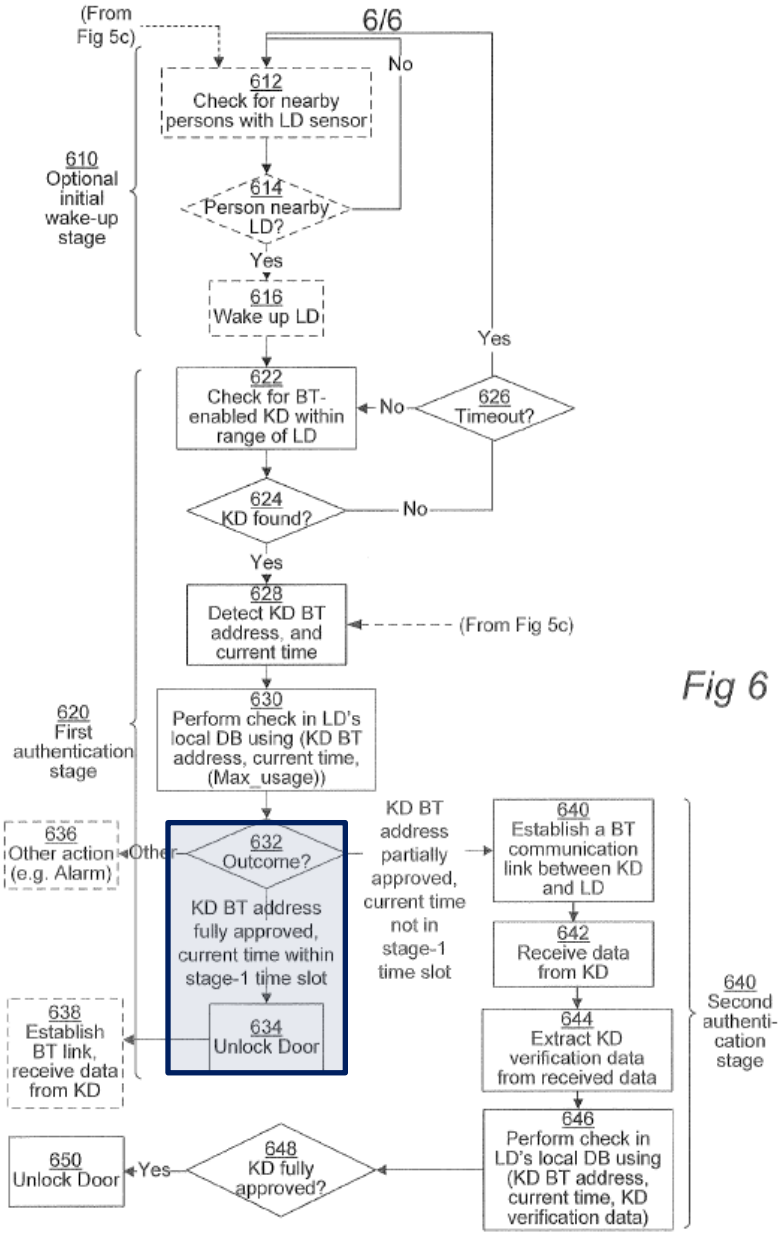


Fig 6

Id., FIG. 6 (annotated).

D. [Claim 4] The access device of claim 1 wherein the interval of the reservation of the current reservation certificate comprises a start time and a duration and the processor is configured to activate

the door lock to allow the portable terminal to unlock the door lock from the start time up to the duration.

91. Claim 4 is substantially similar to claim 2, except that claim 2 has additional limitations related to the "current time," as shown below in underline.

Claim 2	Claim 4
The access device of claim 1	The access device of claim 1
wherein the processor <u>is configured to determine the current time is within the interval of the reservation by determining if the current time is</u> within a start time of the interval of the reservation of the current reservation certificate and a predetermined duration and	wherein the interval of the reservation of the current reservation certificate comprises a start time and a duration and
is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the predetermined duration.	the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the duration.

The underlined additional limitations are covered with reference to claim 2 discussed above in Section X.B. *Knutsson* renders claim 4 obvious for the reasons explained for claim 2 in Section X.B.

E. [Claim 6] The access device of claim 1 wherein the interval of the reservation of the current reservation certificate comprises a start time and an end time.

92. *Knutsson* renders obvious claim 6.

93. As explained in Section X.A.5 for [1D], *Knutsson*'s "CPU 313 … [checks] whether the current time falls within any stage-1 time slot defined for that

Bluetooth® address." *Knutsson*, 20:4-7, FIG. 6 at blocks 628-630. *Knutsson*'s temporal data may be "one [or] more dates and/or times which define start point ('Valid_from') and end point ('Valid_to') for the temporary access permitted." *Id.*, 12:24-26. *Knutsson* discloses its data object 12, as shown in Figures 4a-4b, includes "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.

Structure of generated data object 12:

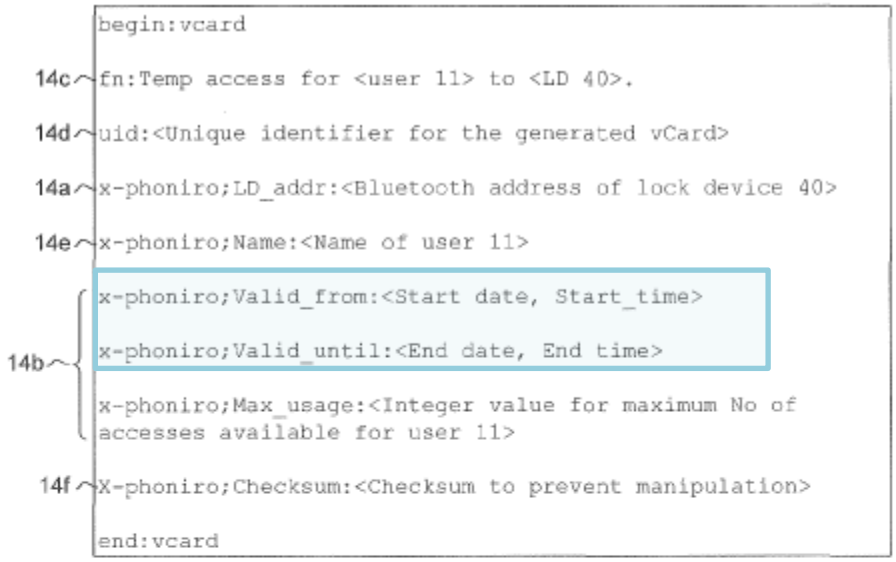


Fig 4a

Example of generated data object 12:



Fig 4b

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

F. [Claim 5] The access device of claim 6 wherein the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the end time.

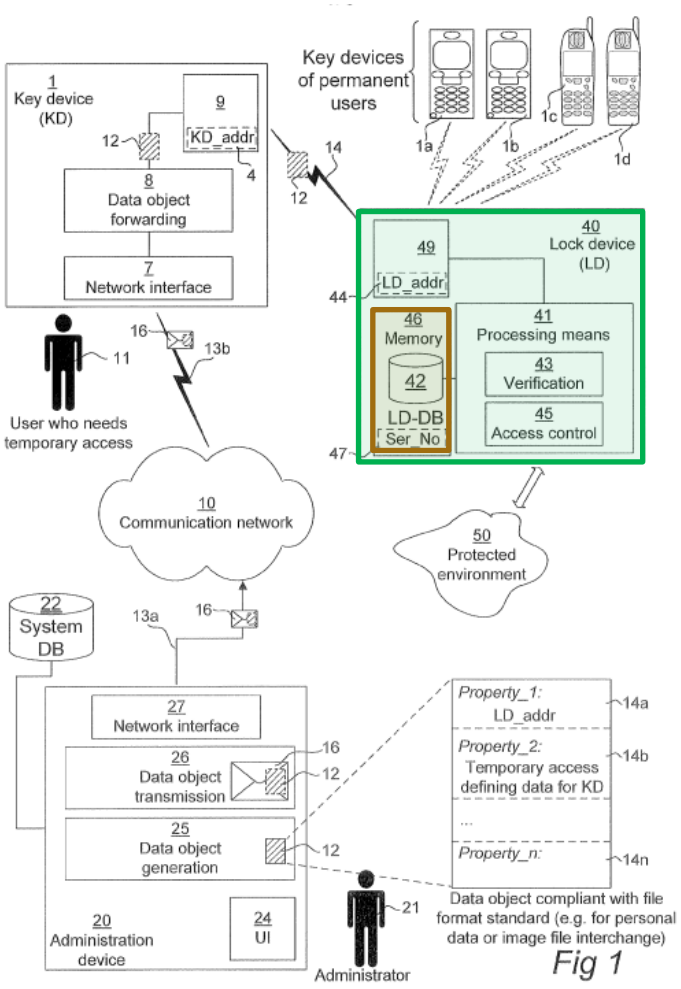
94. As explained in Section X.E for claim 6, *Knutsson*'s temporal data may be "one [or] more dates and/or times which define start point ('Valid_from') and end point ('Valid_to') for the temporary access permitted." *Knutsson*, 12:24-26. *Knutsson*'s "CPU 313 … [checks] whether the current time falls within any stage-1 time slot defined for that Bluetooth® address," (*id.*, 20:4-7, FIG. 6 at blocks 628-630), 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.

G. Claim 8

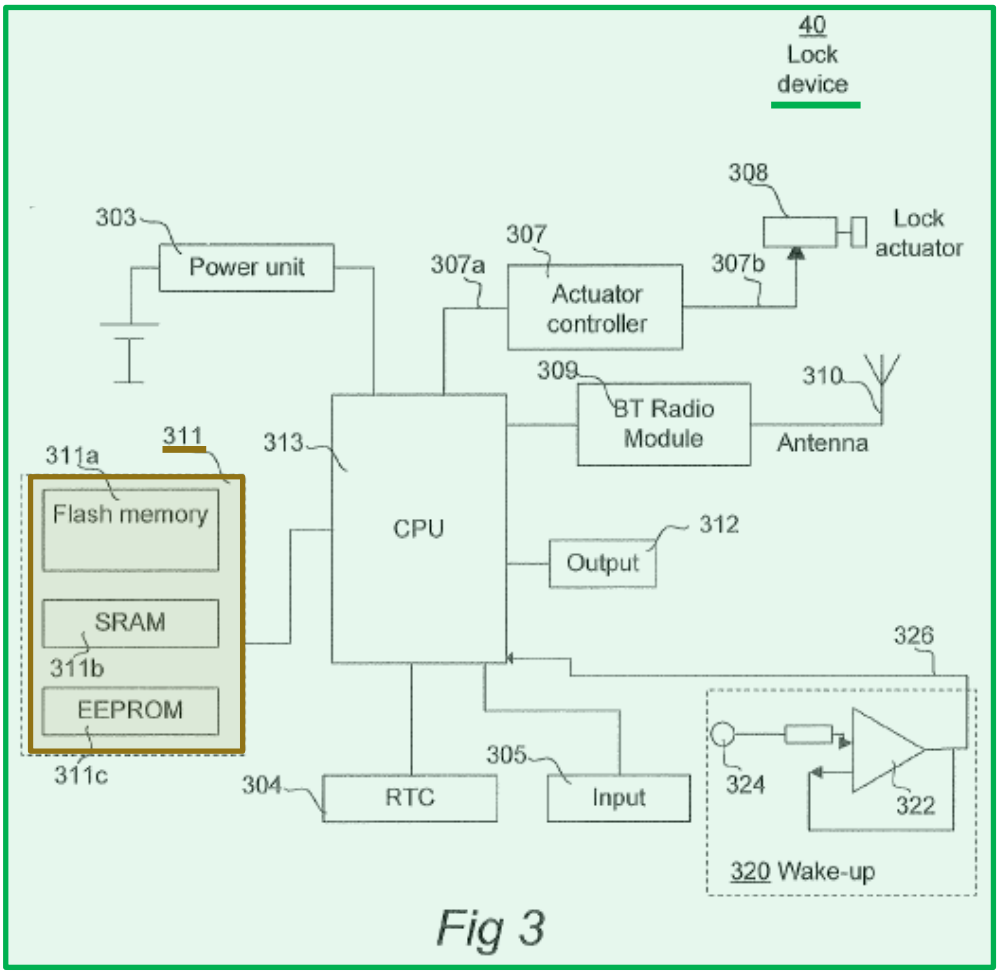
1. [8A] The access device of claim 1 further comprising: a memory to which the processor has access, the memory is configured to comprise a symmetric key:

95. *Knutsson* renders obvious [8A] because *Knutsson* discloses that its lock device includes local memory 46 (memory) coupled to the processor and configured to decipher the data object 12 (a symmetric key).

96. *Knutsson* discloses a "local memory 46 of the lock device," (*Knutsson*, 12:19), and that "the memory 311 may be identical to the aforementioned local memory 46." *Id.*, 17:11-13.



Id., FIG. 1 (annotated).



Id., FIG. 3 (annotated).

97. *Knutsson* discloses storing certain communication information including a communication address and serial number, "of the lock device … in local memory of the lock device." *Id.*, 6:13-17. Further, *Knutsson* discloses the elimination of decryption key distribution because the lock device and administrative device already know the decryption key. *Id.*, 6:17-19. The decryption key, the communication identifier, is the same in both devices, corresponding to "a

symmetrical key," which is decrypted by the processing means 41 of the lock device. *Knutsson*, 16:6-9. Another disclosure of *Knutsson* is "that all communication between key device and lock device may be encrypted in accordance with an encryption algorithm, such as Blowfish." *Id.*, 19:12-14. *Knutsson* discloses its lock device uses "a decryption key." *Id.*, 8:19-22. In my view, a POSA would have found it obvious that a decryption key of Blowfish, for decrypting received communication, such as *Knutsson*'s data object from a key device, would be stored on the lock device because all of *Knutsson*'s communication is encrypted, and the lock device would need to access the decryption key, like its other communication information, in order to read and process the encrypted communications for example to "check" the communication address. *Id.*, 8:19-22, 20:4-7.

98. Based on my experience, a POSA would have understood that Blowfish is a symmetric key encryption method because other cited art describes Blowfish as a known encryption method with a symmetric key/cipher. For example, U.S. Patent No. 8,412,837 provides "[a]n example of encrypting the private key is to encrypt it with a symmetric cipher such as … Blowfish," (U.S. Patent No. 8,412,837 (Ex-1011), 6:37-41), and U.S. Patent No. 5,794,207 describes "a symmetric key embodiment" where the "encryption may be implemented … with any of several

algorithms known in the art such as … Blowfish." U.S. Patent No. 5,794,207 (Ex-1012), 24:24-31.

2. [8B] wherein at least a portion of the current reservation certificate is encrypted by a server of the access system configured to use the symmetric key and the processor is configured to verify that the current reservation certificate is genuine by decrypting the portion with the symmetric key.

99. *Knutsson* renders obvious [8B] because *Knutsson* discloses that data object 12 (current reservation certificate) is encrypted and deciphered by the processor at the lock device (using the symmetric key to verify the reservation certificate).

100. *Knutsson*'s data object 12 is encrypted by a server because data object 12 originates with *Knutsson*'s administration device 20 which can be a "server computer." *Knutsson*, 11:1-6. *Knutsson*'s administration device 20 includes "data object generation module 25 [that] is configured to create a data object 12." *Id.*, 11:24-26. This data object 12 is from administration device 20, where it is packaged into message 16 and then sent through communication network 10 to the key device 1 and to lock device 40, as shown in Figure 1.

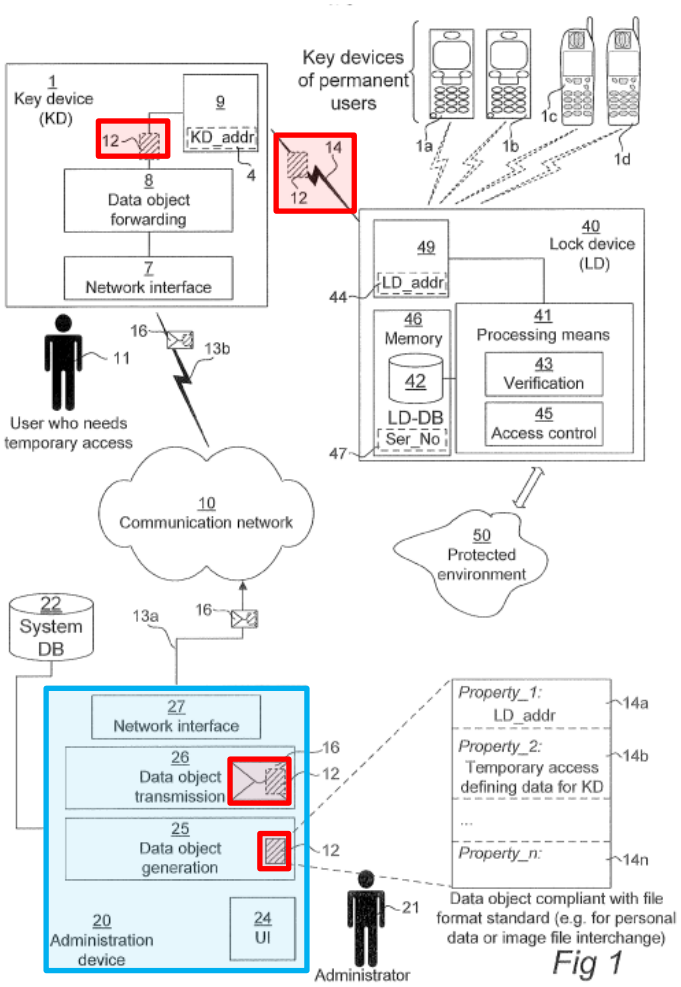


Fig 1

Id., FIG. 1 (annotated).

101. As explained for [8A] in Section X.G.1, *Knutsson* discloses "that all communication between key device and lock device may be encrypted in accordance with an encryption algorithm, such as Blowfish." *Id.*, 19:12-14. *Knutsson* discloses the elimination of decryption key distribution because the lock device and administrative device already know the decryption key. *Id.*, 6:17-19. The decryption key, the communication identifier, is the same in both devices, corresponding to "a

symmetrical key." *Knutsson* discloses "[t]he lock device 40 has processing means 41 for processing the received data object 12" and "[i]f the data object was encrypted at the administration device 20, the processing means 41 performs decryption." *Id.*, 16:6-9. A POSA would have found it obvious that decrypting communications to achieve "enhanced security" would include determining that the communications are from the correct source, the administrative device, corresponding to the claimed "the processor is configured to verify that the current reservation certificate is genuine by **decrypting the portion with the symmetric key**."

102. It is my experience that a POSA would have understood *Knutsson*'s data object 12 from administrator device 20 would be encrypted according to the disclosed Blowfish system, and further, in my view, a POSA would have understood that Blowfish is a known symmetrical key/cipher system as discussed above. *See* U.S. Patent No. 8,412,837 (Ex-1011), 6:37-41; U.S. Patent No. 5,794,207 (Ex-1012), 24:24-31. Accordingly, a POSA would have found it obvious that the data object 12 would be encrypted using a symmetrical key of the Blowfish encryption and then decrypted by the recipient, *Knutsson*'s lock device 40, using the same symmetrical key.

103. *Knutsson* discloses Blowfish is used so "data integrity is ascertained." *Knutsson*, 19:14. Based on my experience, a POSA would have understood data

integrity includes security, one of *Knutsson*'s goals for its encryption, (*id.*, 6:13-17), which would necessarily involve determining that *Knutsson*'s data object 12 (i.e., the claimed "reservation certificate") is from the correct sender, which in this case is *Knutsson*'s administrator device 20. This system corresponds to the claimed "being genuine" because the encryption ensures that the communications originate from known sources for legitimate purposes (i.e., to grant temporary access to protected environments).

H. [Claim 9] The access device of claim 1 wherein the processor is configured to verify that the current reservation certificate is genuine.

104. *Knutsson* renders obvious claim 9 because *Knutsson* discloses using encryption for security and "data integrity," as explained for [8B] in Section X.G.2. Based on my experience, a POSA would have understood that encryption by the server and decryption by the lock device would determine whether *Knutsson*'s data object 12 is genuine, as that is part of ensuring "data integrity." Further, *Knutsson*'s encryption methods ensure that the data object 12 is received by lock device 40, including processing means, from the correct source, the administrative device 20, because the processing means can decrypt the message using a key shared amongst known, trusted devices. Using a similar idea of verifying data object 12, *Knutsson* discloses "the lock device 40 detects the communication identifier (Bluetooth®

address, 'KD_addr') 4 of the key device 1," (*Knutsson*, 16:4-5), and its processor includes "[v]erification means 43 … for verifying that the first property 14a of the received data object 12 matches the communication identifier (Bluetooth® address, 'LD_addr') 44 of the lock device." *Id.*, 16:11-13

I. [Claim 10] The access device of claim 1 further comprising: an identification to which the processor has access, the identification corresponding to one of the access device and the door lock, wherein the processor is configured to determine that the current reservation certificate comprises data representative of the identification.

105. *Knutsson* renders obvious claim 10 because *Knutsson* discloses an identifier (identification) that corresponds to the lock device (access device) that the lock device processor receives and verifies from data object 12 (the processor is configured to determine that the current reservation certificate comprises data representative of the identification).

106. *Knutsson* discloses storing "the communication address (Bluetooth® address) of the lock device's radio transceiver as well as a serial No of the lock device … in local memory of the lock device." *Knutsson*, 6:13-17. *Knutsson* further discloses "**the communication identifier specified in the created data object 12** in the administration device 20 is conveniently the Bluetooth® address 44 of **the lock device's 40 Bluetooth® transceiver 49**." *Id.*, 12:4-7 (emphases added). This data is

included in the data object 12, shown in the first property 14a in FIGS. 4a-4b, reproduced below.

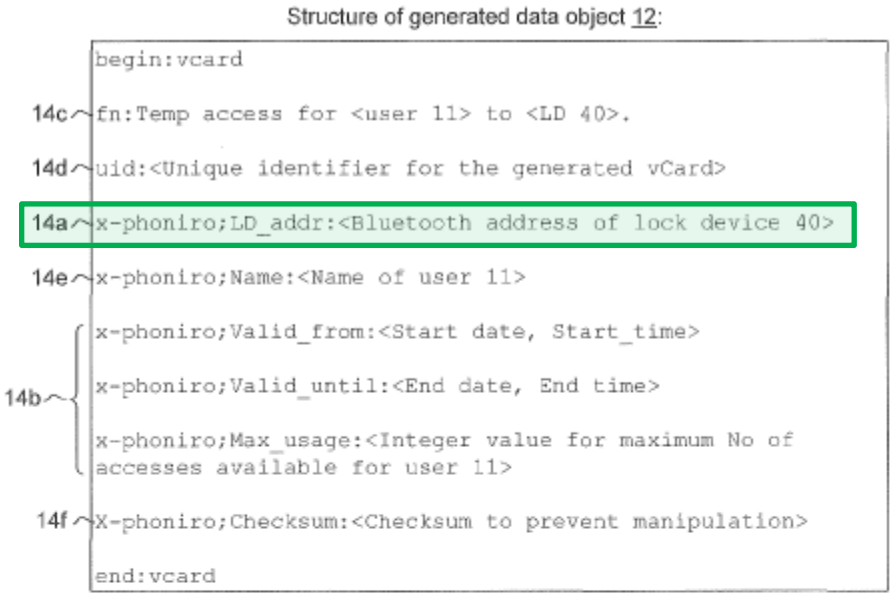


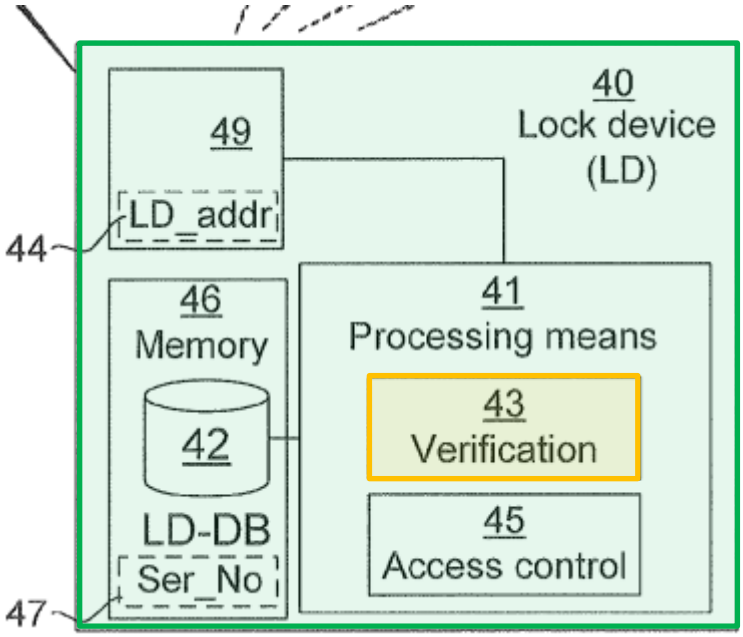
Fig 4a



Fig 4b

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

107. *Knutsson* discloses "the lock device 40 detects the communication identifier (Bluetooth® address, 'KD_addr') 4 of the key device 1," (*id.*, 16:4-5), and its processor or processing means 41 includes "[v]erification means 43 … for verifying that the first property 14a of the received data object 12 matches the communication identifier (Bluetooth® address, 'LD_addr') 44 of the lock device." *Id.*, 16:11-13.



Id., FIG. 1 Excerpt (annotated).

108. The claim only requires, "the identification correspond[s] to one of the access device and the door lock," and *Knutsson* discloses its Bluetooth® address (identification) corresponds to lock device 40 (access device). *Knutsson*'s lock device activates after verification once "data integrity is ascertained," corresponding

to the claimed "activating" step of claim 22: *Knutsson* discloses "the outcome of these checks [being] fully positive … will cause unlocking of the lock." *Knutsson*, 20:7-11.

J. Claim 13

109. *Knutsson* renders obvious claim 13.

1. [13p] "A method for use by an access device in an access control system, the method comprising:"

110. *Knutsson* renders obvious [13p] because *Knutsson* discloses "an associated lock device, an associated administration device for providing temporary access to the lock device for a user of a wireless key device, **as well as associated methods** and computer program products." *Knutsson*, 1:8-11. *Knutsson* further discloses a lock device (the claimed "access device") in "an access control system." *Id.*, 1:6-8.

2. [13A] "accepting, by a processor"

111. *Knutsson* renders obvious [13A], as explained for [1A] in Section X.A.2.

3. [13B] "through a communication module, a reservation certificate… presented with a portable terminal;

112. *Knutsson* renders obvious [13B], as explained for [1B] in Section X.A.3.

4. [13C] "a reservation certificate that comprises an interval of a reservation"

113. *Knutsson* renders obvious [13C], as explained for [1C] in Section X.A.4.

5. [13D] "determining, by the processor, that the reservation certificate presented by the portable terminal is current by comparing the interval of the reservation to a current time accessible to the processor and determining that the current time is within the interval of the reservation; and activating, by the processor on the basis of the reservation certificate being current,"

114. *Knutsson* renders obvious [13D], as explained for [1D] in Section X.A.5. *Knutsson*'s lock device activates after verification once "data integrity is ascertained," including checking whether the current time falls within the time slot of data object 12, corresponding to the claimed "activating" step. *Knutsson*, 17:4-6, 19:14, 20:4-7. *Knutsson* discloses "[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. One of those checks includes determining "authorization [] based solely on the key device's Bluetooth® address…." *Id.*, 18:1-4.

6. [13E] "activating, by the processor … a door lock to allow the portable terminal to unlock the door lock during the interval of the reservation."

115. *Knutsson* renders obvious [13E], as explained for [1E] in Section X.A.6.

K. [Claim 14] The method of claim 13 wherein determining that the current time is within the interval of the reservation comprises determining that the current time is within a start time of the interval of the reservation and a predetermined duration and wherein the certificate is current from the start time up to the predetermined duration.

116. *Knutsson* renders obvious claim 14, as explained for [2A] in Section X.B.1. Regarding the limitation, "wherein the certificate is current from the start time up to the predetermined duration," *Knutsson* discloses its object 12 would be used from its disclosed start time to the end time, also an end of the duration, as compared to the "current time," (*Knutsson*, 20:4-7), and thus the object 12 would be current during this time slot. Further, *Knutsson*'s disclosure of "temporary" access is for a set time, time slot, or an interval. *Id.*, Abstract. *Knutsson* further confirms this by explaining that the lock device including CPU 313 determines whether the current time, which CPU 313 has access to, falls within the "stage-1 time slot," (*id.*, 17:21-22, 20:4-7), where the time slot corresponds to the claimed "interval." *Knutsson* even provides examples of time slots including "00-24," as in from 0000 to 2400 using military time, which would be 12:00 AM to 12:00 AM in 12-hour

time, "2005-03-24: 19-22," as in March 24, 2005, from 1900 to 2200 (7:00 PM to 10:00 PM), and "Mon-Fri: 07-15," as in Monday through Friday, 0700 through 1500 (7:00 AM to 3:00 PM). *Knutsson*, Table 1, 18:16-19:16.

L. [Claim 15] The method of claim 14 wherein the predetermined duration is all day.

117. *Knutsson* renders obvious claim 15, as explained for claim 3 in Section X.C.

M. [Claim 16] The method of claim 13 wherein the interval of the reservation of the reservation certificate further comprises a start time and a duration and the reservation certificate is current from the start time up to the duration.

118. *Knutsson* renders obvious claim 16, as explained for claim 4 in Section X.D.

N. [Claim 18] The method of claim 13 wherein the interval of the reservation comprises a start time and an end time.

119. *Knutsson* renders obvious claim 18, as explained for claim 6 in Section X.E.

O. [Claim 17] The method of claim 18 wherein the reservation certificate is current from the start time up to the end time.

120. *Knutsson* renders obvious claim 18, as explained for claim 5 in Section X.F.

P. [Claim 20] The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a

symmetric key stored in a memory accessible to the processor, wherein the b) determining by the processor is further that the reservation certificate is genuine on the basis of decrypting the portion with the symmetric key, and the c) activating is on the further basis of the reservation certificate being genuine.

121. *Knutsson* renders obvious claim 20, as explained for claim 8 in Section X.G.

122. *Knutsson*'s lock device activates after verification once "data integrity is ascertained," corresponding to the claimed "activating" step. *Knutsson*, 19:14. *Knutsson* discloses "[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. One of those checks includes determining "authorization [] based solely on the key device's Bluetooth® address…." *Id.*, 18:1-4.

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

123. *Knutsson* renders obvious claim 21, as explained for claim 9 in Sections X.H and claim 20 in Section X.P. As to c), if the outcome of checks of blocks 628-630 "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" that "will cause

unlocking of the lock, etc, and allow opening of the door, etc, to the protected environment." *Id.*, 20:7-11. One of those checks includes determining "authorization [] based solely on the key device's Bluetooth® address." *Id.*, 18:1-4.

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

124. *Knutsson* renders obvious claim 22, as explained for claim 10 in Sections X.I and claim 20 in Section X.P. As to c), if the outcome of checks of blocks 628-630 "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" that "will cause unlocking of the lock, etc, and allow opening of the door, etc, to the protected environment." *Id.*, 20:7-11. One of those checks includes determining "authorization [] based solely on the key device's Bluetooth® address." *Id.*, 18:1-4.

XI. GROUND 2: CLAIMS 7, 11, 19, AND 23 ARE RENDERED OBVIOUS BY *KNUTSSON* IN VIEW OF *DEBRY*

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

125. As explained in Section IX.A, claims 7, 11, 19, and 23 require encryption elements that, while suggested by *Knutsson*, are not expressly disclosed. A POSA, however, in my opinion, would have been motivated to implement

DeBry's encryption methods into encryption of *Knutsson*'s data object 12 because *DeBry* discloses, "[s]ome files must be encrypted at the sending end and decrypted at the receiving end to ensure that the file contents are not intercepted by an unauthorized entity during the transmission." *DeBry*, 1:54-57. *Knutsson* generally discloses an "access control system" for a "protected environment" such as "a room, apartment, commercial or public premises" with a "controllable lock actuator configured to unlock the lock mechanism upon detection and successful authorization." *Knutsson*, 10:13-30. In my experience, a POSA would have understood the importance of security to "controllable lock actuators" for a "protected environment" to prevent unauthorized access. *See id*.. *Knutsson* further supports this point as it discloses the goal of "enhanced security" achieved through encryption, and "that all communication between key device and lock device may be encrypted in accordance with an encryption algorithm, such as Blowfish." *Id*., 6:13-17, 19:12-14. A POSA would have understood that "such as Blowfish" is an example and other known encryption algorithms could have been used. *DeBry* discloses that "public key cryptography was first introduced … in 1976" and "can be used to ensure the privacy of transmitted messages." *DeBry*, 2:28-36. *DeBry* discloses that "public key cryptography does solve many of the problems … in [symmetric] cryptography." *Id.*, 2:33-36. For example, "[m]essages encrypted with

a person's public key can only be decrypted with that person's private key. Even if one key is known, it is not feasible to compute the other key." *Id.*, 2:43-45. The reference *Micali* confirms that a POSA would have found it desirable to use public keys because *Micali* discloses use of keys "to prove that a given message M originates from a given user U," where a signature key is kept secret and a related public key is "made as public as possible." *Micali*, 9:16-27. Thus, it is my opinion that a POSA would have incorporated *DeBry*'s encryption methods for "enhanced security" to avoid unauthorized interceptions.

126. In my experience, a POSA would have had reasonable expectations of success combining *DeBry* and *Knutsson* because *DeBry*'s encryption methods are known methods of encryption communications between one device to another, such as *DeBry*'s client system communicating with a printer. *DeBry*, 5:34-36. Similarly, *Knutsson*'s key device that can be a PDA or a mobile phone, (*Knutsson*, 4:32-5:4), communicat[es] to actuate *Knutsson*'s lock device 40 to open a lock. *Id.*, 10:24-30. In my opinion, a POSA would have known that combining *DeBry*'s encryption methods in *Knutsson*'s key device when *Knutsson*'s key device instructs lock device 40 to open would ensure data integrity and security, which are goals of *Knutsson* and *DeBry*.

B. Claim 7

1. [7A] The access device of claim 1 further comprising: a memory to which the processor has access, the memory is configured to comprise a public key for a server of the access system configured to issue the current reservation certificate;

127. *Knutsson* in combination with *DeBry* renders obvious [7A] because *Knutsson* discloses a memory coupled to a processor, as well as encryption of the reservation certificate, and *DeBry* further discloses a specific encryption method using a public key.

128. *Knutsson* discloses "local memory 46 of the lock device," (*Knutsson*, 12:19), and "the memory 311 may be identical to the aforementioned local memory 46." *Id.*, 17:11-13.

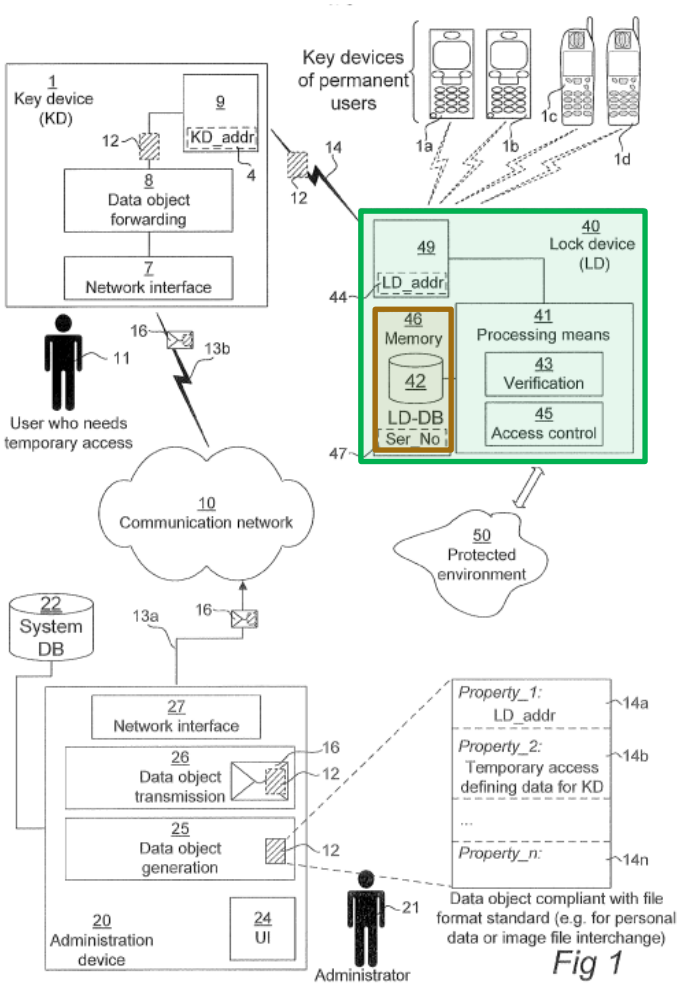
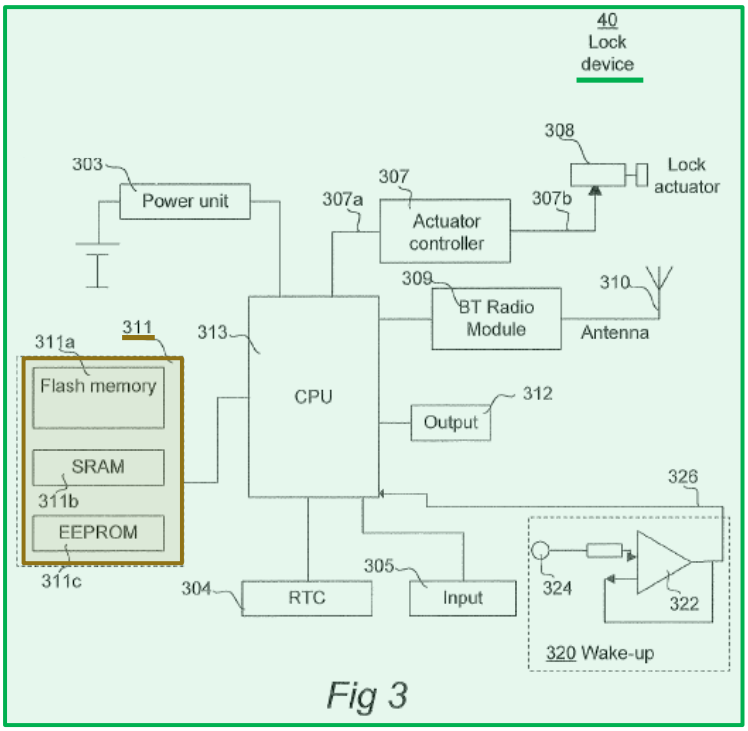


Fig 1

Id., FIG. 1 (annotated).



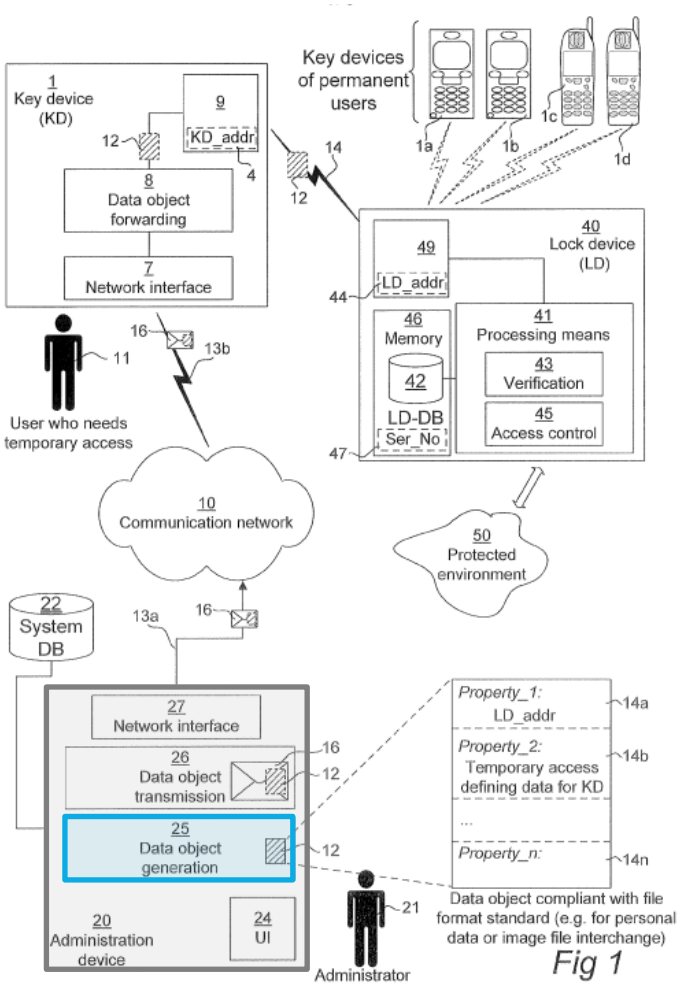
Id., FIG. 3 (annotated).

129. *Knutsson* discloses storing a communication address and serial number, "of the lock device … in local memory of the lock device." *Id.*, 6:13-17. *Knutsson* discloses "the administration device [is configured] to encrypt the contents of the generated data object" using the communication address and serial number of the lock device as an encryption/decryption key. *Id.*, 6:13-19. *Knutsson* discloses that there is no need for "a separate communication of the decryption key from the administration device to the lock device" because the communication address and serial number are stored "in local memory of the lock device." *Id.* Therefore, in my

opinion, a POSA would have understood *Knutsson* teaches storing an encryption/decryption key in the memory of the lock device.

130. Alternatively, *Knutsson* discloses "that all communication between key device and lock device may be encrypted in accordance with an encryption algorithm, such as Blowfish." *Id.*, 19:12-14. A POSA would have found it obvious that a decryption key of Blowfish, for decrypting received communication, such as *Knutsson*'s data object from a key device, would be stored on the lock device so "that all communication between key device and lock device may be encrypted," and that the receiving device could decrypt and thus process the contents of the encrypted messages.

131. In either case, the stored key would relate to communications that originate with *Knutsson*'s administration device 20 which can be a "server computer." *Knutsson*, 11:1-6. *Knutsson*'s administration device 20 includes "data object generation module 25 [that] is configured to create a data object 12." *Id*., 11:24-26. This data object 12 is from administration device 20, as shown in Figure 1.



Id., FIG. 1 (annotated).

132. *Knutsson* does not expressly disclose that its key is a "public key," but *DeBry* does. *DeBry* discloses, "[i]n a public key system, it is possible to communicate privately without transmitting any secret key. For example, the encryption key for each user is made public by being distributed or published." *DeBry*, 2:46-49. A POSA would have found it obvious that *Knutsson*'s memory 46 of FIG. 1 would be used to store a public key that is "distributed or published" in a

public key system. In my opinion, a POSA would have been motivated to combine *DeBry* and *Knutsson*, as discussed above in Section XI.A.

2. [7B] wherein at least a portion of the current reservation certificate is encrypted by the server using a private key and the processor is configured to verify that the current reservation certificate is genuine by decrypting the portion with the public key.

133. *Knutsson* in view of *DeBry* renders obvious [7B] because *Knutsson* discloses encryption of the reservation certificate and *DeBry* further discloses a specific encryption method using both public and private keys.

134. *DeBry* discloses "a user who has made public a public key can digitally sign a message by encrypting the message, or a hash of it, with the user's private key before transmitting the message. Recipients of the message can verify the message or signature by decrypting it with the sender's public encryption key." *DeBry*, 3:11-16. Further, *DeBry* discloses, "[a]nyone who has the sender's public encryption key can read the message or signature. Any such recipient is assured of the authentication of the creator of the message …." *Id.*, 3:20-24. A POSA would have found it obvious to incorporate a known system of encrypting and decrypting using a public/private key pair in the way described by *DeBry* into *Knutsson*'s encrypting and decrypting system because *DeBry*'s system would have been an obvious existing use of encryption to enhance security in similar access systems with similar devices.

See id., 2:33-36; *Knutsson*, 6:13-17, 19:12-14; *Micali*, 9:16-17 ("to prove that a given message M originates from a given user U"). Therefore, in my opinion, a POSA would have been motivated to combine *DeBry* and *Knutsson*, as discussed above in Section XI.A.

C. Claim 11

1. [11A] The access device of claim 1 further comprising: a memory to which the processor has access, the memory is configured to comprise a private key of the access device;

135. *Knutsson* renders obvious [11A] because *Knutsson* discloses a memory coupled to a processor, as well as encryption of the reservation certificate, and *DeBry* further discloses a specific encryption method using a private key.

136. *Knutsson* discloses "local memory 46 of the lock device," (*Knutsson*, 12:19), and "the memory 311 may be identical to the aforementioned local memory 46." *Id*., 17:11-13.

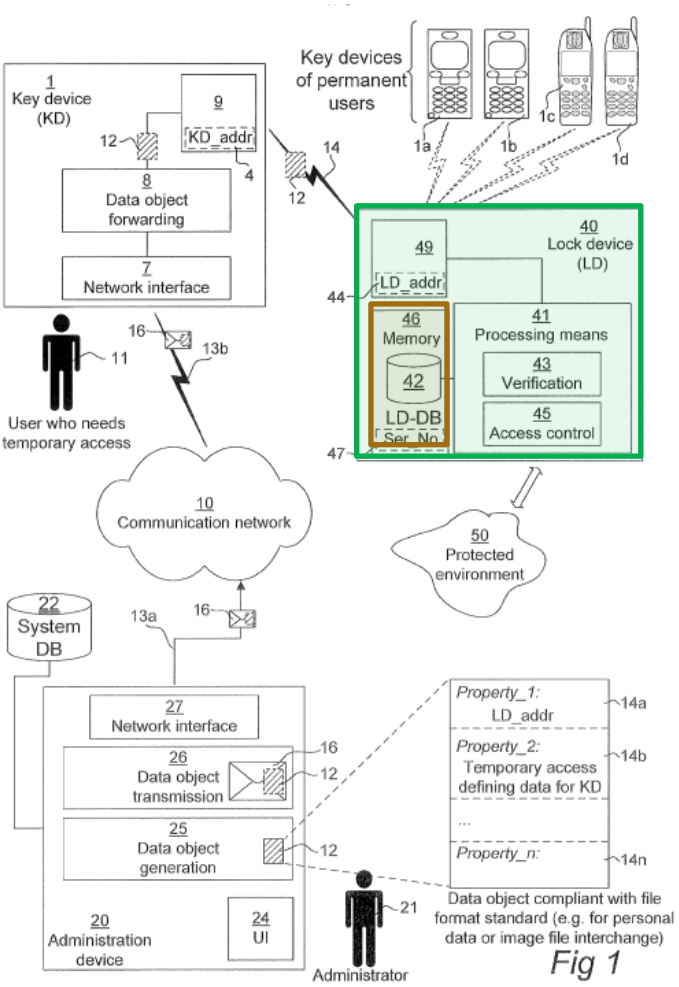
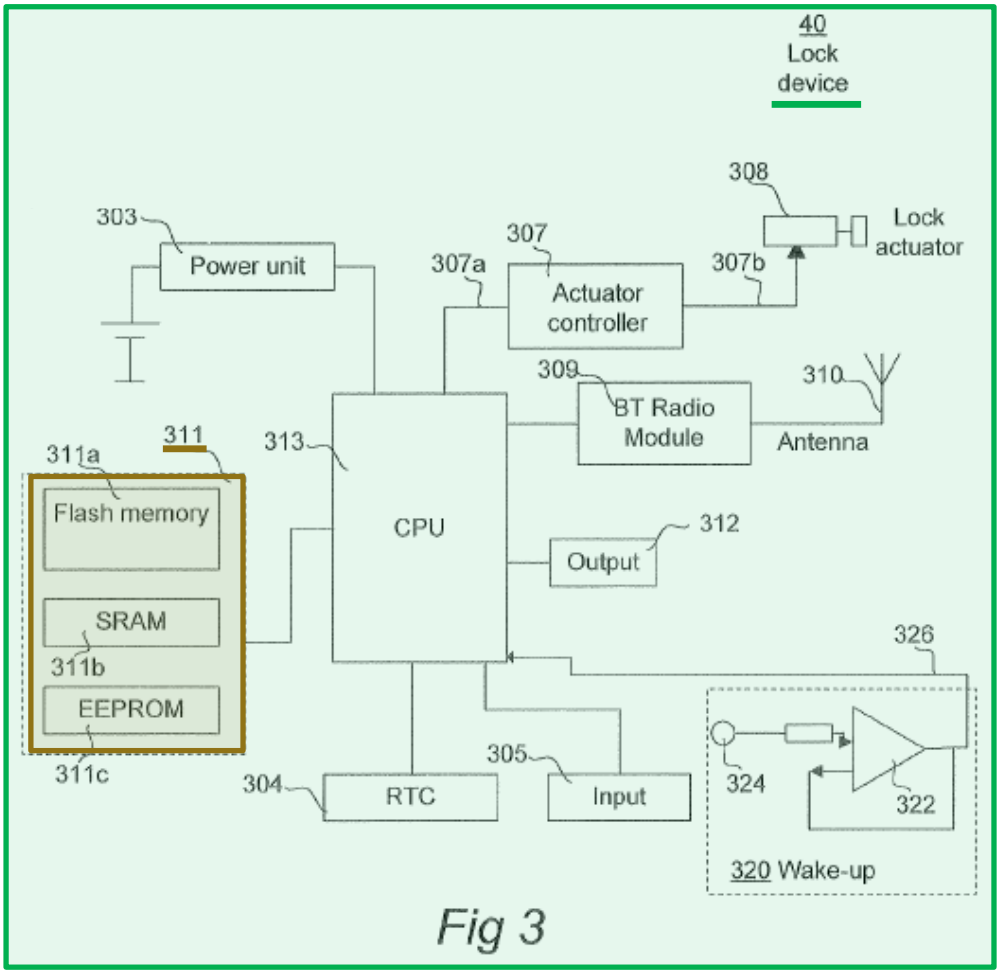


Fig 1

Id., FIG. 1 (annotated).



Id., FIG. 3 (annotated).

137. As discussed above in Section XI.B., *Knutsson* discloses storing a communication address and serial number as a decryption key, "in local memory of the lock device." *Id.*, 6:13-17. *Knutsson* discloses, "the administration device [is configured] to encrypt the contents of the generated data object" using the communication address and serial number of the lock device as an encryption/decryption key. *Id.*, 6:13-19. *Knutsson* discloses that there is no need for

"a separate communication of the decryption key from the administration device to the lock device" because the communication address and serial number are stored "in local memory of the lock device." *Id.* Alternatively, *Knutsson* discloses "that all communication between key device and lock device may be encrypted in accordance with an encryption algorithm, such as Blowfish." *Id.*, 19:12-14. A POSA would have found it obvious that a decryption key, for decrypting received encrypted communication, such as *Knutsson*'s data object from a key device, would be stored on the lock device in order for the lock device to decrypt incoming encrypted messages.

138. To the extent it is argued *Knutsson* does not disclose a "private key," one of the most popular encryption/decryption means at the time, *DeBry* does. *DeBry* discloses, "[p]ublic key cryptography is based on two keys, a private key and a public key, that work together. A person's public key is openly made available to others, while their private key is kept secret." *DeBry*, 2:36-38. *DeBry* discloses, "[a]nyone desiring to communicate in private with a recipient merely encrypts the message under the recipient's public key. Only the recipient, who retains the secret decrypting key, is able to decipher the transmitted message." *Id.*, 2:51-53. A POSA would have found it obvious that *Knutsson*'s memory 46 of FIG. 1 would be used to retain a private key in a public key system. A POSA would have found it obvious

that *Knutsson*'s data object 12 could be encrypted, as disclosed in *Knutsson*, and that encrypting it using public key cryptography, which requires a private key on the receiving device, would have been an obvious existing use of encryption in similar access systems with similar devices. Section XI.A.

2. [11B] wherein at least a portion of the current reservation certificate is encrypted by a server of the access system configured to use a corresponding public key for the access device and the processor is configured to decrypt the portion with the private key.

139. *Knutsson* in view of *DeBry* renders obvious [11B] because *Knutsson* discloses encryption of the reservation certificate and *DeBry* further discloses a specific encryption and decryption method using both public and private keys.

140. *DeBry* discloses, "[p]ublic key cryptography is based on two keys, a private key and a public key, that work together. A person's public key is openly made available to others, while their private key is kept secret." *DeBry*, 2:36-38. *DeBry* discloses, "[i]n a public key system, it is possible to communicate privately without transmitting any secret key. For example, the encryption key for each user is made public by being distributed or published. Anyone desiring to communicate in private with a recipient merely encrypts the message under the recipient's public key. Only the recipient, who retains the secret decrypting key, is able to decipher the transmitted message." *Id*., 2:46-53. A POSA would have found it obvious to

incorporate a known system of encrypting and decrypting using a public/private key pair in the way described by *DeBry* into *Knutsson*'s encrypting and decrypting system because *DeBry*'s system would have been an obvious existing use of encryption. Section XI.A.

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

141. *Knutsson* in view of *DeBry* renders obvious claim 19, as explained for claim 7 in Section XI.B. *Knutsson*'s lock device activates after verification once "data integrity is ascertained," corresponding to the claimed "activating" step. *Knutsson*, 19:14. *Knutsson* discloses "[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.

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

comprising the step of: d) decrypting the portion, by the processor, with the private key.

142. *Knutsson* in view of *DeBry* renders obvious claim 23, as explained for claim 11 in Section XI.C.

XII. GROUND 3: CLAIMS 12, 24 ARE RENDERED OBVIOUS BY *KNUTSSON* IN VIEW OF *WOODARD*

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

143. As explained in Section IX.A, claims 12 and 24 require the processor to report to the server that the door lock was activated on the basis of the reservation certificate that is expressly disclosed by *Knutsson*. However, it is my experience that a POSA would have been motivated to implement *Woodard*'s lockbox access records stored in the lockboxes and those records being reported to the system's servers via a communications link into *Knutsson*'s lock device 40. It is my opinion that a POSA would have understood the importance of maintaining access records of a "protected environment" such as "a room, apartment, commercial or public premises" to address safety or security concerns. *See Knutsson*, 10:13-30. *Knutsson* discloses "registering the [forbidden] access attempt in memory 311 for later reporting." *Id*., 20:17-19. Further, a POSA would have understood that reporting successful and unsuccessful access attempts is beneficial because "[k]nowing when and who has actually accessed" a property "addresses safety concerns" and provides "valuable information" to interested parties. *Woodard*, [0004]. Further, a POSA

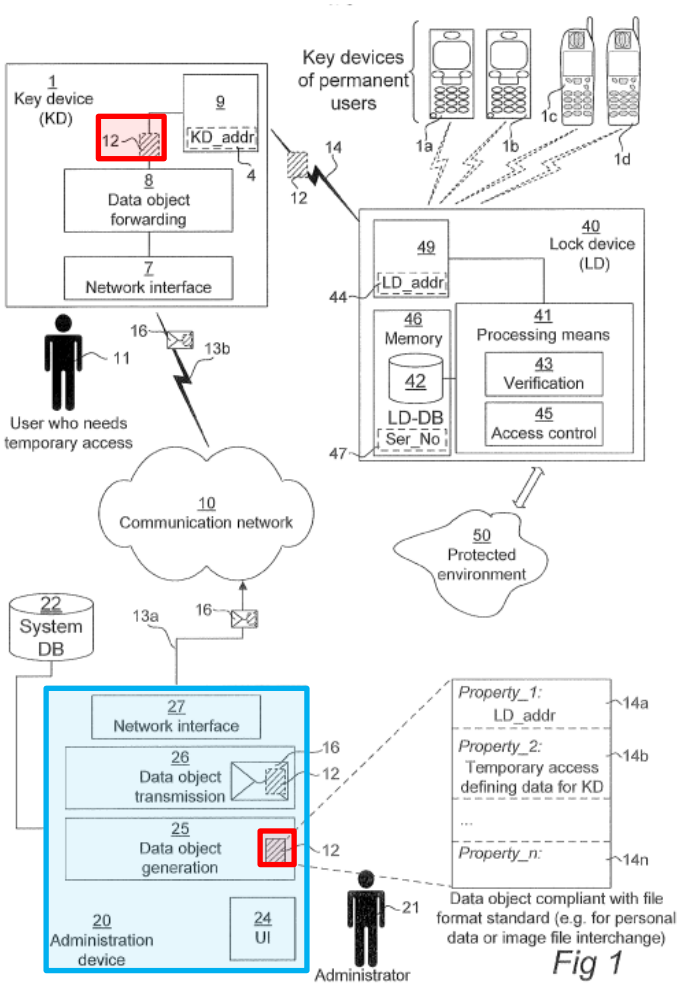
would have known "it can be important to know who went through a given door on a given day" and to thus log access information. *Micali*, 14:56-15:16. *Woodard* discloses, "automatically controlling access to an electronic lockbox utilizing showing appointment data maintained by a central showing management system." *Woodard*, [0010]. *Woodard* teaches that systems without a central management system "do not provide for a … seamless data exchange between a showing management system and associated electronic lockboxes or lockbox management systems." *Id.*, [0009]. *Woodard* teaches reporting access records stored in the lockboxes to the system's servers via a communications link because *Woodard* discloses "the lockbox access records stored in the electronic lockboxes are transmitted via a communications link between the electronic lockbox and the showing management system's servers coupled to the showing management system's database." *Id.*, [0072]. Thus, it is my further opinion that a POSA would have incorporated *Woodard*'s reporting and connectivity concepts into *Knutsson*'s access system to achieve a central management system and "complete the lockbox access record." *Id.*, [0013]. Besides maintaining a complete record, in my opinion, a POSA would have been further motivated to implement *Woodard* so that *Knutsson*'s lock device 40 could synchronize its time with a server so that *Knutsson*'s server and lock device would be "reliable." *Id.*, [0068].

144. In my experience, a POSA would have had reasonable expectations of success combining *Woodard* and *Knutsson* because *Woodard* and *Knutsson* disclose similar key devices, such as *Woodard*'s "electronic key device 104, which can be a PDA, a cell phone," (*id.*, [0003]), and *Knutsson*'s key device that can be a PDA or a mobile phone, (*Knutsson*, 4:32-5:4), to actuate access devices like *Woodard*'s lockbox 103 to "unlock a door," (*Woodard*, [0048]; *Knutsson*, FIG. 6 at block 634), or *Knutsson*'s lock device 40 to open a lock. *Knutsson*, 10:24-30. Commands in both cases are transmitted to an access device (electronic lockbox or lock device) to unlock a lock, and thus, it is my opinion that a POSA would have been able to implement *Woodard*'s central management system with *Knutsson*'s lock devices.

B. [Claim 12] The access device of claim 1 wherein the processor has access to a server of the access system through the communication module and the processor is configured to report to the server that the door lock was activated on the basis of the reservation certificate.

145. *Knutsson* in combination with *Woodard* renders obvious claim 12.

146. *Knutsson*'s administration device 20 can be a "server computer." *Knutsson*, 11:1-6. *Knutsson*'s administration device 20 includes "data object generation module 25 [that] is configured to create a data object 12." *Id.*, 11:24-26. This data object 12 is from administration device 20, as shown in Figure 1.



Id., FIG. 1 (annotated).

147. *Knutsson* does not disclose that its lock device 40 has direct access to administration device 20 or that the lock device 40 reports that it was activated, but *Woodard* does. *Woodard* discloses that "the lockbox access records stored in the electronic lockboxes are transmitted via a communications link between the electronic lockbox and the showing management system's servers coupled to the showing management system's database." *Woodard*, [0072]. It is my opinion that a

POSA would have found it obvious to implement *Woodard*'s lockbox access records stored in the lockboxes and those records being reported to the system's servers via a communications link into *Knutsson*'s lock devices 40 and administration device 20. In my opinion, a POSA would have been motivated to combine *Woodard* and *Knutsson*, as discussed above in Section XII.A.

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

148. *Knutsson* in view of *Woodard* renders obvious claim 24, as explained for claim 12 in Section XII.B.

XIII. GROUND 4: CLAIMS 1-6, 9-10, 12-18, 21-22, AND 24 ARE UNPATENTABLE OVER *ELFSTRÖM* IN VIEW OF *WOODARD*

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

149. As explained in Section IX.B, *Elfström* discloses the majority of claim limitations. *Elfström*, however, does not expressly disclose the reservation timing limitations, such as comparing the interval of the reservation of the current reservation certificate to a current time accessible to the processor, determining that the current time is within the interval of the reservation, and activating the door lock during the reservation interval. But *Woodard* does.

150. In my opinion, a POSA would have been motivated to implement *Woodard*'s timing management system into *Elfström*'s access control system 100

because *Woodard* discloses, "automatically controlling access to an electronic lockbox utilizing showing appointment data maintained by a central showing management system," (*Woodard*, [0010]), where "showing appointment time defines a time range in which access to the electronic lockbox is permitted." *Id.*, [0012]. Further, *Elfström* discloses, that "the access data encoded on the credential 136 may include … stay duration," (*Elfström*, 12:29-36), therefore, a POSA would have understood that *Elfström*'s access control system includes granting access based on time periods or durations. It is thus my opinion that a POSA would have incorporated *Woodard*'s automatic control concepts into *Elfström*'s access system to achieve a central management system. *Woodard*, [0012].

151. It is my opinion that a POSA would have further found it obvious to implement *Woodard*'s verification of an actual access time within a scheduled showing appointment time with *Elfström*'s access control module 116 to meet *Elfström*'s goal of confirming permissions. *Elfström*, 12:14-16. *Elfström* illustrates this point by explaining, "[f]ailure of the credential 136 to provide either valid credential identification information or access data will result in the access control module 136 maintaining its asset under secure conditions." *Id.*, 13:40-43. In my opinion, a POSA would have been motivated to meet *Elfström*'s standards of "secure conditions" by verifying the time, as disclosed in *Woodard*.

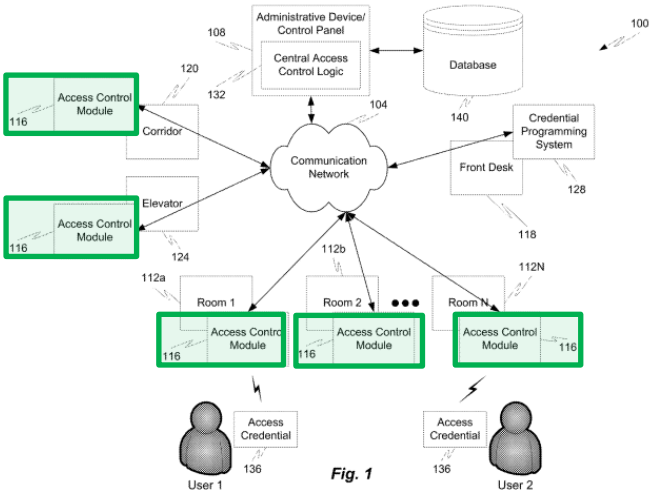
152. In my experience, a POSA would have had reasonable expectations of success implementing *Woodard*'s verification of an actual access time within a scheduled showing appointment time with *Elfström*'s access control module 116 because *Woodard* and *Elfström* disclose key devices, such as *Woodard*'s "electronic key device 104, which can be a PDA, a cell phone," (*Woodard*, [0003]), and *Elfström*'s credential 136 that can be a PDA or a mobile phone, (*Elfström*, 10:18-22), to actuate access devices like *Woodard*'s lockbox 103, (*Woodard*, [0048]), or *Elfström*'s access control device to open a lock. *Elfström*, 6:12-16.

B. Claim 1

153. *Elfström* renders obvious claim 1.

1. [1p] "An access device for use in an access control system, the access device comprising:"

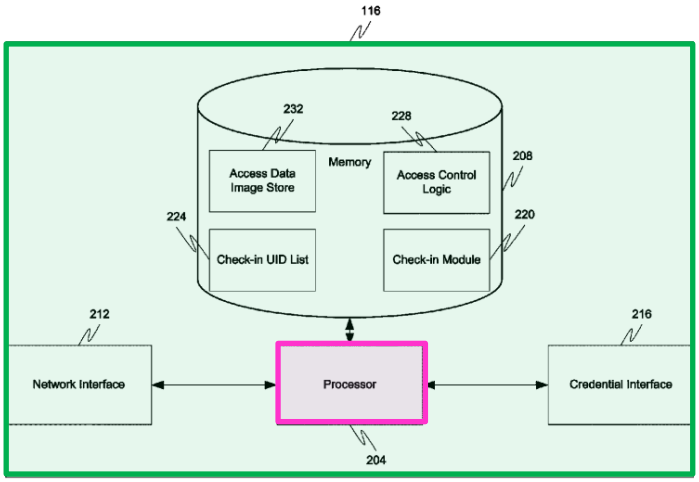
154. *Elfström* renders obvious [1p] because *Elfström* discloses, "[m]ethods, systems, and devices for controlling access within a multi-facility room are provided." *Elfström*, Abstract. *Elfström* discloses its access control system 100 can include "access control modules 116 [] adapted to communicate with access credentials 136 carried by users or guests of the multi-room facility." *Id.*, 4:58-65. *Elfström* further discloses its access control module 116 can include a processor that controls an access control device including, "an electronic lock, a magnetic lock, or an electric strike for a door." *Id.*, 5:60-61, 6:6-16.



Id., FIG. 1 (annotated).

2. [1A] "a processor (16) having control of a door lock (11);"

155. *Elfström* renders obvious [1A] because *Elfström* discloses, "[c]onnected to the communication interface 216 is a controller or processor 204." *Elfström*, 5:60-61. Further, "[t]he processor 204 controls and determines how the access control module 116 behaves when a credential 136 is presented to it." *Id.*, 5:67-6:1.

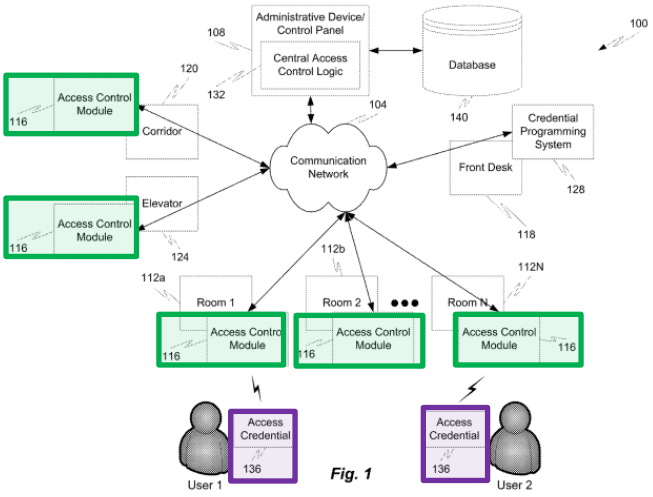


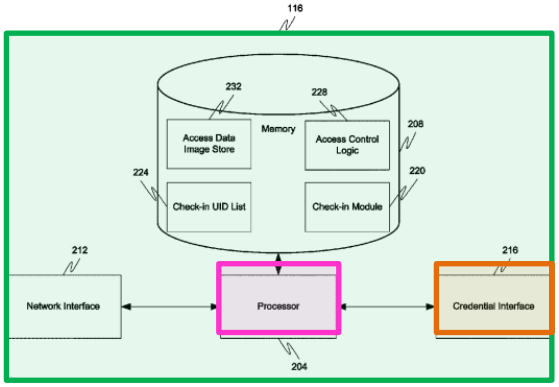
Id., FIG. 2 (annotated).

156. *Elfström* further discloses "[t]he processor 204 is enabled to communicate with the access control device" that is "an electronic lock, a magnetic lock, or an electric strike for a door." *Id.*, 6:6-16. Also "the access control logic 228 may facilitate … operations associated with permitting user access to an asset (e.g., unlocking a door, providing access to an account, etc.)." *Id.*, 6:66-7:3. *Elfström* discloses, "access control modules 116 may be provided at access points to various physical assets (e.g., rooms 112 a-N, corridors 120, elevators 124, safes within rooms, the multi-room facility itself, etc.)." *Id.*, 4:32-35.

3. [1B] "a communication module (17) connected to the processor, the processor is configured to receive a reservation certificate (5) presented by a portable terminal (4) through the communication module;"

157. *Elfström* renders obvious [1B] because *Elfström* discloses, "[t]o facilitate such security policies, the access control modules 116 may be adapted to communicate with access credentials 136 carried by users or guests of the multi-room facility via contactless and/or contact-based communication protocols. Such communications will allow the access control modules 116 to identify the access credential 136 presented thereto as well as determine access permissions for the holder of the access credential 136." *Id.*, 4:58-65. *Elfström* further discloses, "[t]he access control module 116, in accordance with at least one embodiment, comprises a credential communication interface 216 used to communicate back and forth with the credential 136." *Id.*, 5:50-53. As shown below, processor 204 is connected to credential communication interface 216.





Id., FIGS. 1, 2 (annotated).

158. *Elfström*'s access credential 136 is "an RFID card or device having similar functionality like a **mobile phone**, PDA, ebook reader, portable music player, or the like." *Id.*, 10:19-22 (emphasis added).

159. *Elfström*'s message from an access credential corresponds to the claimed "reservation certificate." *Elfström* discloses, "[t]he presentation of the credential 136 to the access control module 116 causes the credential 136 to transmit one or more messages to the access control module 116 which includes its credential identification number 324 and any other pertinent identification information (e.g., credential type)." *Id.*, 13:14-19.

4. [1C] "wherein, when a current reservation certificate that comprises an interval of a reservation is presented by the portable terminal,"

160. *Elfström* renders obvious [1C] because *Elfström* discloses its message from the credential (i.e., the claimed "reservation certificate") is on a credential device for use (the claimed "current reservation certificate"). *Elfström* explains, "a guest presents an access credential 136, such as an RFID card, at an access control module 116 enabled with a check-in module 220 (step 504)." *Elfström*, 11:54-56. *Elfström* discloses, "access data images that are capable of being written to a credential 136," and the "access data may include … guest stay duration … depending upon the user of the credential 136 and the reservations associated with the user of the credential 136." *Id.*, 8:7-9, 8:20-34. *Elfström* further discloses, "the access data encoded on the credential 136 may include … stay duration (identifying either a departure date or an expiration date for the access data)." *Id.*, 12:29-36, claim 20.

5. [1D] "the processor is configured to compare the interval of the reservation of the current reservation certificate to a current time accessible to the processor, determine the current time is within the interval of the reservation, and"

161. *Elfström* renders obvious [1D] because *Elfström* discloses, "[o]nce the credential identification number, and possibly credential type information, has been obtained the check-in module 220 searches the locally maintained check-in UID list

224 (step 512). The check-in module 220 compares the credential identification number and/or credential type information to the information maintained in the list 224 searching for matches (step 516).” *Elfström*, 11:63-12:3, FIG. 5 at block 512, 516. *Elfström* discloses, “access data images” of “a credential 136,” and the “access data may include … guest stay duration … depending upon the user of the credential 136 and the reservations associated with the user of the credential 136.” *Id.*, 8:7-9, 8:20-34. *Elfström* discloses, “[i]f permissions are confirmed, then the access control module 116 will release or otherwise make available such assets to the holder of the credential 136.” *Id.*, 12:14-16.

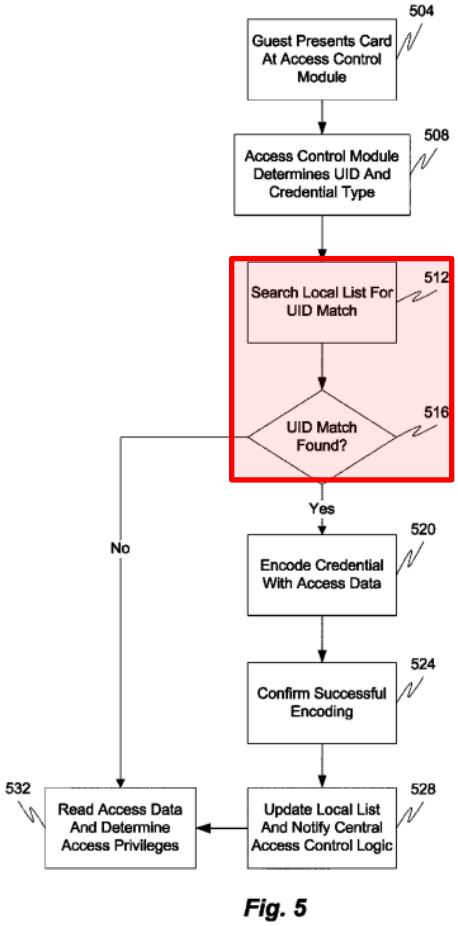


Fig. 5

Id., FIG. 5 (annotated).

162. *Elfström* does not explicitly disclose "compar[ing] the interval of the reservation of the current reservation certificate to a current time accessible to the processor," but *Woodard* does. *Woodard* discloses, "provid[ing] automatic access control to an electronic real estate lockbox utilizing showing appointment data maintained by a showing management system, whereby the showing appointment data is transmitted directly to the electronic lockbox and/or an electronic key device." *Woodard*, [0012]. *Woodard* discloses, "[t]he electronic lockbox 103 will

open only when the actual access time is within the scheduled showing appointment time." *Id.*, [0048]. *Woodard*'s "electronic lockbox 103 needs to include … an internal controller [and] an accurate timer which may be capable of synchronization with a time server." *Id.*, [0051]. *Woodard* further discloses, "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]. Access is granted when *Woodard*'s lockbox 103 determines the current date and time is within the time (interval) of the allowed access (reservation) when data (reservation certificate), including the temporal data describing the showing time, is able to allow access (current). In my opinion, a POSA would have been motivated to combine *Elfström* and *Woodard*, as discussed above in Section XIII.A.

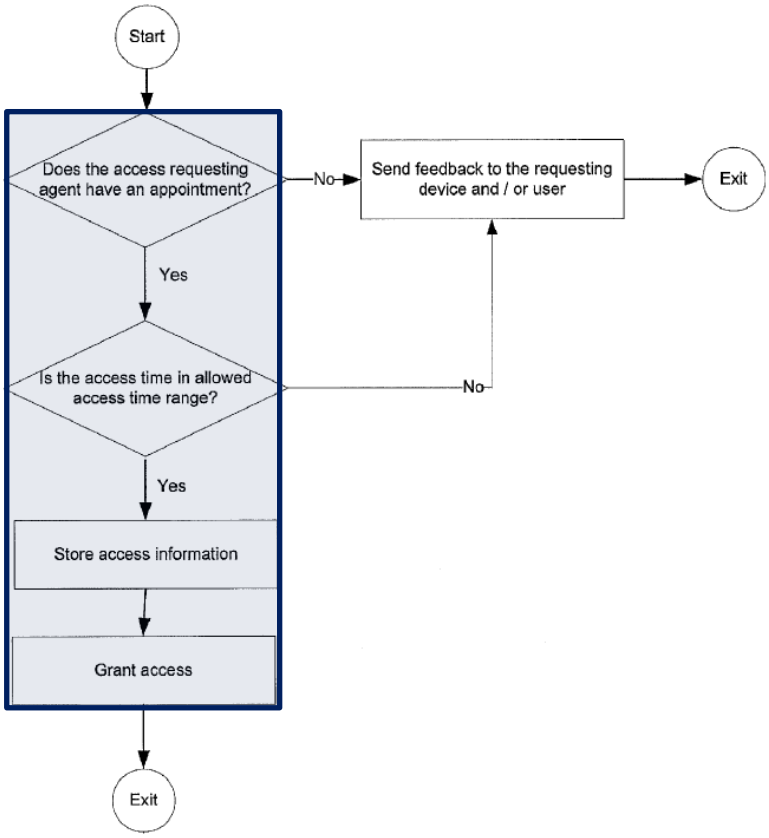
6. [1E] "activate the door lock to allow the portable terminal to unlock the door lock during the interval of the reservation."

163. *Elfström* renders obvious [1E] because *Elfström* discloses its access control module 116 can include processor 204 that controls an access control device including, "an electronic lock, a magnetic lock, or an electric strike for a door." *Elfström*, 5:60-61, 6:6-16. And "[t]hus, the access control logic 228 may facilitate … operations associated with permitting user access to an asset (e.g., unlocking a

door, providing access to an account, etc.)." *Id.*, 6:66-7:3. *Elfström* discloses, "[i]f permissions are confirmed, then the access control module 116 will release or otherwise make available such assets to the holder of the credential 136." *Id.*, 12:14-16. One of those permissions is "duration," as discussed above in Section XIII.B.4 for [1C]. *Id.*, 8:7-9, 8:20-34, 12:29-36, claim 20. *Elfström* permits user access because its "processor 204 actuates the access control device by sending a signal to the access control device … based on results of an access decision made by the processor 204." *Id.*, 6:16-20. As discussed above in Section XIII.B.5 for [1D], *Elfström* discloses "access data may include … guest stay duration," which a POSA would have understood to be one of the permissions checked as part of an access decision. *Id.*, 8:7-9, 8:20-34.

164. To the extent that *Elfström* does not disclose this limitation, *Woodard* does, as described above in Section XIII.B.5 for [1D], regarding *Woodard*'s disclosure of granting access, or in other words, allowing a lock to be unlocked, "within the scheduled showing appointment time," (*Woodard*, [0048], FIG. 9), corresponding to the claimed "during the interval of the reservation."

FIG. 9



Id., FIG. 9 (annotated).

165. In my opinion, a POSA would have been motivated to combine *Elfström* and *Woodard*, as discussed above in Section XIII.A.

C. Claim 2

1. [2A] The access device of claim 1 wherein the processor is configured to determine the current time is within the interval of the reservation by determining if the current time is within a start time of the interval of the reservation of the current reservation certificate and a predetermined duration and

166. *Elfström*, alone or in view of *Woodard*, renders obvious this claim. As discussed above in Section XIII.B.5 for [1D], *Woodard* discloses, "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." *Woodard*, [0065]. The "internal timer inside the electronic lockbox 103 … [ensures] that access is actually granted during the predetermine[d] showing times." *Id.*, [0068]. *Woodard* discloses, "[t]he time range may begin exactly at the scheduled start time of the showing appointment and end exactly at the scheduled end time of the showing appointment." *Id.*, [0012]. Further, in my view, a POSA would have understood *Woodard*'s interval corresponds to the claimed "predetermined duration." It is my opinion that a POSA would have further found it obvious that *Woodard*'s interval would be defined by the start time and the end time, and thus *Woodard*'s interval corresponds to the claimed "predetermined duration." Thus, *Woodard* discloses its "access data may include … guest stay duration" would be used from its disclosed start time to the

end time, also an end of the duration, as compared to the "current date and time," (*Woodard*, [0065]), and thus the access data would be current during this duration.

167. *Woodard* also discloses, "said showing time period comprises a start time and one of a duration and an end time," and *Woodard*'s data (certificate), or *Elfström*'s access credential (certificate) with data as disclosed by *Woodard*, is current from the start time up to the "duration." *Id.*, claim 2.

168. In my opinion, a POSA would have been motivated to combine *Elfström* and *Woodard*, as discussed above in Section XIII.A.

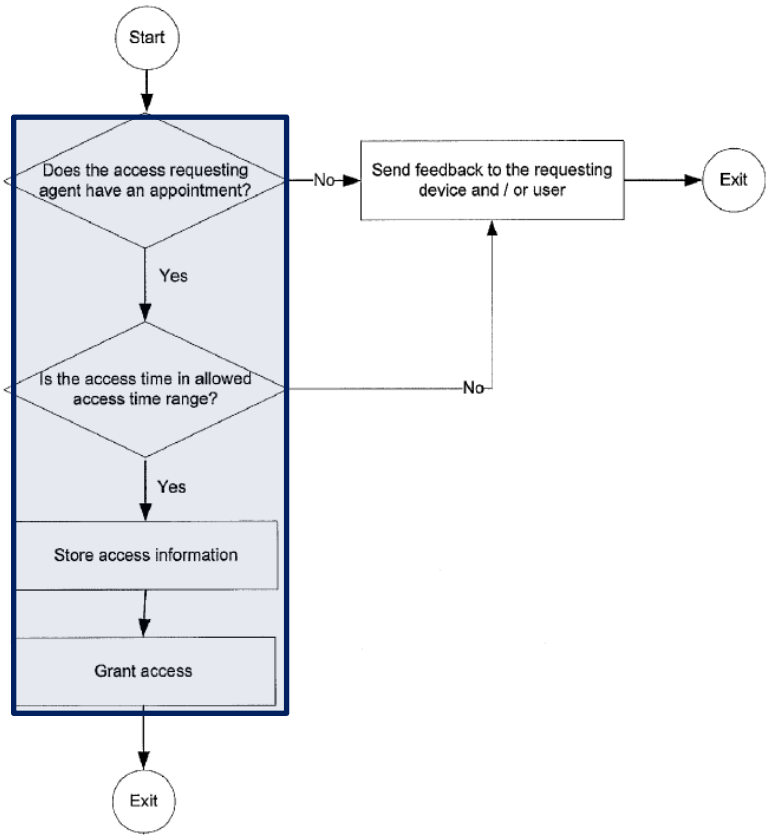
2. [2B] is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the predetermined duration.

169. *Elfström* renders obvious [2B] because *Elfström* discloses its access control module 116 can include processor 204 that controls an access control device including, "an electronic lock, a magnetic lock, or an electric strike for a door." *Elfström*, 5:60-61, 6:6-16. And "[t]hus, the access control logic 228 may facilitate … operations associated with permitting user access to an asset (e.g., unlocking a door, providing access to an account, etc.)." *Id.*, 6:66-7:3. *Elfström* discloses, "[i]f permissions are confirmed, then the access control module 116 will release or otherwise make available such assets to the holder of the credential 136." *Id.*, 12:14-16. Where one of those permissions is "duration," as discussed above in

Section XIII.B.4 for [1C], (*id.*, 8:7-9, 8:20-34, 12:29-36, claim 20), *Elfström* permits user access by its "processor 204 actuat[ing] the access control device by sending a signal to the access control device … based on results of an access decision made by the processor 204." *Id.*, 6:16-20. As discussed above in Section XIII.B.5 for [1D], *Elfström* similarly discloses "the access control module 116 will release or otherwise make available such assets to the holder of the credential 136." *Id.*, 12:14-16.

170. To the extent that *Elfström* does not disclose this limitation, *Woodard* does, as described above in Section XIII.C.1 for [2A], regarding *Woodard*'s disclosure of granting access, or in other words, allowing a lock to be unlocked, "within the scheduled showing appointment time," corresponding to the claimed "from the start time up to the predetermined duration." *Woodard*, [0048], FIG. 9.

FIG. 9



Id., FIG. 9 (annotated).

171. In my opinion, a POSA would have been motivated to combine *Elfström* and *Woodard*, as discussed above in Section XIII.A.

D. [Claim 3] The access device of claim 2 wherein the processor is configured to activate the door lock to allow the portable terminal

to unlock the door lock during the interval of the reservation from the start time up to the predetermined duration that is all day.

172. *Elfström*, alone or in view of *Woodard*, renders obvious this claim. As discussed above in Section XIII.B.6, *Elfström* discloses its access control module 116 can include processor 204 that controls an access control device including, "an electronic lock, a magnetic lock, or an electric strike for a door." *Elfström*, 5:60-61, 6:6-16. *Elfström* discloses, "[i]f permissions are confirmed, then the access control module 116 will release or otherwise make available such assets to the holder of the credential 136." *Id.*, 12:14-16. *Elfström* accomplishes this by "processor 204 actuat[ing] the access control device by sending a signal to the access control device … based on results of an access decision made by the processor 204." *Id.*, 6:16-20.

173. As discussed above in Section XIII.B.5, *Woodard* further discloses, "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." *Woodard*, [0065]. The "internal timer inside the electronic lockbox 103 … [ensures] that access is actually granted during the predetermine[d] showing times." *Id.*, [0068]. *Woodard* discloses, "[t]he time range may begin exactly at the scheduled start time of the showing appointment and end exactly at the scheduled end time of the showing appointment." *Id.*, [0012]. Based on my experience, a POSA would have understood

Woodard's interval corresponds to the claimed "predetermined duration." I believe a POSA would have further found it obvious that *Woodard*'s interval would be defined by the start time and the end time, and thus *Woodard*'s interval corresponds to the claimed "predetermined duration."

174. *Woodard* also discloses, "said showing time period comprises a start time and one of a duration and an end time." *Id.*, claim 2.

175. *Elfström* renders obvious the claimed "predetermined duration that is all day," because *Elfström* discloses controlling access in a "multi-room facility" that includes "guest stay duration." *Elfström*, 8:7-9, 8:20-34. I believe a POSA would have found it obvious that a "guest stay duration" in a hotel, as disclosed by *Elfström*, could include the claimed "all day," as staying for one day at a hotel is commonly known. U.S. Patent Pub. No. 2010/0293011, [0025] (referring to "available hotels having at least one day availability").

E. [Claim 4] The access device of claim 1 wherein the interval of the reservation of the current reservation certificate comprises a start time and a duration and the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the duration.

176. *Elfström*, alone or in view of *Woodard*, renders obvious this claim. Claim 4 is substantially similar to claim 2, except that claim 2 has additional limitations related to the "current time," as discussed above in Section X.D. For the

same reasons discussed above in Section XIII.C, *Elfström*, alone or in view of *Woodard*, renders obvious this claim.

F. [Claim 6] The access device of claim 1 wherein the interval of the reservation of the current reservation certificate comprises a start time and an end time.

177. *Elfström*, alone or in view of *Woodard*, renders obvious this claim. *Woodard* discloses, "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." *Woodard*, [0065]. The "internal timer inside the electronic lockbox 103 … [ensures] that access is actually granted during the predetermine[d] showing times." *Id.*, [0068]. *Woodard* discloses, "[t]he time range may begin exactly at the scheduled start time of the showing appointment and end exactly at the scheduled end time of the showing appointment." *Id.*, [0012].

G. [Claim 5] The access device of claim 6 wherein the processor is configured to activate the door lock to allow the portable terminal to unlock the door lock from the start time up to the end time.

178. *Elfström*, alone or in view of *Woodard*, renders obvious this claim. As discussed above for Section XIII.F for claim 6, *Woodard* discloses, "[t]he time range may begin exactly at the scheduled start time of the showing appointment and end exactly at the scheduled end time of the showing appointment." *Woodard*, [0012].

179. As discussed above in Section XIII.B.6, *Elfström* discloses its access control module 116 can include processor 204 that controls an access control device including, "an electronic lock, a magnetic lock, or an electric strike for a door." *Elfström*, 5:60-61, 6:6-16. *Elfström* discloses, "[i]f permissions are confirmed, then the access control module 116 will release or otherwise make available such assets to the holder of the credential 136." *Id.*, 12:14-16. *Elfström* accomplishes this by "the processor 204 actuat[ing] the access control device by sending a signal to the access control device … based on results of an access decision made by the processor 204." *Id.*, 6:16-20. The *Elfström-Woodard* combination renders obvious actuating *Elfström*'s access control device within *Woodard*'s start time and end time.

H. [Claim 9] The access device of claim 1 wherein the processor is configured to verify that the current reservation certificate is genuine.

180. *Elfström* renders obvious claim 9 because *Elfström* discloses "an instruction set (e.g., firmware, software, configuration data, and/or security data) is resident on the access control module 116 to support and control the functions of the access control module 116," (*Elfström*, 4:54-57), and that "[i]f a match of information is found in the locally maintained list 224, the access control module 116 allows the holder of the credential 136 to access the asset secured by the access control module (step 620)," (*Elfström*, 4:54-57), and it is my opinion that a POSA

would have found it obvious that secure messages are verified as genuine within *Elfström*'s secure access system 100. *Id.*, 3:51-54.

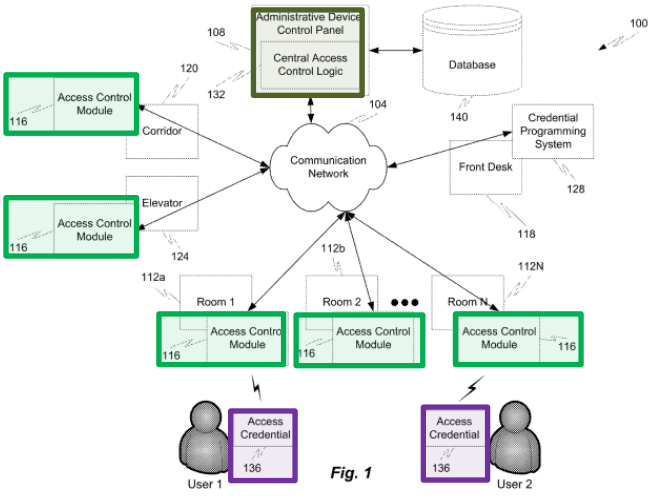
I. [Claim 10] The access device of claim 1 further comprising: an identification to which the processor has access, the identification corresponding to one of the access device and the door lock, wherein the processor is configured to determine that the current reservation certificate comprises data representative of the identification.

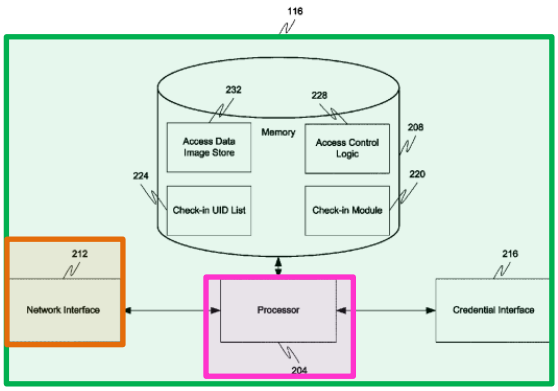
181. *Elfström* renders obvious claim 10 because *Elfström* discloses "the access control module 116 is enabled to read an identification number from the credential 136, confirm that the identification number from the credential 136 matches an identification number associated with a guest that has confirmed reservations and is allowed to check-in at a location other than the front desk 118, and encode the credential 136 with the appropriate access data in a minimal amount of time." *Elfström*, 7:36-42. *Elfström* discloses "access control module 116 parses the message(s) received from the credential 136 and determines the credential identification number 324 along with any other credential identification information (step 608) … [and] [i]f a match of information is found in the locally maintained list 224, the access control module 116 allows the holder of the credential 136 to access the asset secured by the access control module (step 620)." *Elfström*, 13:20-31.

J. [Claim 12] The access device of claim 1 wherein the processor has access to a server of the access system through the communication module and the processor is configured to report to the server

that the door lock was activated on the basis of the reservation certificate.

182. *Elfström*, alone or in view of *Woodard*, renders obvious this claim. *Elfström*'s administrative device 108 is a server because, "administrative device 108 may include access control logic 132 that is generally responsible for administering the secure access system 100 of the multi-room facility. In other words, the access control logic 132 of the administrative device 108 may provide a central location for administering the security of the multi-room facility." *Elfström*, 3:51-56. *Elfström* further discloses that its processor 204 of access control module 116 communicates with other components in the network, such as administrative device 108, through network interface 212. *Id.*, 6:9-12.





Id., FIGS. 1, 2 (annotated).

Elfström discloses its access control module 116 can include processor 204 that controls an access control device including, "an electronic lock, a magnetic lock, or an electric strike for a door." *Elfström*, 5:60-61, 6:6-16. *Elfström* discloses, "[i]f permissions are confirmed, then the access control module 116 will release or otherwise make available such assets to the holder of the credential 136." *Id.*, 12:14-16. *Elfström* accomplishes this by "processor 204 actuat[ing] the access control device by sending a signal to the access control device … based on results of an access decision made by the processor 204." *Id.*, 6:16-20.

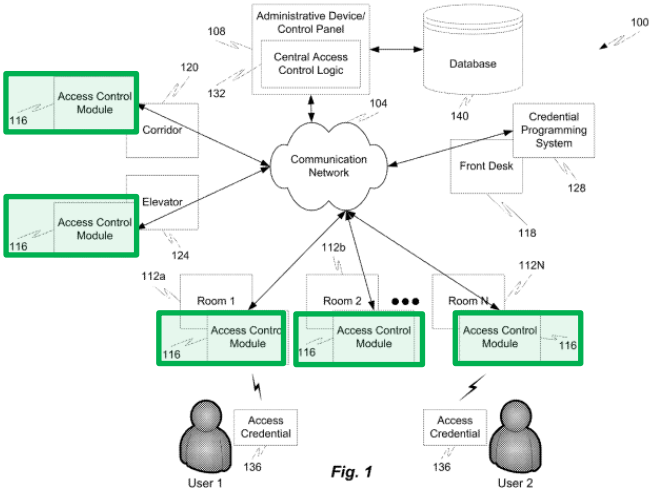
183. *Elfström* does not disclose that its access control module 116 reports that it was activated to administrative device 108, but *Woodard* does. *Woodard* discloses, "the lockbox access records stored in the electronic lockboxes are transmitted via a communications link between the electronic lockbox and the showing management system's servers coupled to the showing management system's database." *Woodard*, [0072]. It is my opinion that a POSA would have found it obvious to implement *Woodard*'s lockbox access records stored in the lockboxes and those records being reported to the system's servers via a communications link into *Elfström*'s access control module 116 and administrative device 108. In my opinion, as discussed above, a POSA would have been motivated to combine *Elfström* and *Woodard* in Section XIII.A.

K. Claim 13

184. *Elfström* renders obvious claim 13.

1. [13p] "A method for use by an access device in an access control system, the method comprising:"

185. *Elfström* renders obvious [13p] because *Elfström* discloses, "Methods, systems, and devices for controlling access within a multi-facility room are provided." *Elfström*, Abstract. *Elfström* discloses its access control system 100 can include "access control modules 116 [] adapted to communicate with access credentials 136 carried by users or guests of the multi-room facility." *Id.*, 4:58-65. *Elfström* further discloses its access control module 116 can include a processor that controls an access control device including, "an electronic lock, a magnetic lock, or an electric strike for a door." *Id.*, 5:60-61, 6:6-16.



Id., FIG. 1 (annotated).

2. [13A] "accepting, by a processor"

186. *Elfström* in view of *Woodard* renders obvious [13A], as explained for [1A] in Section XIII.B.2.

3. [13B] "through a communication module, a reservation certificate… presented with a portable terminal;"

187. *Elfström* in view of *Woodard* renders obvious [13B], as explained for [1B] in Section XIII.B.3.

4. [13C] "a reservation certificate that comprises an interval of a reservation"

188. *Elfström* in view of *Woodard* renders obvious [13C], as explained for [1C] in Section XIII.B.4.

5. [13D] "determining, by the processor, that the reservation certificate presented by the portable terminal is current by comparing the interval of the reservation to a current time accessible to the processor and determining that the current time is within the interval of the reservation; and activating, by the processor on the basis of the reservation certificate being current"

189. *Elfström* in view of *Woodard* renders obvious [13D], as explained for [1D] in Section XIII.B.5. *Elfström* accomplishes "activating" by "processor 204 actuat[ing] the access control device by sending a signal to the access control device … based on results of an access decision made by the processor 204." *Elfström*, 6:16-20.

6. [13E] "activating… a door lock to allow the portable terminal to unlock the door lock during the interval of the reservation."

190. *Elfström* in view of *Woodard* renders obvious [13E], as explained for [1E] in Section XIII.B.6.

L. [Claim 14] The method of claim 13 wherein determining that the current time is within the interval of the reservation comprises determining that the current time is within a start time of the interval of the reservation and a predetermined duration and wherein the certificate is current from the start time up to the predetermined duration.

191. *Elfström*, alone or in view of *Woodard*, renders obvious this claim. *Elfström* renders obvious claim 14, as explained for [2A] in Section XIII.C.1. Regarding the limitation, "wherein the certificate is current from the start time up to the predetermined duration," *Woodard* discloses its "access data may include … guest stay duration" would be used from its disclosed start time to the end time, also an end of the duration, as compared to the "current date and time," (*Woodard*, [0065]), and thus the access data would be current during this duration. *Woodard* further discloses, "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]. *Woodard* also teaches its "showing time period comprises a start time

and one of a duration and an end time," thus disclosing that its certificate is current from the start time to the "duration." *Woodard*, claim 2.

M. [Claim 15] The method of claim 14 wherein the predetermined duration is all day.

192. *Elfström* renders obvious claim 15, as explained for claim 3 in Section XIII.D.

N. [Claim 16] The method of claim 13 wherein the interval of the reservation of the reservation certificate further comprises a start time and a duration and the reservation certificate is current from the start time up to the duration.

193. *Elfström* renders obvious claim 16, as explained for claim 4 in Section XIII.E.

O. [Claim 17] The method of claim 18 wherein the reservation certificate is current from the start time up to the end time.

194. *Elfström* in view of *Woodard* renders obvious this claim. *Woodard* discloses, "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." *Woodard*, [0065]. The "internal timer inside the electronic lockbox 103 … [ensures] that access is actually granted during the predetermine[d] showing times." *Id.*, [0068]. *Woodard* discloses, "[t]he time range may begin exactly at the scheduled start time of the

showing appointment and end exactly at the scheduled end time of the showing appointment." *Id.*, [0012].

195. In my experience, a POSA would have found it obvious that *Woodard*'s disclosure of the time range including both a start time and an end time in the appointment data renders obvious the claimed "the reservation certificate is current from the start time up to the end time" because *Woodard*'s temporary access, like *Elfström*'s guest stay duration, begins at a starting point and ends at an end point. By providing meaningful start and end times, access can only be used between the start and end times. *Elfström*, Abstract; *Woodard*, Abstract. In my opinion, a POSA would have been motivated to combine *Elfström* and *Woodard*, as discussed above in Section XII.A.

P. [Claim 18] The method of claim 13 wherein the interval of the reservation comprises a start time and an end time.

196. *Elfström* renders obvious claim 18, as explained for claim 6 in Section XIII.F.

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

197. *Elfström* in view of *Woodard* renders obvious claim 21, as explained for claim 9 in Section XIII.H. As to c), *Elfström* discloses its access control module

116 can include processor 204 that controls an access control device including, "an electronic lock, a magnetic lock, or an electric strike for a door." *Elfström*, 5:60-61, 6:6-16. *Elfström* discloses, "[i]f permissions are confirmed, then the access control module 116 will release or otherwise make available such assets to the holder of the credential 136," (*id.*, 12:14-16), such as determining that identification information matches the locally maintained list. *Id.*, 13:20-31. *Elfström* accomplishes this by "processor 204 actuat[ing] the access control device by sending a signal to the access control device … based on results of an access decision made by the processor 204." *Id.*, 6:16-20.

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

198. *Elfström* renders obvious claim 22, as explained for claim 10 in Section XIII.I. As to c), *Elfström* discloses its access control module 116 can include processor 204 that controls an access control device including, "an electronic lock, a magnetic lock, or an electric strike for a door." *Elfström*, 5:60-61, 6:6-16. *Elfström* discloses, "[i]f permissions are confirmed, then the access control module 116 will release or otherwise make available such assets to the holder of the credential 136,"

(*id.*, 12:14-16), such as determining that identification information matches the locally maintained list. *Id.*, 13:20-31. *Elfström* accomplishes this by "processor 204 actuat[ing] the access control device by sending a signal to the access control device … based on results of an access decision made by the processor 204." *Id.*, 6:16-20.

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

199. *Elfström* in view of *Woodard* renders obvious claim 24, as explained for claim 12 in Section XIII.J. As to d), *Elfström* discloses its access control module 116 can include processor 204 that controls an access control device including, "an electronic lock, a magnetic lock, or an electric strike for a door." *Elfström*, 5:60-61, 6:6-16. *Elfström* discloses, "[i]f permissions are confirmed, then the access control module 116 will release or otherwise make available such assets to the holder of the credential 136," (*id.*, 12:14-16), such as determining that identification information matches the locally maintained list. *Id.*, 13:20-31. *Elfström* accomplishes this by "processor 204 actuat[ing] the access control device by sending a signal to the access control device … based on results of an access decision made by the processor 204." *Id.*, 6:16-20.

XIV. GROUND 5: CLAIMS 7, 8, 11, 19, 20, AND 23 ARE UNPATENTABLE OVER *ELFSTRÖM* IN VIEW OF *WOODARD* AND *DEBRY*

A. Motivation to Combine *Elfström*, *Woodard*, and *DeBry*

200. In my opinion, a POSA would have been motivated to implement *Woodard*'s timing management system into *Elfström*'s access control system for the reasons explained in Section XIII.A. As explained in Section IX.B, claims 7, 8, 11, 19, 20, and 23 further require encryption elements that are not expressly disclosed by *Elfström* and *Woodard*.

201. However, I believe a POSA would have been motivated to implement *DeBry*'s encryption methods into *Elfström*'s messages because *DeBry* discloses, "[s]ome files must be encrypted at the sending end and decrypted at the receiving end to ensure that the file contents are not intercepted by an unauthorized entity during the transmission." *DeBry*, 1:54-57. *Elfström* discloses "an encryption key used … by the multi-room facility." *Elfström*, 8:22-24. While *Elfström* does not expressly disclose specific methods of encryption, a POSA would have understood that known methods of cryptography could be used. For example, *DeBry* discloses the known systems of both convention or symmetric cryptography and public key cryptography. *DeBry*, 1:62-2:62. It is my further opinion that a POSA would have found it obvious to incorporate these known systems of encrypting and decrypting using a public/private key pair or a symmetric key in the way described by *DeBry*

into *Elfström*'s encrypting and decrypting system because *DeBry*'s system would have been an obvious existing use of encryption. It is thus my opinion that a POSA would have incorporated *DeBry*'s encryption methods to avoid unauthorized interceptions. Further, to meet *Elfström*'s goals of secure communication managed by administrative device 108, in my opinion, a POSA would have been motivated to implement *DeBry*'s method of ensuring authorized users through encryption.

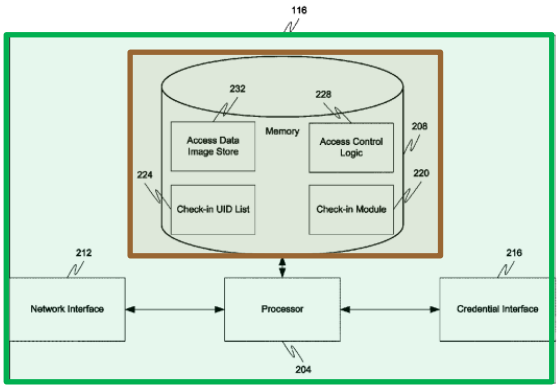
202. In my experience, a POSA would have had reasonable expectations of success combining *DeBry* and *Elfström* because *DeBry*'s encryption methods are known methods of encryption communications between one device to another. For instance, *DeBry* discloses a client system communicating with a printer, (*DeBry*, 5:34-36), and *Elfström* discloses an access credential that can be a mobile phone, (*Elfström*, 10:19-22), communicating with an access control module to actuate a door lock or other lock mechanism to open a lock. *Id.*, 5:60-61, 6:6-16.

B. Claim 7

1. [7A] The access device of claim 1 further comprising: a memory to which the processor has access, the memory is configured to comprise a public key for a server of the access system configured to issue the current reservation certificate;

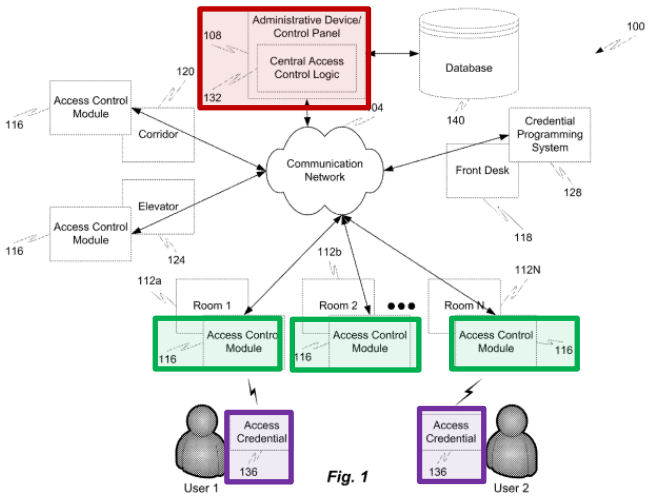
203. *Elfström* in combination with *Woodard* and *DeBry* renders obvious [7A] because *Elfström* discloses a memory coupled to a processor and *DeBry* further discloses a specific encryption method using a public key.

204. *Elfström* renders obvious "a memory to which the processor has access," because *Elfström* discloses "the memory 208 and the processor 204 are designed to utilize known security features to prevent unauthorized access to the contents of the memory 208 such as side channel analysis and the like." *Elfström*, 8:42-45. *Elfström* also discloses, "an instruction set (e.g., firmware, software, configuration data, and/or security data) is resident on the access control module 116 to support and control the functions of the access control module 116." *Id.*, 4:54-57.



Id., FIG. 2 (annotated).

205. *Elfström* renders obvious, "a server of the access system configured to issue the current reservation certificate," because *Elfström* discloses "[t]he administrative device 108 may include access control logic 132 that is generally responsible for administering the secure access system 100 of the multi-room facility. In other words, the access control logic 132 of the administrative device 108 may provide a central location for administering the security of the multi-room facility." *Id.*, 3:51-56.



Id., FIG. 1 (annotated).

206. While *Elfström* discloses encryption, it does not expressly disclose a public key, but *DeBry* does. *DeBry* discloses, "[i]n a public key system, it is possible to communicate privately without transmitting any secret key. For example, the

encryption key for each user is made public by being distributed or published." *DeBry*, 2:46-49. In my opinion, a POSA would have found it obvious that *Elfström*'s memory 208 of FIG. 1 would be used to store a public key that is "distributed or published" in a public key system because *Elfström*'s memory is "designed to utilize known security features." *Elfström*, 8:42-45. It is further my opinion, as discussed above in Section XIV.A, that a POSA would have been motivated to combine *DeBry* and the *Elfström-Woodard* combination.

2. [7B] wherein at least a portion of the current reservation certificate is encrypted by the server using a private key and the processor is configured to verify that the current reservation certificate is genuine by decrypting the portion with the public key.

207. *Elfström* in view of *DeBry* renders obvious [7B] because *DeBry* discloses a specific encryption method using both public and private keys.

208. *DeBry* discloses "a user who has made public a public key can digitally sign a message by encrypting the message, or a hash of it, with the user's private key before transmitting the message. Recipients of the message can verify the message or signature by decrypting it with the sender's public encryption key." *DeBry*, 3:11-16. Further, *DeBry* discloses, "[a]nyone who has the sender's public encryption key can read the message or signature. Any such recipient is assured of the authentication of the creator of the message …." *Id.*, 3:20-24. In my experience, a POSA would

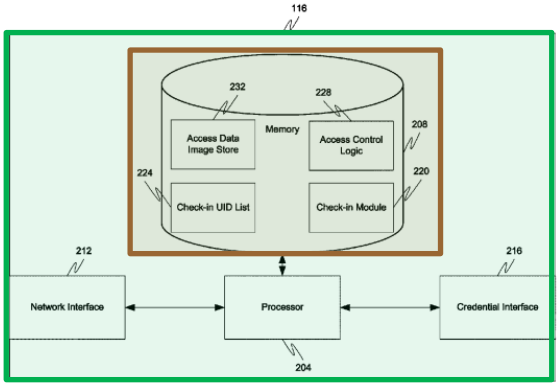
have found it obvious to incorporate a known system of encrypting and decrypting using a public/private key pair in the way described by *DeBry* using *Elfström*'s secure message system because *DeBry*'s system would have been an obvious existing use of keeping a message secure and private. In my opinion, as discussed above in Section XIV.A, a POSA would have been motivated to combine *DeBry* and the *Elfström-Woodard* combination.

C. Claim 8

1. [8A] The access device of claim 1 further comprising: a memory to which the processor has access, the memory is configured to comprise a symmetric key:

209. *Elfström* in combination with *Woodard* and *DeBry* renders obvious [8A].

210. *Elfström* renders obvious "a memory to which the processor has access," because *Elfström* discloses "the memory 208 and the processor 204 are designed to utilize known security features to prevent unauthorized access to the contents of the memory 208 such as side channel analysis and the like." *Elfström*, 8:42-45. *Elfström* also discloses, "an instruction set (e.g., firmware, software, configuration data, and/or security data) is resident on the access control module 116 to support and control the functions of the access control module 116." *Id.*, 4:54-57.



Id., FIG. 2 (annotated).

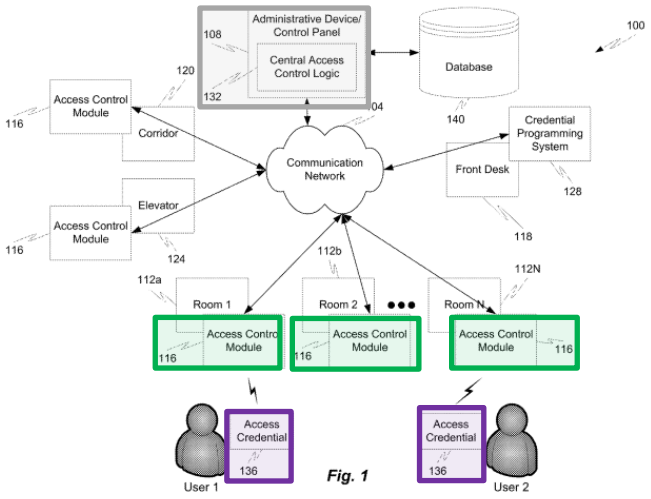
211. While *Elfström* discloses encryption, it does not expressly disclose a symmetrical key, but *DeBry* does. *DeBry* discloses "[c]onventional cryptography, or in other words traditional symmetric cryptography, is used to maintain the privacy of the information contents. Conventional cryptography requires that the sender and receiver of an encrypted message share the same secret key. The same key is used to both scramble (encrypt) and unscramble (decrypt) information." *DeBry*, 1:63-2:1. Symmetric keys are a common way to pass encrypted information, as discussed above in Section XIV.A, and a POSA would have been able to choose between known encryption systems based on the devices being used and the available memory and processing speed at each device. It is my experience that a POSA would have found it obvious that a decryption key, corresponding to a message encrypted with a symmetric key, would be stored in *Elfström*'s memory 208 for its access device 116 so it could receive encrypted messages from credential 136 and/or

administration device 108 to "maintain privacy," (*id.*), and "utilize known security features." *Elfström*, 8:42-45. In my opinion, as discussed above in Section XIV.A, a POSA would have been motivated to combine *DeBry* and the *Elfström-Woodard* combination.

2. [8B] wherein at least a portion of the current reservation certificate is encrypted by a server of the access system configured to use the symmetric key and the processor is configured to verify that the current reservation certificate is genuine by decrypting the portion with the symmetric key.

212. *Elfström* in combination with *Woodard* and *DeBry* renders obvious [8B]

213. *Elfström*'s use of encryption would occur with *Elfström*'s messages from credential 136 and/or administration device 108 to access control module 116. *Elfström*, 5:23-26, 13:14-19. *Elfström*'s administration device 108, "which may also be referred to as a control panel," includes "access control logic 132 that is generally responsible for administering the secure access system 100 of the multi-room facility. In other words, the access control logic 132 of the administrative device 108 may provide a central location for administering the security of the multi-room facility." *Id.*, 3:46-56.



Elfström, FIG. 1 (annotated).

214. *Elfström* does not disclose that its administrative device 108 would encrypt the message or that its access control module 116 would decrypt the message, but it would have been obvious in view of *DeBry* to encrypt the message at the administrative device 108 and to decrypt it at the recipient, the access control module 116. *DeBry* discloses, "[a]n authorized user must have the key that was used to encipher the data in order to decipher it. Unauthorized recipients of the ciphered information content who may know the DES algorithm but who do not know the key cannot decipher the information content." *DeBry*, 2:5-10. Accordingly, meeting *Elfström*'s goals of secure communication managed by administrative device 108 in view of *DeBry*'s method of ensuring authorized users renders obvious this claim

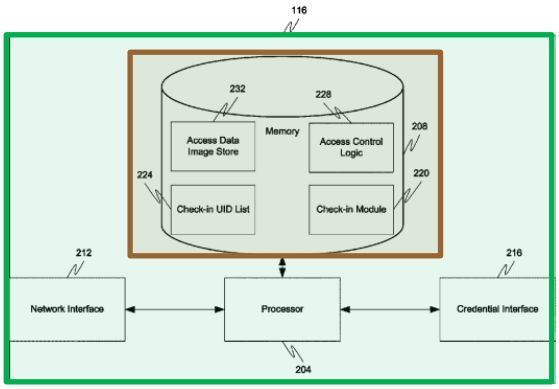
limitation. In my opinion, a POSA would have been motivated to combine *DeBry* and the *Elfström-Woodard* combination, as disclosed above in Section XIV.A.

D. Claim 11

1. [11A] The access device of claim 1 further comprising: a memory to which the processor has access, the memory is configured to comprise a private key of the access device;

215. *Elfström* in combination with *Woodard* and *DeBry* renders obvious [11A].

216. *Elfström* renders obvious "a memory to which the processor has access," because *Elfström* discloses "the memory 208 and the processor 204 are designed to utilize known security features to prevent unauthorized access to the contents of the memory 208 such as side channel analysis and the like." *Elfström*, 8:42-45. *Elfström* also discloses, "an instruction set (e.g., firmware, software, configuration data, and/or security data) is resident on the access control module 116 to support and control the functions of the access control module 116." *Id.*, 4:54-57.



Id., FIG. 2 (annotated).

217. *Elfström* does not disclose a symmetrical key, but *DeBry* does. *DeBry* discloses "[c]onventional cryptography, or in other words traditional symmetric cryptography, is used to maintain the privacy of the information contents. Conventional cryptography requires that the sender and receiver of an encrypted message share the same secret key. The same key is used to both scramble (encrypt) and unscramble (decrypt) information." *DeBry*, 1:63-2:1. In my experience, a POSA would have found it obvious that a decryption key, corresponding to a message encrypted with a symmetric key, would be stored in *Elfström*'s memory 208 for its access device 116 so it could receive encrypted messages from credential 136 and/or administration device 108 to "maintain privacy," (*id.*), and "utilize known security features." *Elfström*, 8:42-45.

2. [11B] wherein at least a portion of the current reservation certificate is encrypted by a server of the access system configured to use a corresponding public key for the access device and the processor is configured to decrypt the portion with the private key.

218. *Elfström* in combination with *Woodard* and *DeBry* renders obvious [11B].

219. *DeBry* discloses, "[i]n a public key system, it is possible to communicate privately without transmitting any secret key. For example, the

encryption key for each user is made public by being distributed or published. Anyone desiring to communicate in private with a recipient merely encrypts the message under the recipient's public key. Only the recipient, who retains the secret decrypting key, is able to decipher the transmitted message." *DeBry*, 2:46-53. It is my opinion that a POSA would have found it obvious to incorporate a known system of encrypting and decrypting using a public/private key pair in the way described by *DeBry* into *Elfström*'s secure messaging between its administrative device 108 and its access control module 116 because *DeBry*'s system would have been an obvious existing use of encryption. In my opinion, a POSA would have been motivated to combine *DeBry* and the *Elfström-Woodard* combination, as disclosed above in Section XIV.A.

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

220. *Elfström* in view of *Woodard* and *DeBry* renders obvious claim 19, as explained for claim 7 in Section XIV.B. As to d), *Elfström* discloses its access control module 116 can include processor 204 that controls an access control device including, "an electronic lock, a magnetic lock, or an electric strike for a door."

Elfström, 5:60-61, 6:6-16. *Elfström* discloses, "[i]f permissions are confirmed, then the access control module 116 will release or otherwise make available such assets to the holder of the credential 136," (*id.*, 12:14-16), such as determining that identification information matches the locally maintained list. *Id.*, 13:20-31. *Elfström* accomplishes this by "processor 204 actuat[ing] the access control device by sending a signal to the access control device … based on results of an access decision made by the processor 204." *Id.*, 6:16-20.

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

221. *Elfström* in view of *Woodard* and *DeBry* renders obvious claim 20, as explained for claim 8 in Section XIV.C. As to c), *Elfström* discloses its access control module 116 can include processor 204 that controls an access control device including, "an electronic lock, a magnetic lock, or an electric strike for a door." *Elfström*, 5:60-61, 6:6-16. *Elfström* discloses, "[i]f permissions are confirmed, then the access control module 116 will release or otherwise make available such assets to the holder of the credential 136," (*id.*, 12:14-16), such as determining that identification information matches the locally maintained list. *Id.*, 13:20-31.

Elfström accomplishes this by its "processor 204 actuat[ing] the access control device by sending a signal to the access control device … based on results of an access decision made by the processor 204." *Id.*, 6:16-20.

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

222. *Elfström* in view of *Woodard* and *DeBry* renders obvious claim 23, as explained for claim 11 in Section XIV.D.

XV. GROUND 6: CLAIMS 3 AND 15 ARE RENDERED OBVIOUS BY *ELFSTRÖM* IN VIEW OF *WOODARD* AND *MICALI*

A. Motivation to Combine *Elfström*, *Woodard*, and *Micali*

223. In my opinion, a POSA would have been motivated to implement *Woodard*'s timing management system into *Elfström*'s access control system for the reasons explained in Section XIII.A. As explained in Section IX.B, claims 3 and 15 further require the reservation certificate to be valid for an interval of a predetermined duration that is all day.

224. However, it is my experience that a POSA would have been motivated to implement *Micali*'s duration of a certificate into *Elfström*'s certificates because *Micali* discloses, "[c]ontrolling physical access includes reviewing real time credentials, where the real time credentials include a first part that is fixed and a

second part that is modified on a periodic basis, where the second part provides a proof that the real time credentials are current, verifying validity of the real time credentials by performing an operation on the second part and comparing the result to the first part, and allowing physical access only if the real time credentials are verified as valid." *Micali*, 6:21-29. *Micali* also discloses the same goal of "security … without incurring excessive costs and sacrificing convenience" for "[s]mart doors" capable of being unlocked through "contactless devices." *Micali*, 7:40-67. Thus, in my opinion, a POSA would have incorporated *Micali*'s duration of a certificate to improve security for smart doors and ensure credentials are valid.

225. In my experience, a POSA would have had reasonable expectations of success combining *Micali* and the *Elfström-Woodard* combination because *Micali*'s certificates are carried by contactless devices or wireless devices used to unlock doors, (*id.*, 8:13-16), just like *Woodard*'s key device and *Elfström*'s credentials 136. Further, *Micali* describes known methods of use of digital certificates with a unique serial number, (*id.*, 4:62-63, 9:45-47), such as *Elfström*'s messages that include a unique identifier. *Elfström*, 8:25-27.

B. [Claim 3] The access device of claim 2 wherein the processor is configured to activate the door lock to allow the portable terminal

to unlock the door lock during the interval of the reservation from the start time up to the predetermined duration that is all day.

226. *Elfström* in combination with *Woodard* and *Micali* renders obvious this claim. As explained in Section XIII.B.6 for [1E], *Elfström* discloses its access control module 116 can include processor 204 that controls an access control device including, "an electronic lock, a magnetic lock, or an electric strike for a door." *Elfström*, 5:60-61, 6:6-16. *Elfström* discloses, "[i]f permissions are confirmed, then the access control module 116 will release or otherwise make available such assets to the holder of the credential 136." *Id.*, 12:14-16. *Elfström* accomplishes this by "the processor 204 actuat[ing] the access control device by sending a signal to the access control device … based on results of an access decision made by the processor 204." *Id.*, 6:16-20.

227. As discussed above in Section XIII.C.1, *Woodard* further discloses, "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." *Woodard*, [0065]. The "internal timer inside the electronic lockbox 103 … [ensures] that access is actually granted during the predetermine[d] showing times." *Id.*, [0068]. *Woodard* discloses, "[t]he time range may begin exactly at the scheduled start time of the showing appointment and end exactly at the scheduled end time of the showing

appointment." *Id.*, [0012]. Based on my experience, a POSA would have understood *Woodard*'s interval corresponds to the claimed "predetermined duration." It is my opinion that a POSA would have further found it obvious that *Woodard*'s interval would be defined by the start time and the end time, and thus *Woodard*'s interval corresponds to the claimed "predetermined duration." *Woodard* also discloses, "said showing time period comprises a start time and one of a duration and an end time." *Id.*, claim 2.

228. To the extent that *Elfström* and *Woodard* do not disclose a "predetermined duration that is all day," my opinion is that *Micali* renders this obvious because *Micali* discloses "controlling physical access through a digital certificate validation process that works with standard certificate formats (e.g., X.509v3) and that enables a certifying authority (CA) to prove the validity status of each certificate C at any time interval (e.g., every day, hour, or minute) starting with C's issue date, D_1." *Micali*, 15:57-62. Based on my experience, a POSA would have understood that a certificate could be issued for a day, as disclosed by *Micali*. Indeed, *Micali* provides an example where "every morning—e.g., at midnight—a wireless user may receive a 20-byte proof of the validity of his certificate for the remainder of the day," (*id.*, 18:17-19), corresponding to the claimed "reservation from the start time up to the predetermined duration that is all day." In my opinion, a POSA would

have been motivated to combine *Micali* and the *Elfström-Woodard* combination, as disclosed above in Section XV.A.

C. [Claim 15] The method of claim 14 wherein the predetermined duration is all day.

229. *Elfström* combination with *Woodard* and *Micali* renders obvious claim 15, as explained for claim 3 in Section XV.B.

XVI. CONCLUSION

230. 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 22nd day of May 2023, in Windsor, MA.

Respectfully submitted,

