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 C1

Case No. IPR2023-00815

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

LIST OF EXHIBITS

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-1003	Declaration of Benjamin B. Bederson
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-1013	Reserved.
Ex-1014	U.S. Patent Publication No. 2010/0293011 A1 to Lebreton et al.
Ex-1015	Reserved.
Ex-1016	Complaint, *Liberty Access Technologies Licensing LLC v. ASSA ABLOY AB*, 2:22-cv-00507, Dkt. 1 (E.D. Tex. Dec. 30, 2022).

Ex-1017	Complaint, *ASSA ABLOY Global Solutions, Inc. v. Liberty Access Technologies Licensing LLC*, 1:23-cv-00756, Dkt. 1 (N.D. Ill. Feb. 7, 2023).

I. PRELIMINARY STATEMENT

Petitioners request *inter partes* review of claims 1-24 of U.S. Patent No. 9,373,205 C1 (Ex-1001, Ex-1010),[1] assigned to Urban Intel Inc. ("Urban").

The '205 patent describes allowing a terminal (smartphone) to activate a door lock when it receives a current reservation certificate. Ex-1001, Abstract. But this concept of unlocking a door using a smartphone based on a current reservation was well known before the '205 patent. It was, in fact, invented by Petitioners.

The two primary references in this Petition, *Knutsson* and *Elfström*, both owned by Petitioner ASSA ABLOY Global Solutions, Inc. directly or through its related entity, Phoniro AB, disclose processors with communication modules configured to receive a reservation certificate from a smartphone terminal, determine whether the reservation certificate is current, and activate the door lock if it is—the exact process claimed by the '205 patent.

Alone or when combined in routine, predictable ways with the other secondary references herein, *Knutsson* and *Elfström*—neither considered by the USPTO during prosecution of the '205 patent—render all claims of the '205 patent obvious.

[1] An ex parte reexamination certificate issued that modified claims 1-14 and 16-18 of the '205 patent, but not claims 15 and 19-24. Ex-1001, 14-17.

II. STATEMENT OF PRECISE RELIEF REQUESTED

Petitioners respectfully request review under 35 U.S.C. § 311 of claims 1-24 of the ’205 patent over the following references and grounds.

Reference	**Publication/Filing Date**	**Relevant Prior Art Pre-AIA Statute[2]**
WO Publication WO2008/076074 A1 (“*Knutsson*”)	Published June 26, 2008	35 U.S.C. § 102(b)
U.S. Patent No. 6,385,728 B1 (“*DeBry*”)	Published May 7, 2002	35 U.S.C. § 102(b)
U.S. Patent No. 2009/0219133 A1 (“*Woodard*”)	Published September 3, 2009	35 U.S.C. § 102(a), (e)
U.S. Patent No. 8,730,004 B2 (“*Elfström*”)	Filed January 29, 2010	35 U.S.C. § 102(a), (e)
U.S. Patent No. 7,353,396 B2 (“*Micali*”)	Published April 1, 2008	35 U.S.C. § 102(b)

Ground	**References**	**Basis**	**Challenged Claim(s)**
1	*Knutsson*	§ 103	1-6, 8-10, 13-18, 20-22
2	*Knutsson*, *DeBry*	§ 103	7, 11, 19, 23
3	*Knutsson*, *Woodard*	§ 103	12, 24

[2] Petitioners list certain statutes for convenience, but Petitioners also rely on any applicable pre-AIA 35 U.S.C. § 102 statute.

4	*Elfström, Woodard*	§ 103	1-6, 9-10, 12-18, 21-22, 24
5	*Elfström, Woodard, DeBry*	§ 103	7, 8, 11, 19, 20, 23
6	*Elfström, Woodard, Micali*	§ 103	3, 15

III. OVERVIEW OF THE COMBINATIONS

The ’205 patent, filed on January 23, 2015, claims priority to U.S. Provisional Application No. 61/309,813, filed March 2, 2010. March 2, 2010, is thus the ’205 patent’s earliest possible priority date.

The ’205 patent describes a smartphone or terminal activating a door lock when it receives a reservation certificate presented by the terminal through a communication module. Ex-1001, Abstract. Representative 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**
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.**[3]

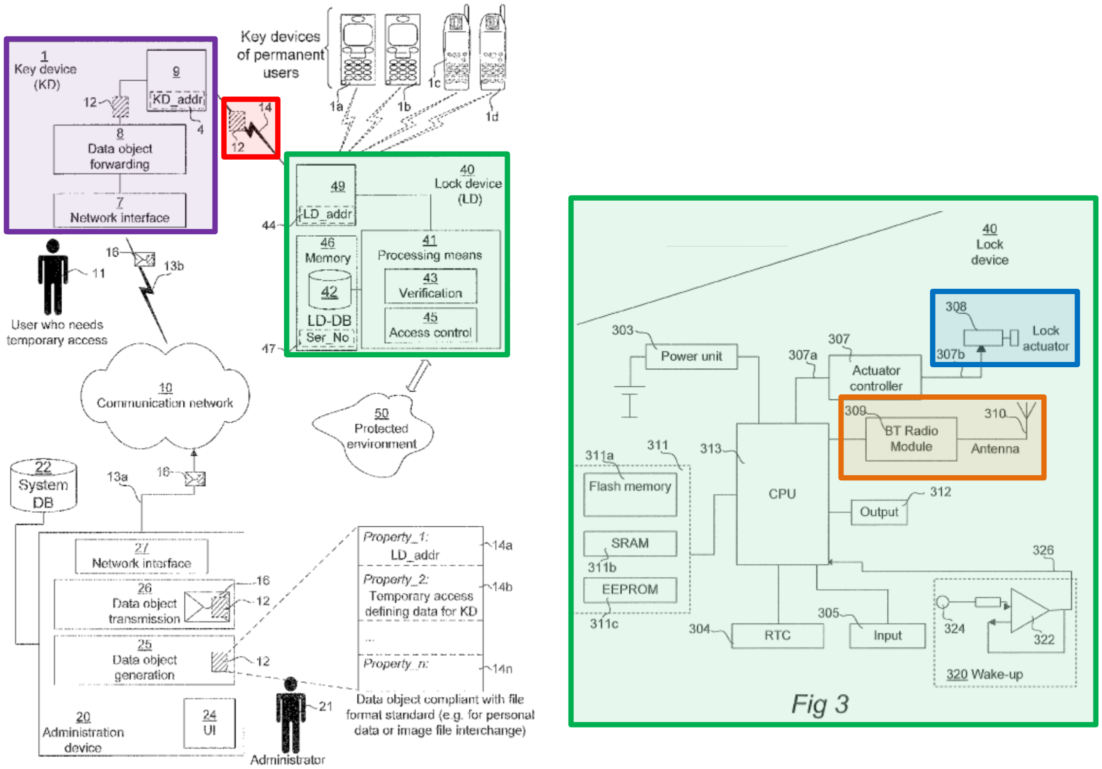
Knutsson and *Elfström*, the primary Petitioner-owned references relied on, each disclose processors with communication modules receiving a reservation certification from a PDA or mobile phone, determining whether the reservation certificate is current, and activating the door lock if so, like those claimed by the '205 patent.

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

Knutsson discloses or renders obvious all limitations of the independent claims and many dependent claims of the '205 patent (**Ground 1**). Ex-1003, ¶53. *Knutsson* discloses "[a]n access control system … to provide temporary access for a wireless key device to a lock device." *Knutsson*, Abstract. *Knutsson*'s "lock

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

device 40 … ha[s] a controllable lock actuator configured to unlock the lock mechanism upon detection and successful authorization of the key device 1." *Id.*, 10:24-30. *Knutsson*'s "lock device 40 has a Bluetooth® radio module 309 with an antenna 310." *Id.*, 17:18-19.



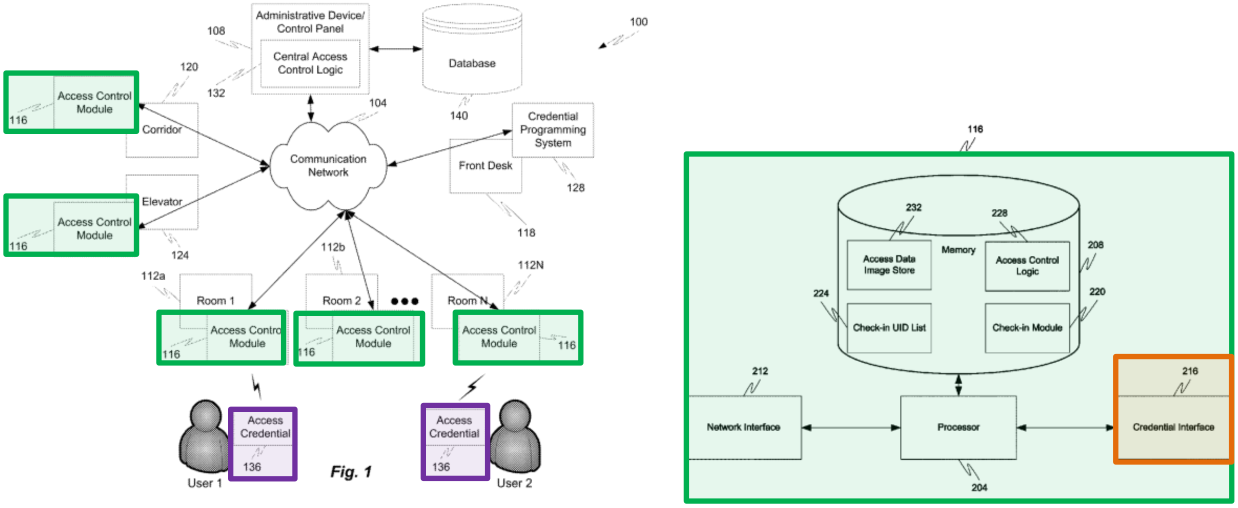
Id., FIGS. 1, 3.

Certain dependent claims in the '205 patent further require encryption methods (claims 7, 11, 19, and 23, **Ground 2**). While *Knutsson* discloses using encryption, it does not expressly disclose using public/private key pairs, but *DeBry* does. Ex-1003, ¶¶54-55.

Certain dependent claims in the ’205 patent 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. Ex-1003, ¶¶56-57.

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

Elfström, like *Knutsson*, discloses the majority of the features of the ’205 patent claims. Ex-1003, ¶58. *Elfström* discloses “access control modules 116 may be adapted to communicate with access credentials 136 carried by users.” *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. *Elfström* explains that “the access data encoded on the credential 136 may include … stay duration.” *Id.*, 12:30-36.



Id., FIGS. 1, 2.

For the independent claims of the ’205 patent (**Ground 4**), *Elfström* 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. But *Woodard* does. Ex-1003, ¶¶59-61.

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**). While *Elfström* does not expressly disclose particular encryption methods, as explained above, *DeBry* does. Ex-1003, ¶61.

Certain dependent claims in the ’205 patent further require the reservation certificate to be valid for an **all-day** interval (claims 3 and 15, **Ground 6**). To the extent that Patent Owner contends the *Elfström-Woodard* combination does not expressly disclose a duration interval that is all day, *Micali* does. Ex-1003, ¶62.

IV. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art (“POSA”) at the time of the purported invention would have had a Bachelor of Science degree in Computer Science or an equivalent field, with at least two years of academic or industry experience with wireless systems or comparable experience. Ex-1003, ¶46. Additional education could substitute for professional experience and vice versa. *Id.*

V. CLAIM CONSTRUCTION

Only claim terms "in controversy" need be construed in IPR "and only to the extent necessary to resolve the controversy." *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (citation omitted), *cert. denied*, 138 S. Ct. 1695 (2018). For the purposes of this IPR, the plain meaning of each claim term is applied. Petitioners reserve the right to contend that any '205 claims are indefinite.

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

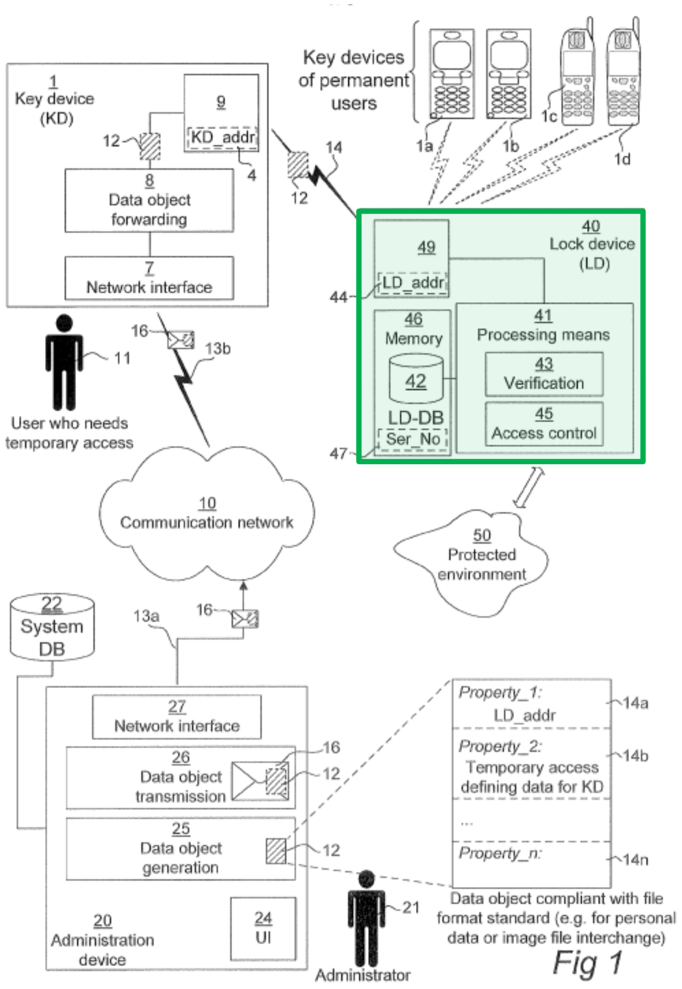
A. Claims 1, 13

Knutsson renders obvious claims 1, 13. Ex-1003, ¶¶64, 109.

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

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

Knutsson renders obvious [1p]/[13p] 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 … **a lock device**." *Id.*, 9:27-28; Ex-1003, ¶¶65, 110.



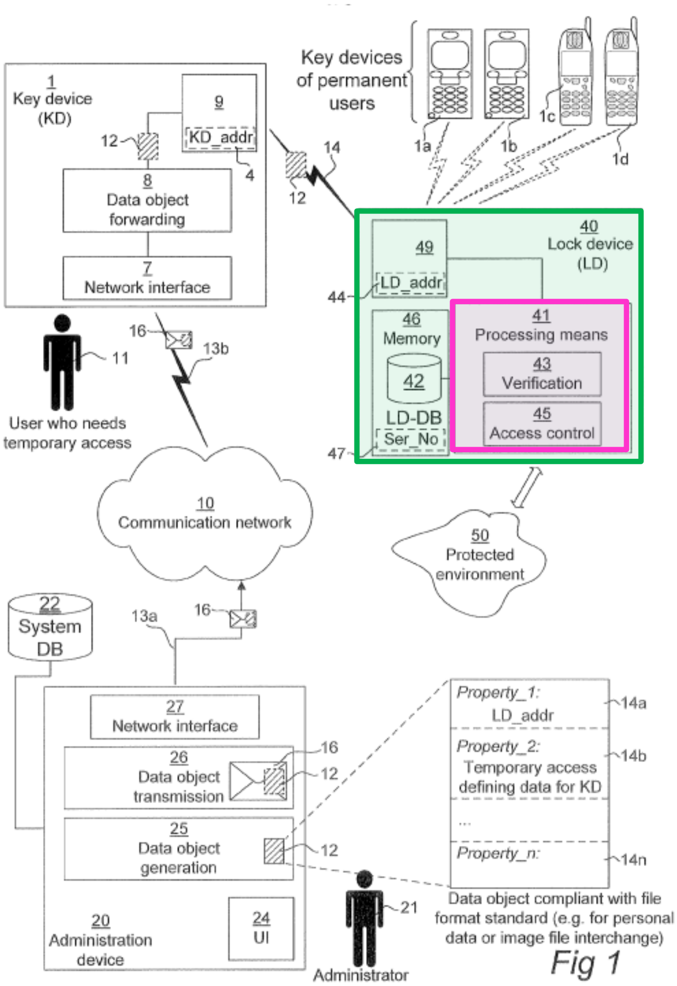
Knutsson, FIG. 1.

Knutsson also discloses "an associated lock device … providing temporary access to the lock device … [and] **associated methods**." *Id.*, 1:8-11; Ex-1003, ¶110.

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

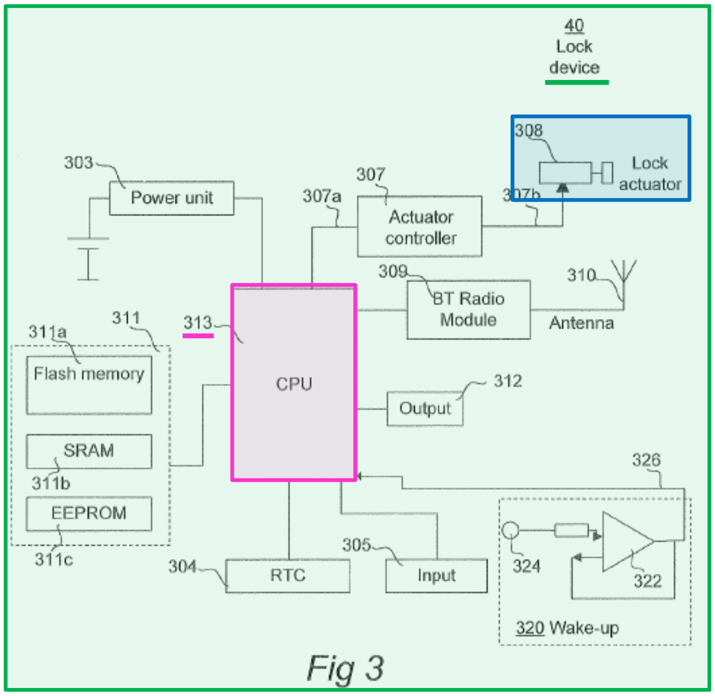
[13A] "accepting, by **a processor**"

Knutsson renders obvious [1A]/[13A] 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; Ex-1003, ¶¶66, 111.



Knutsson, FIG. 1.

FIG. 3 below shows the internal components of *Knutsson*'s lock device. *Id.*, 9:31-32; Ex-1003, ¶67.



Knutsson, FIG. 3.

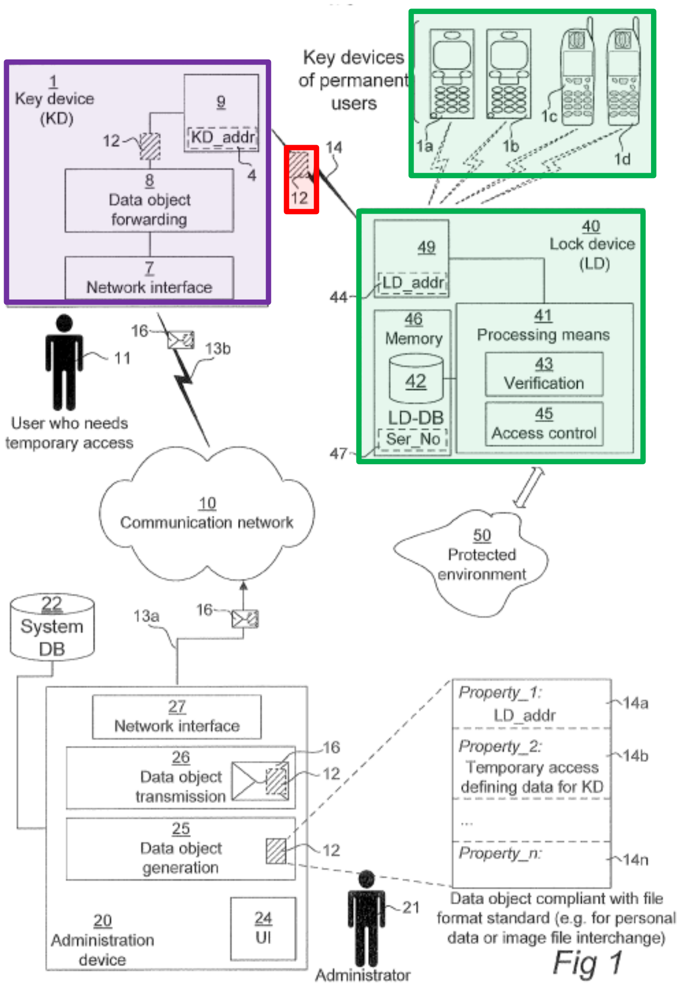
Knutsson's "CPU [313]" is the "processing means 41" of FIG. 1. *Id.*, 17:11-13. *Knutsson* discloses that "CPU 313 … generates the control signal 307a to the actuator controller 307 … [to] cause unlocking of the lock" through "actuator controller 307 … [that] **provide[s] a control signal 307b for engaging [or] disengaging the lock actuator** 308." *Id.*, 17:4-6, 20:7-11; Ex-1003, ¶68.

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**;"

   [13B] "accepting, by a processor through a **communication module**, a **reservation certificate** … presented with a **portable terminal**"

Knutsson renders obvious [1B]/[13B] because *Knutsson* discloses a key device, a mobile phone (portable terminal), that sends access defining data within a data object (reservation certificate) to the lock device's short-range wireless data communication means, a Bluetooth radio module (communication module), connected to its CPU 313 (processor). Ex-1003, ¶¶69, 112.

Knutsson discloses its "lock device 40 will be integrated with or coupled to a lock mechanism in the lockable door" and will "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 contains the temporary access data. *Id.*, 11:32-33. *Knutsson*'s 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," shown below. *Id.*, 13:31-34; Ex-1003, ¶70.

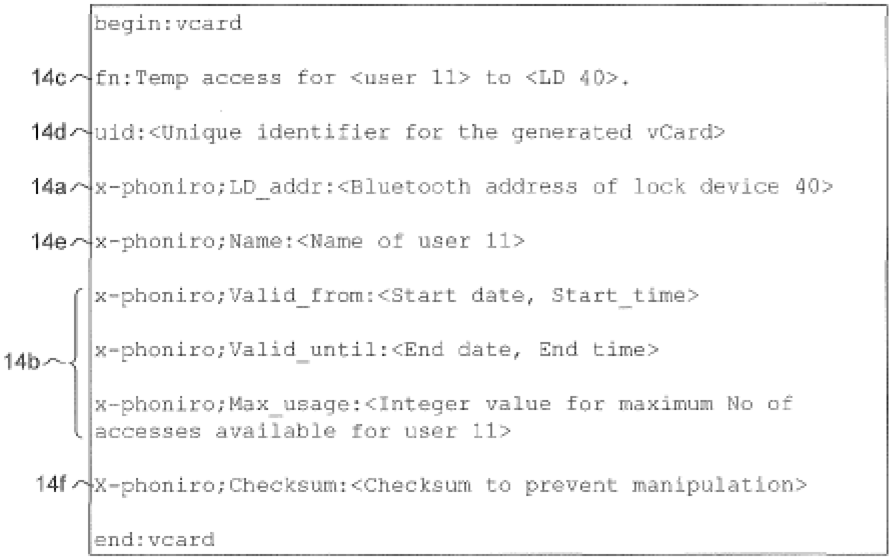


Knutsson, FIG. 1.

Knutsson's key device is the claimed "portable terminal": "[T]he wireless key device is advantageously a **mobile terminal**, such as a mobile phone." *Id.*, 4:32-5:4; FIGS. 1, 2. Further, *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; Ex-1003, ¶71.

Knutsson's data object 12 corresponds to the claimed "reservation certificate." *Knutsson* teaches that **data object 12** is "assigned the data which is necessary for the lock device 40 to be able to **grant temporary access for the key device 1** …. This necessary data includes a communication identifier ('LD_addr' in Fig 1) of the lock device 40." *Knutsson*, 11:32-12:1. "[T]he temporary access defining data assigned to the second vCard property 14b includes temporal data which defines one or more **time frames during which access is permitted for the key device 1** to the protected environment 50." *Id.*, 12:21-26. Data object 12's structure is shown below. Ex-1003, ¶72.

Structure of generated data object 12:

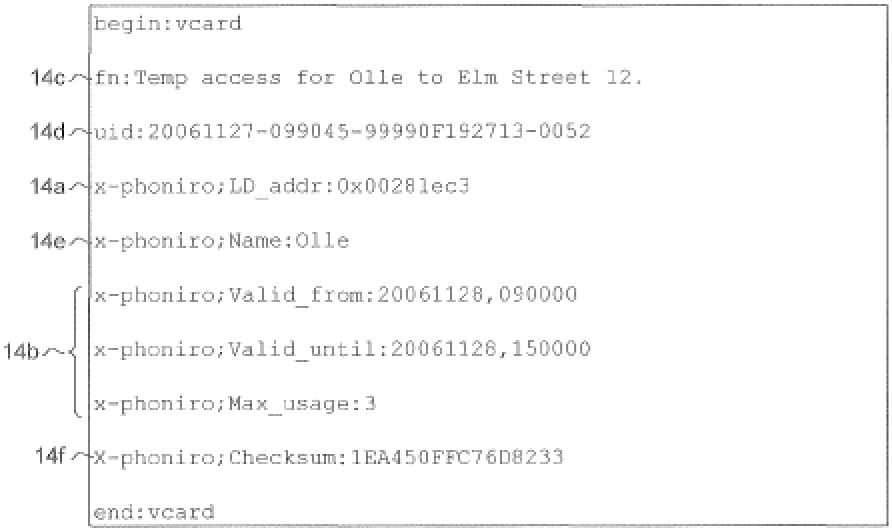


```
begin:vcard
fn:Temp access for <user 11> to <LD 40>.
uid:<Unique identifier for the generated vCard>
x-phoniro;LD_addr:<Bluetooth address of lock device 40>
x-phoniro;Name:<Name of user 11>
x-phoniro;Valid_from:<Start date, Start_time>
x-phoniro;Valid_until:<End date, End time>
x-phoniro;Max_usage: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

14c
14d
14a
14e
14b
14f

Fig 4a

Example of generated data object 12:



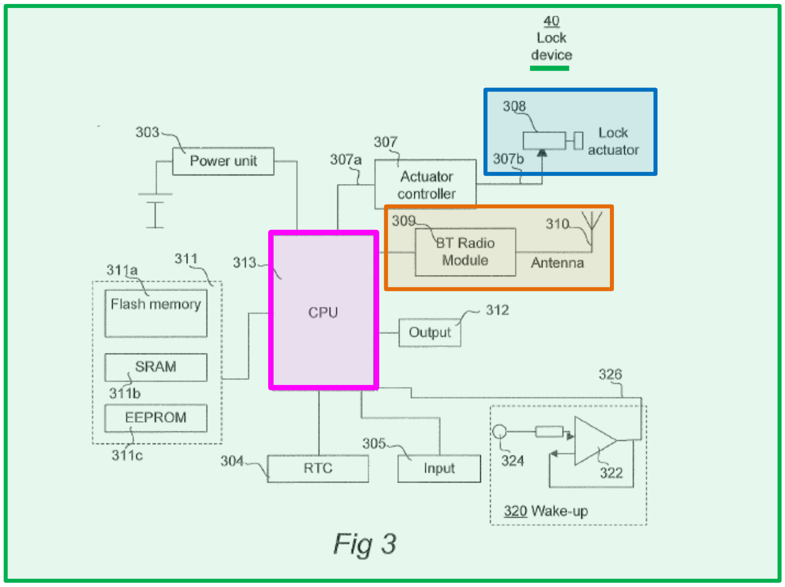
```
begin:vcard
fn:Temp access for Olle to Elm Street 12.
uid:20061127-099045-99990F192713-0052
x-phoniro;LD_addr:0x00281ec3
x-phoniro;Name:Olle
x-phoniro;Valid_from:20061128,090000
x-phoniro;Valid_until:20061128,150000
x-phoniro;Max_usage:3
X-phoniro;Checksum:1EA450FFC76D8233
end:vcard
```

14c
14d
14a
14e
14b
14f

Fig 4b

Knutsson, FIGS. 4A-4B.

Knutsson's "communication means 49" corresponds to the claimed "communication module." "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. "[L]ock device 40 has short-range wireless data communication means 49 in the form of a Bluetooth® transceiver," *id.*, 12:3-7, also described as "a Bluetooth® radio module 309 with an antenna 310" and is shown connected to CPU 313 in figure 3 below. *Id.*, 17:18-20; Ex-1003, ¶73.



Knutsson, FIG. 3.

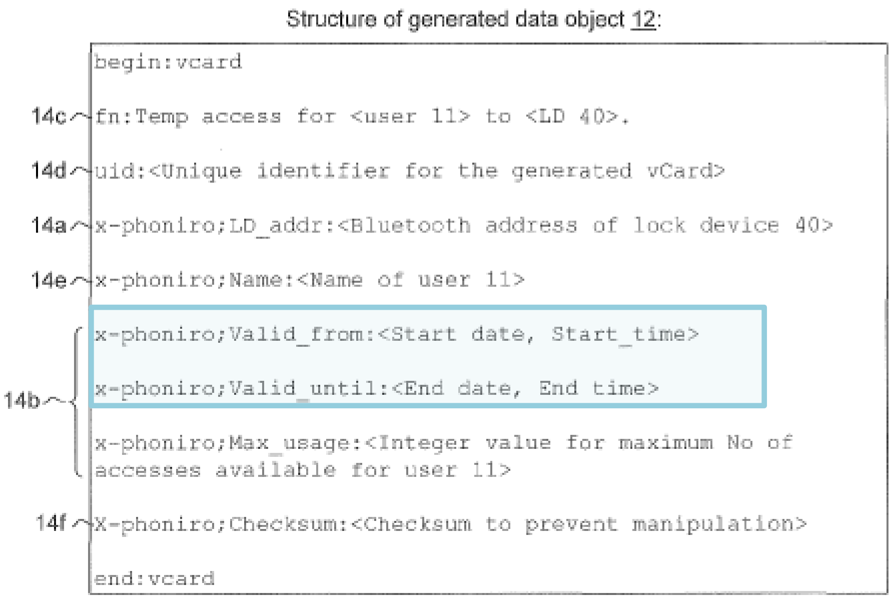
Using such communications, *Knutsson* discloses "**data object (vCard) 12 will be transmitted by the key device 1** [] and **be received by the lock device 40**." *Id.*, 16:1-3, FIG. 5C; Ex-1003, ¶74.

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

   [13C] "a **reservation certificate** that comprises an **interval** of a reservation …"

Knutsson renders obvious [1C]/[13C] because data object 12 (reservation certificate) includes "temporal data which defines one or more time frames," and "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; FIGS. 5-6; Ex-1003, ¶¶75, 113.

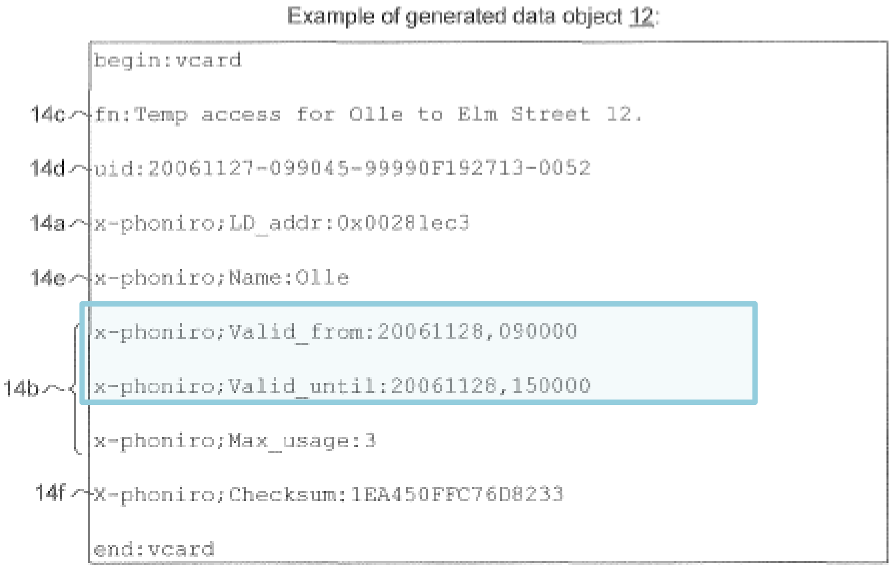
Figures 4a-4b show that the "temporary access defining data assigned to the second vCard property 14b includes temporal data." *Knutsson*, 12:21-24; Ex-1003, ¶76.



Structure of generated data object 12:

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

Fig 4a



Example of generated data object 12:

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

Fig 4b

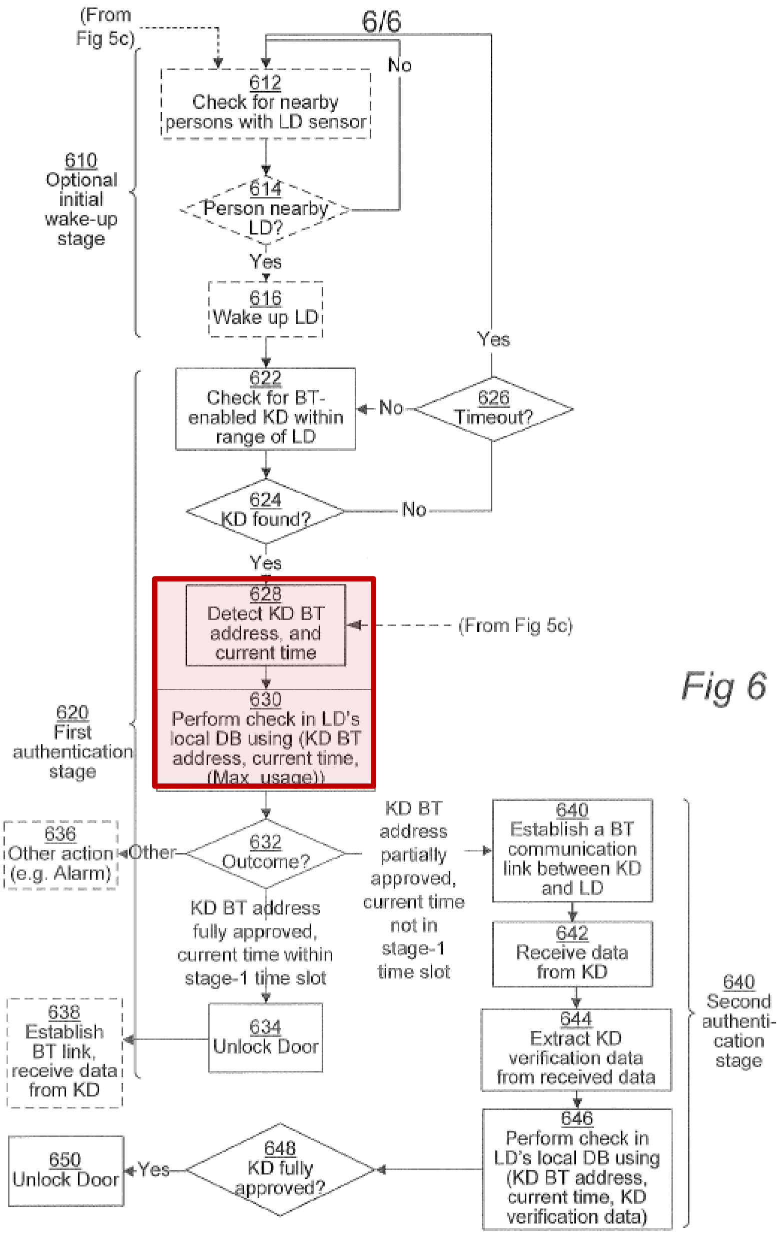
Knutsson, FIGS. 4A-4B.

Knutsson's data object 12, specifying start and end times of temporary access, is an "interval of a reservation" because an interval is defined by a starting point and an end point. Ex-1003, ¶77. By providing start and end times, an interval is presented by *Knutsson*'s key device (portable terminal), *Knutsson*, 12:21-26, as confirmed by *Knutsson*'s CPU 313 determining whether the current time, which the CPU 313 has access to, falls within a "time-slot." *Knutsson*, 17:21-22, 18:16-19:16, 20:4-7, 20:12-15, Table 1; Ex-1003, ¶77. Dr. Bederson also opines, "[t]he 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." Ex-1003, ¶77.

A POSA would have also understood that *Knutsson*'s "temporary access" for "a room … with a controllable physical access interface in the form of a lockable door" satisfies the ordinary meaning of a "reservation." Ex-1003, ¶78. This is confirmed by the '205 patent's disclosure of a reservation as allowing access to "a hotel room lock." Ex-1001, 1:64-2:1; Ex-1003, ¶78.

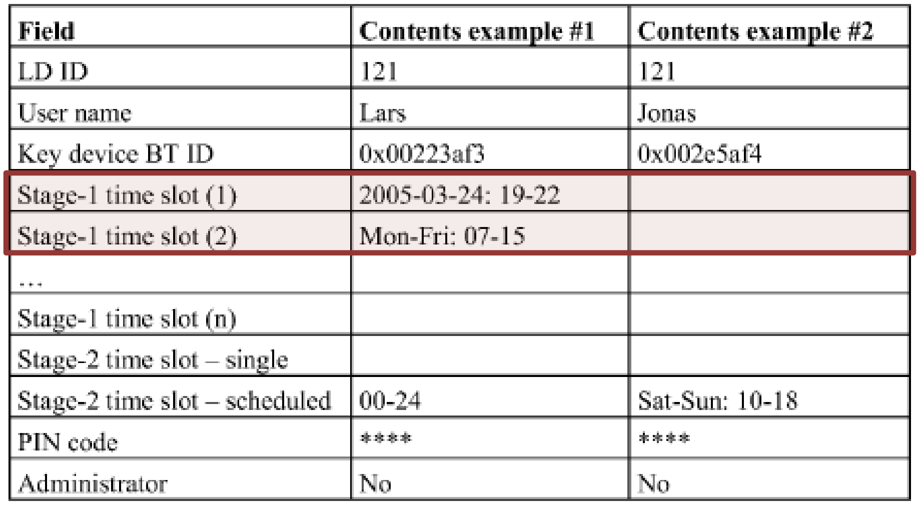
5. **[1D]** "the processor is configured to **compare the interval of the reservation of the current reservation certificate to a current time** accessible to the processor, **determine the current time is within the interval of the reservation**, and"

   [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**," *Knutsson* renders obvious [1D]/[13D] because lock device 40 "includes a real-time clock 304 capable of providing the CPU 313 with an accurate value of the **current time**," *Knutsson*, 17:21-22, and "the CPU … [checks] whether the current time falls within any stage-1 time slot defined for that Bluetooth® address." *Id.*, 20:4-7, FIG. 6 at 628-630; Ex-1003, ¶¶79, 114.


(From Fig 5c)
6/6
612 Check for nearby persons with LD sensor
No
610 Optional initial wake-up stage
614 Person nearby LD?
Yes
616 Wake up LD
Yes
622 Check for BT-enabled KD within range of LD
No
626 Timeout?
624 KD found?
No
Yes
628 Detect KD BT address, and current time
(From Fig 5c)
Fig 6
630 Perform check in LD's local DB using (KD BT address, current time, (Max. usage))
620 First authentication stage
KD BT address partially approved, current time not in stage-1 time slot
640 Establish a BT communication link between KD and LD
636 Other action (e.g. Alarm)
Other
632 Outcome?
KD BT address fully approved, current time within stage-1 time slot
642 Receive data from KD
640 Second authenti-cation stage
638 Establish BT link, receive data from KD
634 Unlock Door
644 Extract KD verification data from received data
646 Perform check in LD's local DB using (KD BT address, current time, KD verification data)
650 Unlock Door
Yes
648 KD fully approved?

Knutsson, FIG. 6.

Knutsson's stage-1 "authorization is based solely on the key device's Bluetooth® address and the current time." *Id.*, 18:1-4. Authorization therefore corresponds to determining the current time is in the time slot (interval) of the allowed temporary access (reservation) when temporal data of object 12 (reservation certificate) is verified to allow access (current). *Id.*, FIG. 6 at 632-634; Ex-1003, ¶80. Regarding "activating," *Knutsson* discloses "the outcome of these checks [being] fully positive … will cause unlocking of the lock." *Knutsson*, 20:7-11; Ex-1003, ¶114. Time slots are shown below in an example of object 12. Ex-1003, ¶80.



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

Knutsson, Table 1.

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

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

Knutsson renders obvious [1E]/[13E] because "CPU 313 is programmed to … perform a method for wireless automatic unlocking in response to the appearance and proper authentication of a key device." *Knutsson*, 17:9-11;

Ex-1003, ¶¶81, 116. “If the outcome of these checks is fully positive, as checked in step 632, the CPU 313 proceeds to step 634 and generates the control signal 307a to the actuator controller 307. As described above, this will cause unlocking of the lock.” *Knutsson*, 20:7-11; Ex-1003, ¶81.

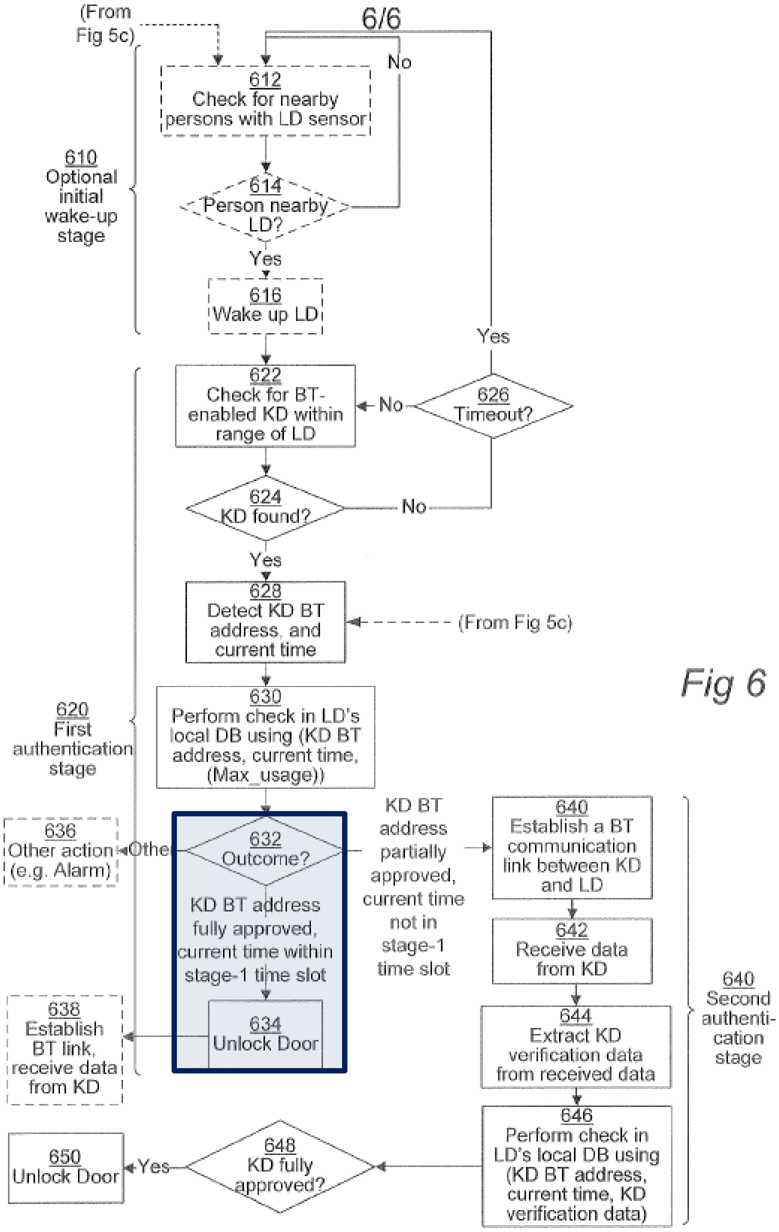

(From Fig 5c)
6/6
No
612 Check for nearby persons with LD sensor
610 Optional initial wake-up stage
614 Person nearby LD?
Yes
616 Wake up LD
Yes
622 Check for BT-enabled KD within range of LD
No
626 Timeout?
624 KD found?
No
Yes
628 Detect KD BT address, and current time
(From Fig 5c)
620 First authentication stage
630 Perform check in LD's local DB using (KD BT address, current time, (Max_usage))
636 Other action (e.g. Alarm)
Other
632 Outcome?
KD BT address fully approved, current time within stage-1 time slot
KD BT address partially approved, current time not in stage-1 time slot
640 Establish a BT communication link between KD and LD
642 Receive data from KD
640 Second authentication stage
638 Establish BT link, receive data from KD
634 Unlock Door
644 Extract KD verification data from received data
646 Perform check in LD's local DB using (KD BT address, current time, KD verification data)
648 KD fully approved?
Yes
650 Unlock Door

Fig 6

Knutsson, FIG. 6.

Knutsson discloses that "CPU 313 … [checks] whether the current time falls within any stage-1 time slot defined for that Bluetooth® address" and, upon determining the current time falls within a stage-1 time slot, effectuates "engaging or disengaging the lock actuator 308 to cause unlocking when appropriate" and thus unlocking the door lock. *Knutsson*, 17:4-6, 20:4-7, FIG. 6 at 628-630; Ex-1003, ¶¶81-82.

B. Claims 2, 14

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"

[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**."

Knutsson renders obvious [2A]/[14]. Ex-1003, ¶¶83, 116.

As explained in Sections VI.A.5-6, *Knutsson* discloses that "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 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; Ex-1003, ¶84.

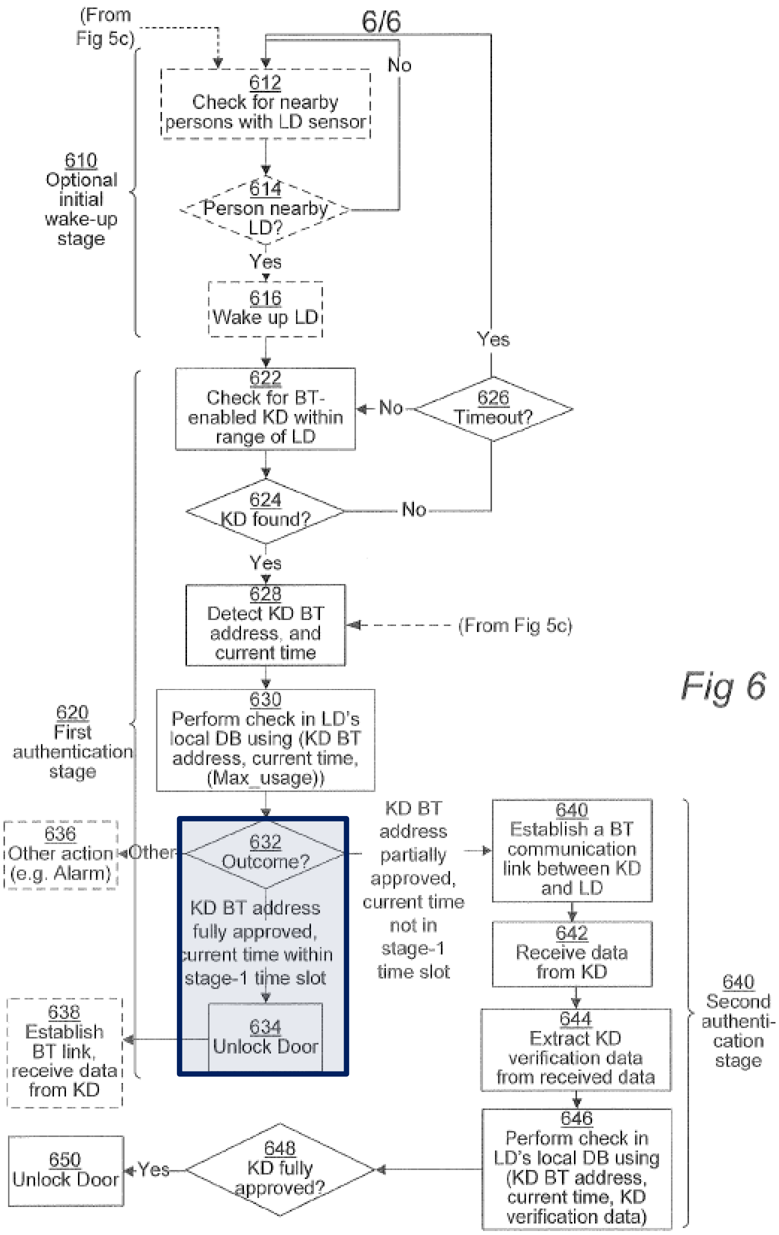
A POSA would have understood that *Knutsson*'s disclosure of object 12 including both a start time and an end time of a temporary access renders obvious the claimed "interval" because an interval is defined by a starting point and an end point. Ex-1003, ¶85; Section VI.A.4. Similarly, a POSA would have understood *Knutsson*'s disclosures of the object 12 including both a start time and an end time and a "time slot" of a temporary access as disclosing a "predetermined duration." Ex-1003, ¶85 (citing *Knutsson*, 20:4-7). This is confirmed by *Knutsson*'s disclosure of "temporary" access because *Knutsson* is disclosing access for a set time, i.e., a "duration," and "because a POSA would have understood that a duration can be calculated by subtracting the start time from the end time." Ex-1003, ¶85. Thus, *Knutsson* discloses its object 12 (certificate) is used from the start time to the end time, also an end of the duration, as compared to the "current time," *Knutsson*, 12:24-26, 20:4-7, and thus the object 12 would be current during its time slot. *Id.*; Ex-1003, ¶85.

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**."

Knutsson renders obvious [2B]. Ex-1003, ¶¶86, 116.

Knutsson discloses that "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 628-630. And, upon determining the current time falls within a stage-1 time slot, CPU 313 causes "engaging or disengaging [of[the lock actuator 308 to cause unlocking when appropriate." *Knutsson*, 17:4-6; Ex-1003, ¶87.

Knutsson's temporal data within data object 12 includes "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. Thus, unlocking occurs when the current time falls within the time slot defined by the start and end points. Ex-1003, ¶88.


(From Fig 5c)
6/6
612 Check for nearby persons with LD sensor
No
610 Optional initial wake-up stage
614 Person nearby LD?
Yes
616 Wake up LD
Yes
622 Check for BT-enabled KD within range of LD
No
626 Timeout?
624 KD found?
No
Yes
628 Detect KD BT address, and current time
(From Fig 5c)
Fig 6
620 First authentication stage
630 Perform check in LD's local DB using (KD BT address, current time, (Max_usage))
636 Other action (e.g. Alarm)
Other
632 Outcome?
KD BT address partially approved, current time not in stage-1 time slot
640 Establish a BT communication link between KD and LD
KD BT address fully approved, current time within stage-1 time slot
642 Receive data from KD
638 Establish BT link, receive data from KD
634 Unlock Door
644 Extract KD verification data from received data
640 Second authentication stage
646 Perform check in LD's local DB using (KD BT address, current time, KD verification data)
650 Unlock Door
Yes
648 KD fully approved?

Knutsson, FIG. 6.

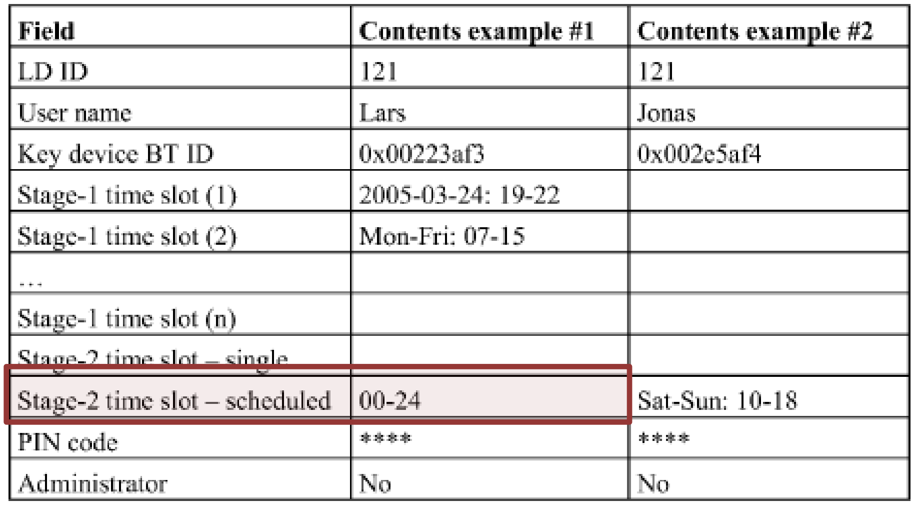
C. Claims 3, 15

[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**."

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

Knutsson renders obvious claims 3, 15. Ex-1003, ¶¶89, 117.

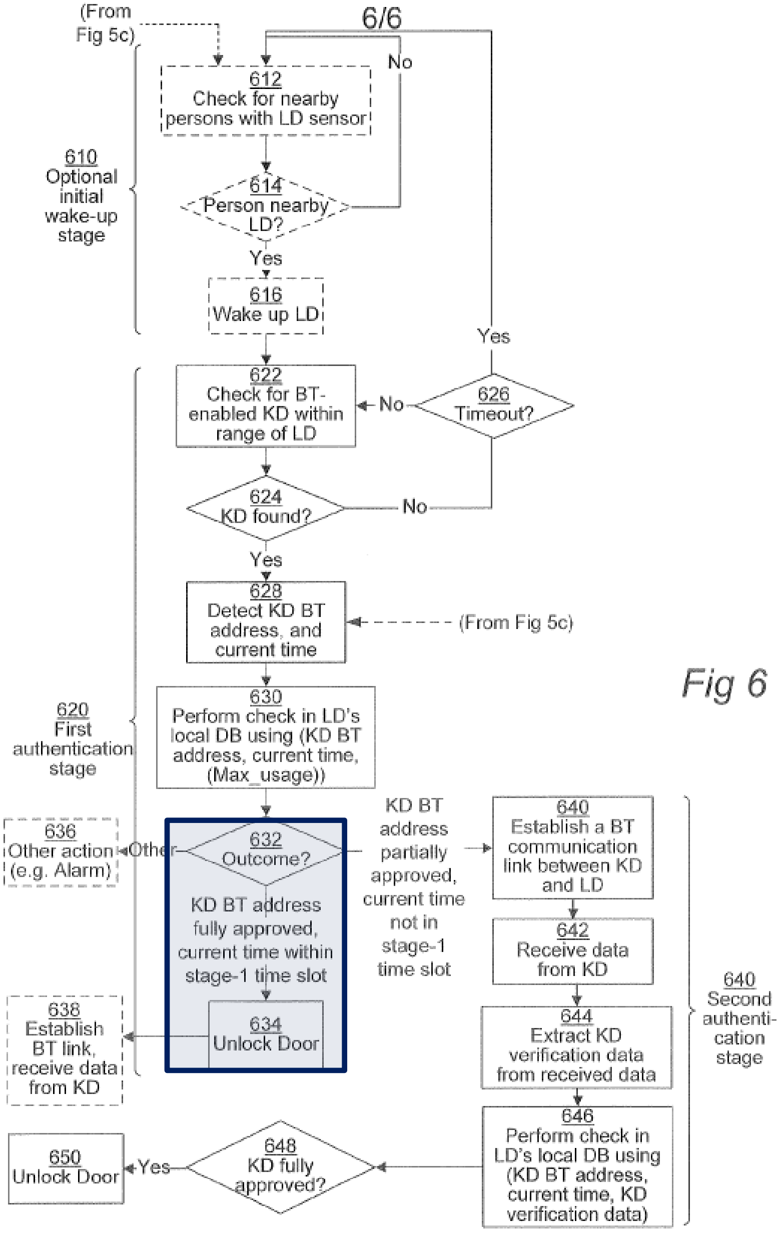
As explained in Section VI.B, *Knutsson*'s temporal data may be "one [or] more dates and/or times" when temporary access permitted." *Knutsson*, 12:24-26. A POSA would have found it obvious that *Knutsso*n's one date includes where the time slot defined by the start point and end point is the length of "a day," because a single date corresponds to all day. Ex-1003, ¶90. *Knutsson* provides examples of stage-1 or stage-2 authentication of "during working days" or "any time (**00-24**)," *Knutsson*, 18:16-19:1, which a POSA would have found corresponds to "all day." Ex-1003, ¶90. *Knutsson* illustrates 00-24 in Table 1:



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

Knutsson, Table 1.

Knutsson discloses that 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" when temporary access is permitted. *Id.*, 12:24-26, 20:7-11; Ex-1003, ¶90.


6/6
(From Fig 5c)
612 Check for nearby persons with LD sensor
No
610 Optional initial wake-up stage
614 Person nearby LD?
Yes
616 Wake up LD
Yes
622 Check for BT-enabled KD within range of LD
No
626 Timeout?
624 KD found?
No
Yes
628 Detect KD BT address, and current time
(From Fig 5c)
Fig 6
620 First authentication stage
630 Perform check in LD's local DB using (KD BT address, current time, (Max_usage))
636 Other action (e.g. Alarm)
Other
632 Outcome?
KD BT address partially approved, current time not in stage-1 time slot
640 Establish a BT communication link between KD and LD
KD BT address fully approved, current time within stage-1 time slot
642 Receive data from KD
640 Second authenti-cation stage
638 Establish BT link, receive data from KD
634 Unlock Door
644 Extract KD verification data from received data
646 Perform check in LD's local DB using (KD BT address, current time, KD verification data)
650 Unlock Door
Yes
648 KD fully approved?

Knutsson, FIG. 6.

D. Claims 4, 16

> **[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**."

> **[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**."

Claims 4, 16 are substantially similar to claims 2, 14 except that claims 2, 14 have additional limitations related to the "current time." Ex-1003, ¶91 (comparing claims), 118. *Knutsson* renders claim 4, 16 obvious for the reasons explained for claims 2, 14 in Section VI.B. *Id.*

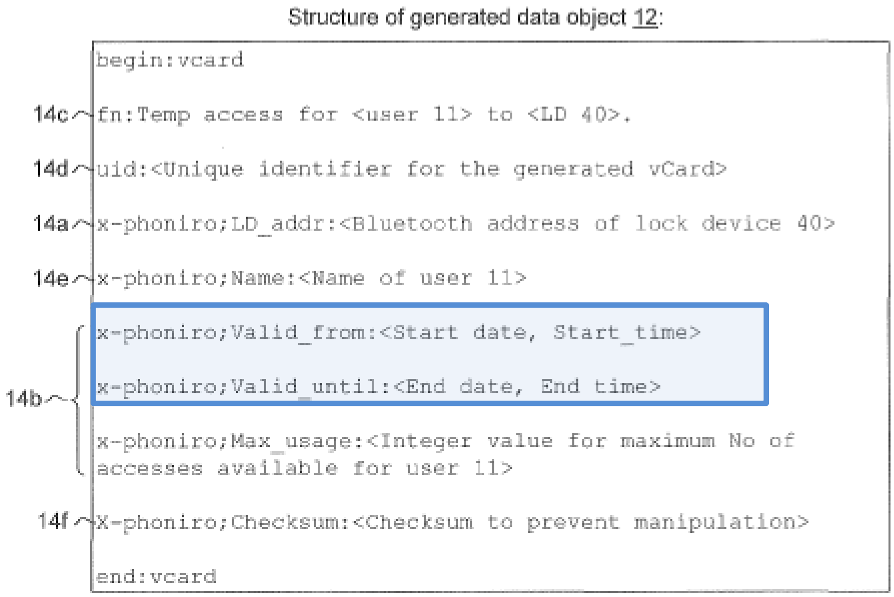
E. Claims 6, 18

> **[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**."

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

Knutsson renders obvious claims 6, 18. Ex-1003, ¶¶92, 119.

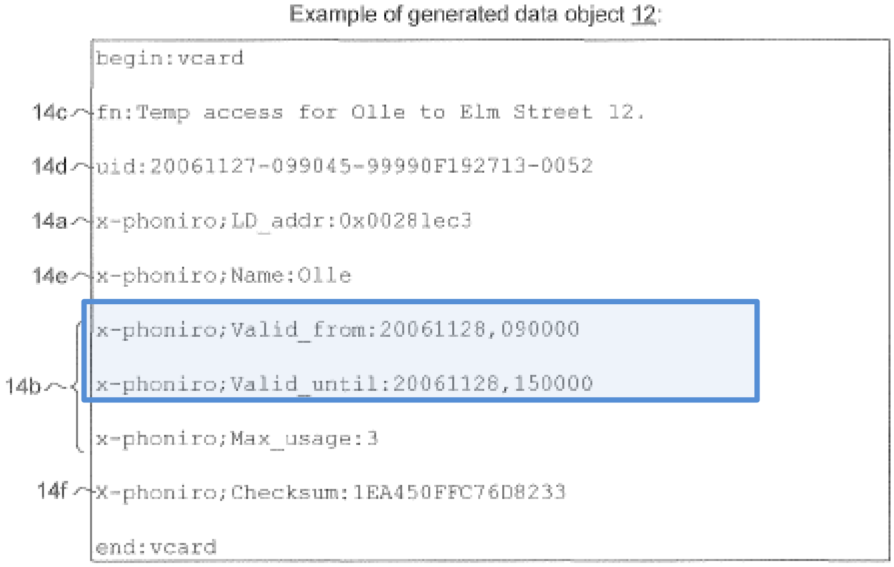
Knutsson's "CPU 313 … [checks] whether the current time falls within any stage-1 time slot defined for that Bluetooth® address." *Knutsson*, 20:4-7, FIG. 6 at 628-630. *Knutsson*'s temporal data may be "one [or] more dates and/or times which define start point ('Valid_from') and end point ('Valid_to') for the temporary access permitted." *Id.*, 12:24-26, 12:21-24. *Knutsson* shows the temporal data in Figures 4a-4b, shown below.



Structure of generated data object 12:

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

Fig 4a



Example of generated data object 12:

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

Fig 4b

Knutsson, FIGS. 4A-4B.

F. Claims 5, 17

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

Knutsson renders obvious claims 5, 17. Ex-1003, ¶¶94, 120. *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 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" resulting in "unlocking of the lock." *Id.*, 20:7-11; Ex-1003, ¶94.

G. Claims 8, 20

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**:"

> **[20A]** "The method of claim 13 wherein … a **symmetric key** stored in a **memory** accessible to the processor,"

Knutsson discloses [8A]/[20A] because *Knutsson* discloses that its lock device includes local memory 46 (memory) coupled to the processor and configured to decipher the data object 12 (data encrypted with a symmetric key). Ex-1003, ¶¶95, 121.

Knutsson discloses a "local memory 46 of the lock device," *Knutsson*, 12:19, and that "memory 311" is "local memory 46." *Id.*, 17:11-13. Ex-1003, ¶96.

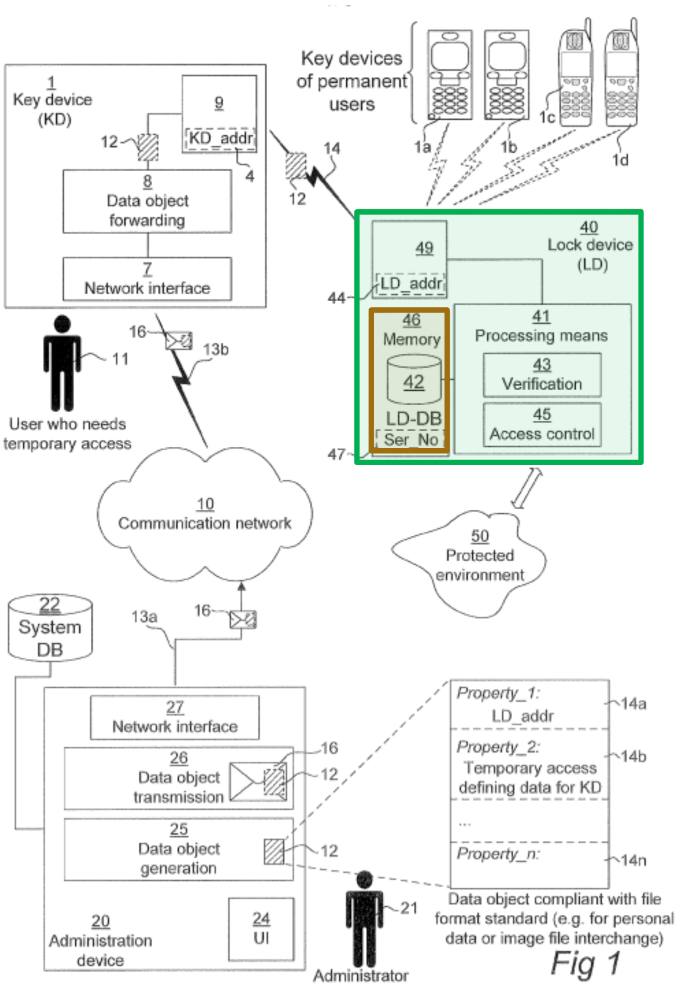
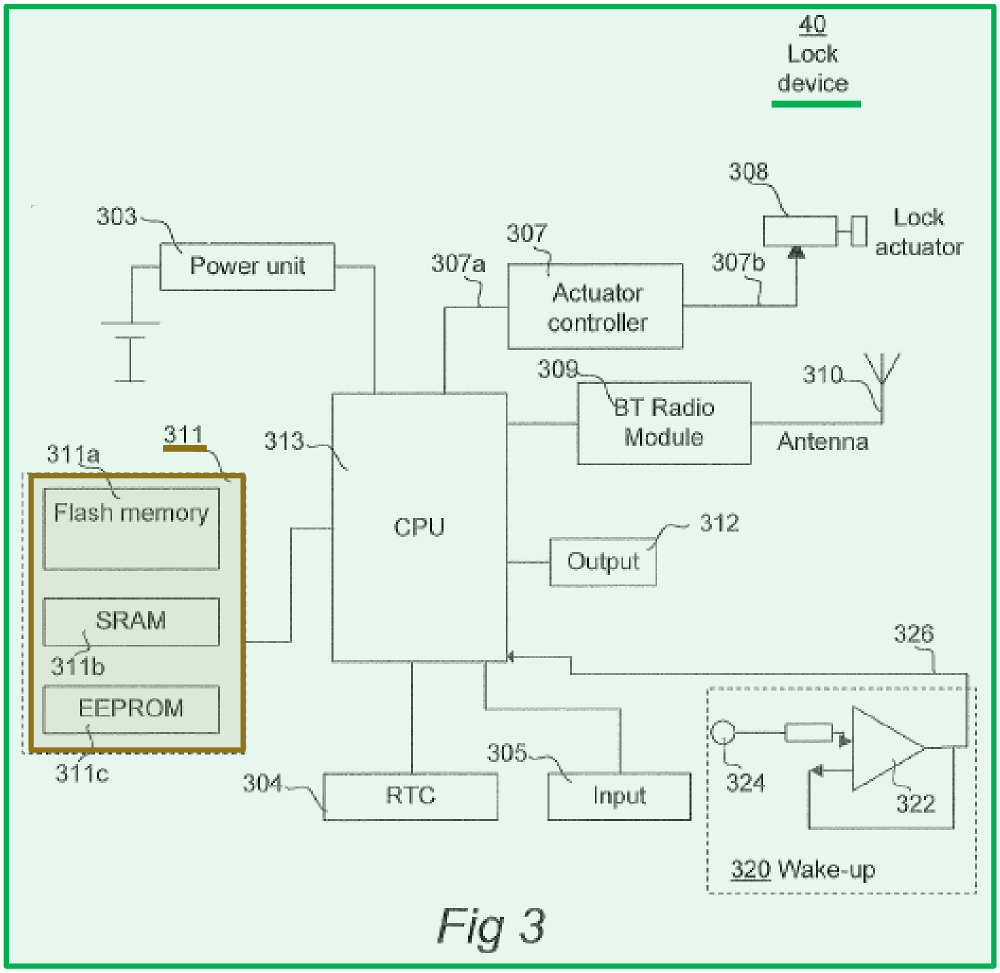


Fig 1



Knutsson, FIGS. 1, 3.

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 elimination of decryption key distribution because the lock device and administrative device already know the decryption key. *Id.*, 6:18-19. 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. *Id.*, 16:6-9; Ex-1003, ¶97.

Alternatively, *Knutsson* discloses "that all communication between key device and lock device may be **encrypted** in accordance with an encryption algorithm, such as **Blowfish**." *Knutsson*, 19:12-14. *Knutsson*'s lock device processing means "performs decryption." *Id.*, 16:6-9. 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 the lock device can decrypt received encrypted communications. Ex-1003, ¶97.

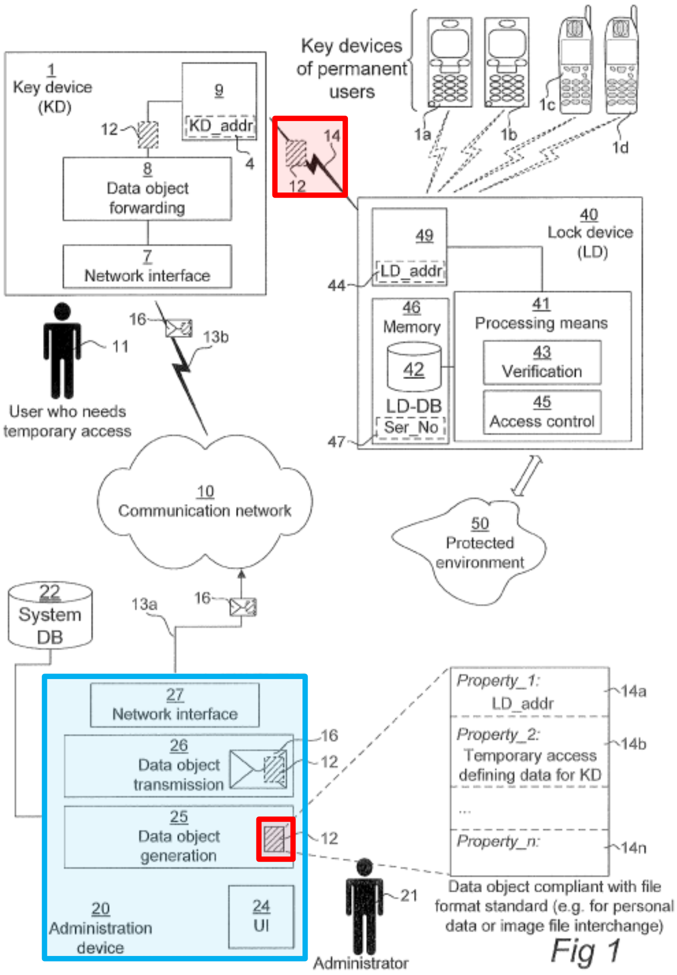
A POSA would have known that Blowfish is a symmetric key encryption method. Ex-1003, ¶98 (quoting U.S. Patent No. 8,412,837 (Ex-1011), 6:37-41 ("[a]n example of encrypting the private key is to encrypt it with a symmetric cipher such as … Blowfish"); U.S. Patent No. 5,794,207 (Ex-1012), 24:24-31 ("a symmetric key … may be implemented … with … Blowfish")).

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**."

[20B] "The method of claim 13 wherein at least a portion of the reservation certificate is **encrypted by a server using a symmetric key** … 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."

Knutsson renders obvious [8B]/[20B] because *Knutsson* discloses that data object 12 (current reservation certificate) is encrypted and is being deciphered by the processor at the lock device (using the symmetric key to verify the reservation certificate). Ex-1003, ¶¶99, 121.

Knutsson's data object 12 is encrypted by a server because data object 12 originates with *Knutsson*'s administration device 20 which is 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. Ex-1003, ¶100.



Knutsson, FIG. 1.

As explained in Section VI.G.1, *Knutsson*'s lock device processor decrypts communications from the administrative device, *Knutsson*, 16:6-9, and thus achieves "enhanced security," *id.*, 6:13, which includes determining the communications are from the correct source, the administrative device, corresponding to the claimed verifying genuineness. Ex-1003, ¶101.

Alternatively, as explained in Section VI.G.1, *Knutsson* discloses "that **all communication** … [is] **encrypted** in accordance with an encryption algorithm, such as **Blowfish**." *Knutsson*, 19:12-14. A POSA would have understood Blowfish is a symmetrical key/cipher system. Ex-1003, ¶102. Accordingly, a POSA would have found it obvious that the data object 12 is encrypted using a symmetrical key of the Blowfish encryption and then decrypted by the recipient, i.e., *Knutsson*'s lock device 40, using the same symmetrical key. *Id.*

Knutsson discloses that Blowfish ensures "data integrity is ascertained," meeting *Knutsson*'s goal of "security." *Knutsson*, 6:13-17, 19:14. A POSA would have understood data integrity involves determining that *Knutsson*'s data object 12 (i.e., the claimed "reservation certificate") is from the correct sender, i.e., *Knutsson*'s administrator device 20, corresponding to "being genuine." Ex-1003, ¶103.

Knutsson's lock device activates after verification once "data integrity is ascertained," corresponding to the claimed "activating" step of [20B]. *Knutsson* discloses that "[i]f the outcome of these checks is fully positive … this will cause unlocking of the lock." *Knutsson*, 20:7-11; Ex-1003, ¶122.

H. Claims 9, 21

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

Knutsson renders obvious claims 9, 21 because *Knutsson* discloses using encryption for, e.g., "data integrity" as explained in Section VI.G.2. A POSA would have understood that encryption by the server and decryption by the lock device to maintain "data integrity" corresponds to the claimed verification that the reservation certificate "is genuine." Ex-1003, ¶¶104, 123.

Knutsson's lock device activates after verification once "data integrity is ascertained," corresponding to the claimed "activating" step of claim 21. As discussed in the previous section, "the outcome of these checks [being] fully positive," including matching communication identifiers and being able to decrypt data object 12, "will cause unlocking of the lock." *Knutsson*, 20:7-11; Ex-1003, ¶104, 123.

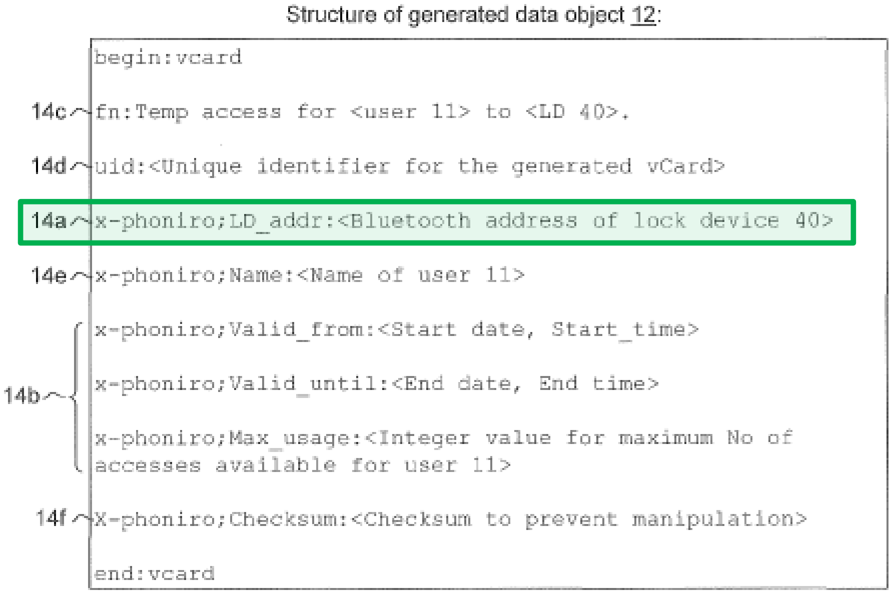
I. Claims 10, 22

> **[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**."

> **[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."

Knutsson renders obvious claims 10, 22 because *Knutsson* discloses an identifier (identification) of the lock device (access device) as part of data object 12 (current reservation certificate) that the lock device processor receives and verifies to activate the door lock. Ex-1003, ¶¶105, 124.

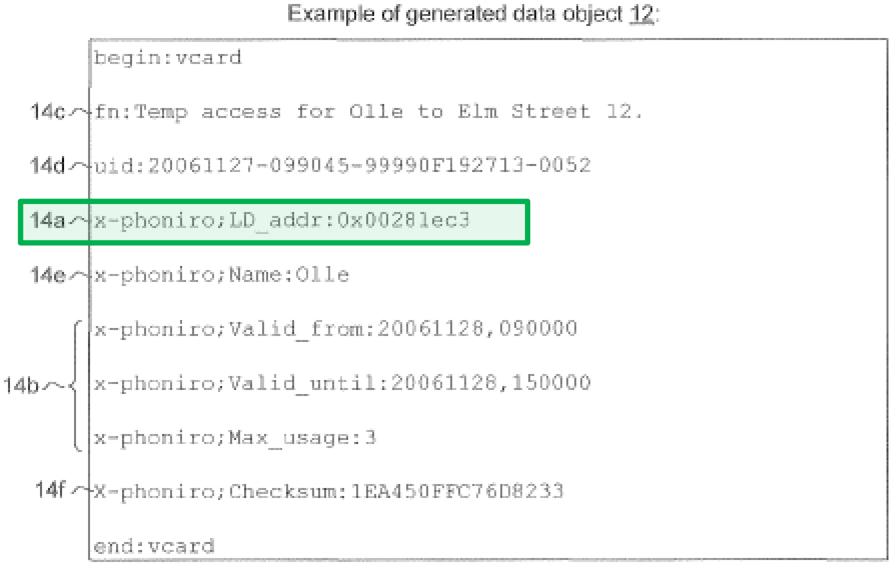
Knutsson discloses storing "the communication address" and "a serial [n]o of the lock device … in local memory of the lock device." *Knutsson*, 6:13-17. *Knutsson* further discloses "**the communication identifier specified in the created data object 12** in the administration device 20 is … the Bluetooth® address 44 of **the lock device's 40 Bluetooth® transceiver 49**." *Id.*, 12:4-7. This data is in data object 12, shown in the first property 14a in figure 4. Ex-1003, ¶106.



Structure of generated data object 12:

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

Fig 4a



Example of generated data object 12:

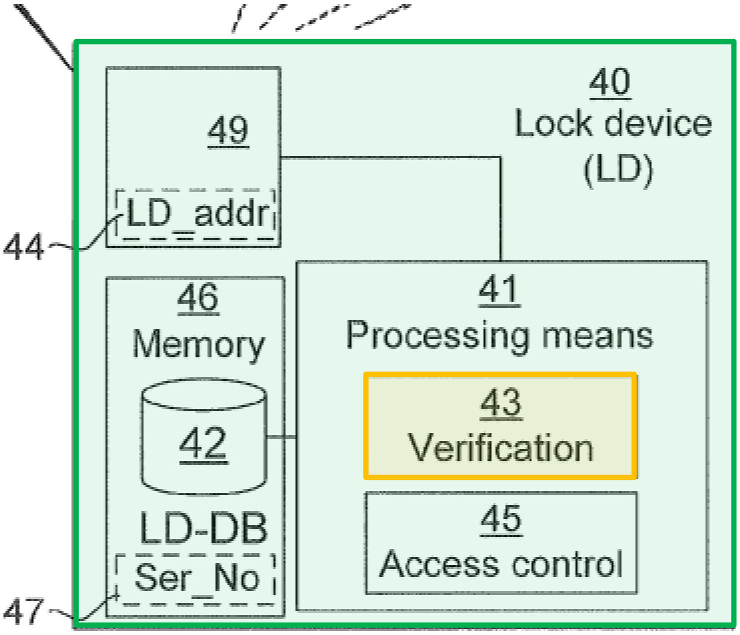
```
begin:vcard
fn:Temp access for Olle to Elm Street 12.
uid:20061127-099045-99990F192713-0052
x-phoniro;LD_addr:0x00281ec3
x-phoniro;Name:Olle
x-phoniro;Valid_from:20061128,090000
x-phoniro;Valid_until:20061128,150000
x-phoniro;Max_usage:3
X-phoniro;Checksum:1EA450FFC76D8233
end:vcard
```

Fig 4b

Id., FIGS. 4A-4B.

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; Ex-1003, ¶107.



Knutsson, FIG. 1 Excerpt.

The claim only requires that "the identification correspond[s] to one of the access device and the door lock," and *Knutsson*'s Bluetooth® address (identification) corresponds to lock device 40 (access device). Ex-1003, ¶108.

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; Ex-1003, ¶108.

.

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

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

As explained in Section III.A, claims 7, 11, 19, and 23 require types of encryption elements that, while suggested by *Knutsson*, are not expressly disclosed. A POSA, however, would have been motivated to implement *DeBry*'s encryption methods into *Knutsson*'s data object 12 because, as *DeBry* explains, "[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; Ex-1003, ¶125. *Knutsson* also discloses the same goal of "enhanced security" achieved through encryption, and *Knutsson* provides an example of encryption using Blowfish. *Knutsson*, 6:13-17; 19:12-14; Ex-1003, ¶125. A POSA would thus have incorporated *DeBry*'s encryption methods to avoid unauthorized interceptions, for example to "ensure the privacy of transmitted messages." Ex-1003, ¶125 (quoting *DeBry*, 2:28-36).

A POSA would have had reasonable expectations of success combining *DeBry* and *Knutsson* because *DeBry*'s encryption methods were well-known methods of encrypting communications between one device to another, such as *DeBry*'s client system communicating with a printer. *DeBry*, 5:34-36; Ex-1003, ¶126. Similarly, a POSA would have known using *DeBry*'s encryption methods in

Knutsson's key device (a PDA or a mobile phone) when instructing *Knutsson*'s lock device 40 to open a lock would ensure data integrity and security. *Knutsson*, 10:24-30; Ex-1003, ¶126.

B. Claims 7, 19

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"

[19A] "The method of claim 13 wherein … for which the corresponding **public key** is stored in a **memory** accessible to the processor"

Knutsson in combination with *DeBry* renders obvious [7A]/[19A] because *Knutsson* discloses a memory coupled to a processor and encryption of the reservation certificate, and *DeBry* further discloses a specific encryption method using a public key. Ex-1003, ¶127.

Knutsson discloses "local memory 46 of the lock device," *Knutsson*, 12:19, 17:11-13. Ex-1003, ¶¶127-128, 141.

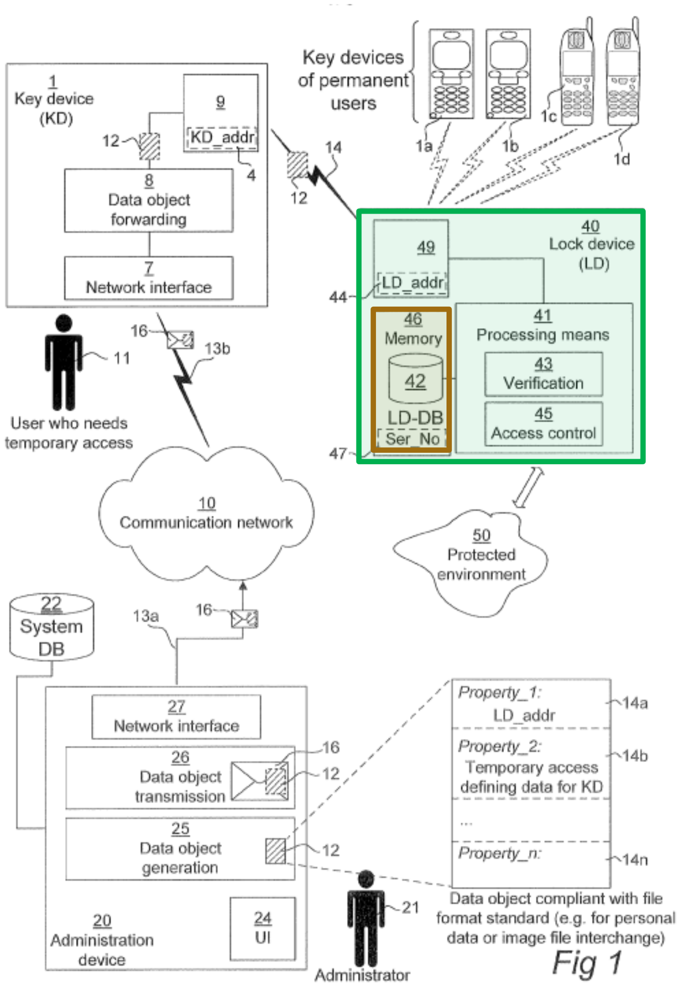
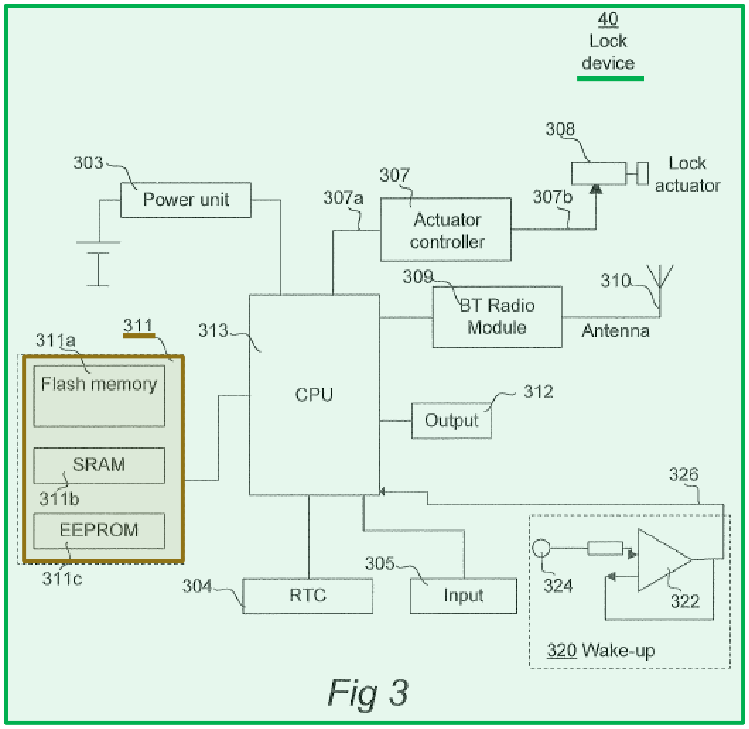

1
Key device
(KD)
9
KD_addr
4
12
8
Data object
forwarding
7
Network interface
Key devices
of permanent
users
1a
1b
1c
1d
14
12
40
Lock device
(LD)
49
LD_addr
44
46
Memory
42
LD-DB
Ser_No
47
41
Processing means
43
Verification
45
Access control
16
13b
11
User who needs
temporary access
10
Communication network
50
Protected
environment
22
System
DB
13a
16
27
Network interface
26
Data object
transmission
16
12
25
Data object
generation
12
20
Administration
device
24
UI
21
Administrator
Property_1:
LD_addr
14a
Property_2:
Temporary access
defining data for KD
14b
...
Property_n:
14n
Data object compliant with file
format standard (e.g. for personal
data or image file interchange)

Fig 1

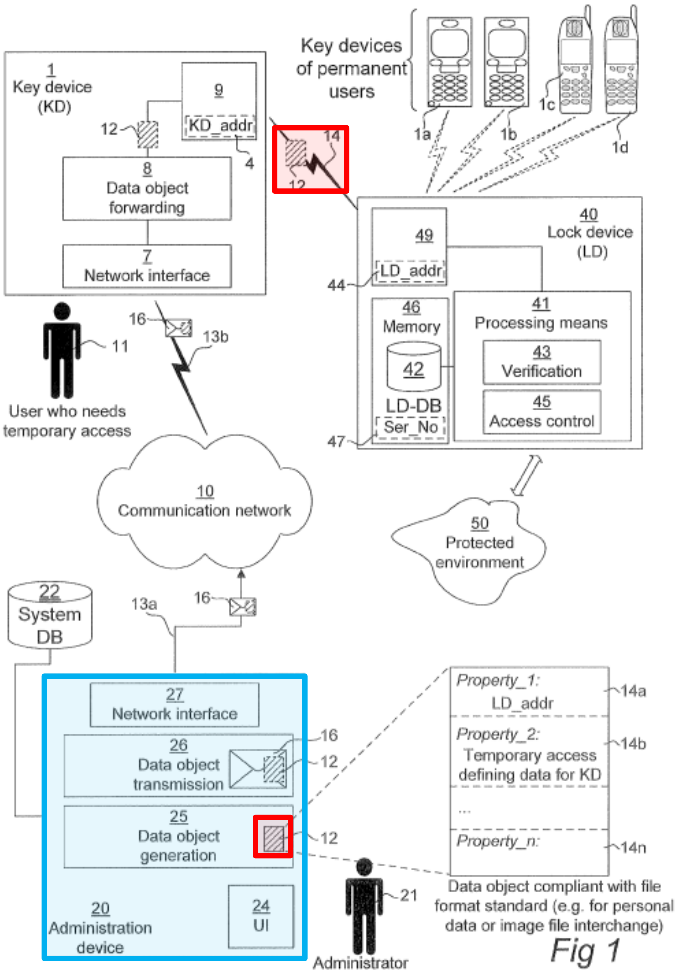


Knutsson, FIGS. 1, 3.

Knutsson discloses storing a communication address and a serial number "of the lock device … in local **memory** of the lock device." *Knutsson*, 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.*, 6:16-19. A POSA would have understood *Knutsson* teaches storing an encryption/decryption key in the memory of the lock device. Ex-1003, ¶¶129, 141.

Knutsson explains “that **all communication** between key device and lock device **may be encrypted** in accordance with an encryption algorithm, such as Blowfish.” *Knutsson*, 19:12-14; Ex-1003, ¶130.

In either case, the stored key would relate to communications that originate with *Knutsson*’s administration device 20, which is 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. Ex-1003, ¶¶130-131.



Knutsson, FIG. 1.

Knutsson does not expressly disclose that its key is a "public key," but *DeBry* does. *DeBry* teaches that, "[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 would be used to store a public key that is "distributed or published" in a public key system. Ex-1003, ¶132. A POSA would have been motivated to combine *DeBry* and *Knutsson*, as discussed above in Section VII.A. *Id.*

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**."

> **[19B]** "The method of claim 13 wherein at least a portion of the reservation certificate is encrypted by a server using a **private key** … 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."

Knutsson in view of *DeBry* renders obvious [7B]/[19B] because *Knutsson* discloses encryption/decryption of the reservation certificate and *DeBry* further discloses a specific encryption/decryption method using both public and private keys. Ex-1003, ¶¶133, 141.

DeBry discloses "a user who has made public a public key can … encrypt[] [a] message …with the user's private key before transmitting the message. Recipients of the message can verify the message … by decrypting it with the sender's public encryption key." *DeBry*, 3:11-16. Further, "[a]nyone who has the sender's public encryption key can read the message …. 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/decrypting system because *DeBry*'s system would have been an obvious existing use of encryption in similar access systems. Ex-1003, ¶134. A POSA would have been motivated to combine *DeBry* and *Knutsson*, as discussed above in Section VII.A. *Id.*

Knutsson's lock device activates after verification once "data integrity is ascertained," corresponding to the claimed "activating" step of [19B], and *Knutsson* further discloses "[i]f the outcome of these checks is fully positive… this will cause unlocking of the lock." *Knutsson*, 20:7-11; Ex-1003, ¶141.

C. Claims 11, 23

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"

[23A] "The method of claim 13 wherein … for which the corresponding **private key** is stored in a **memory** accessible to the processor"

Knutsson renders obvious [11A]/[23A] 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. Ex-1003, ¶¶135, 142.

Knutsson discloses "local memory 46 of the lock device," *Knutsson*, 12:19, 17:11-13; Ex-1003, ¶¶135-136.

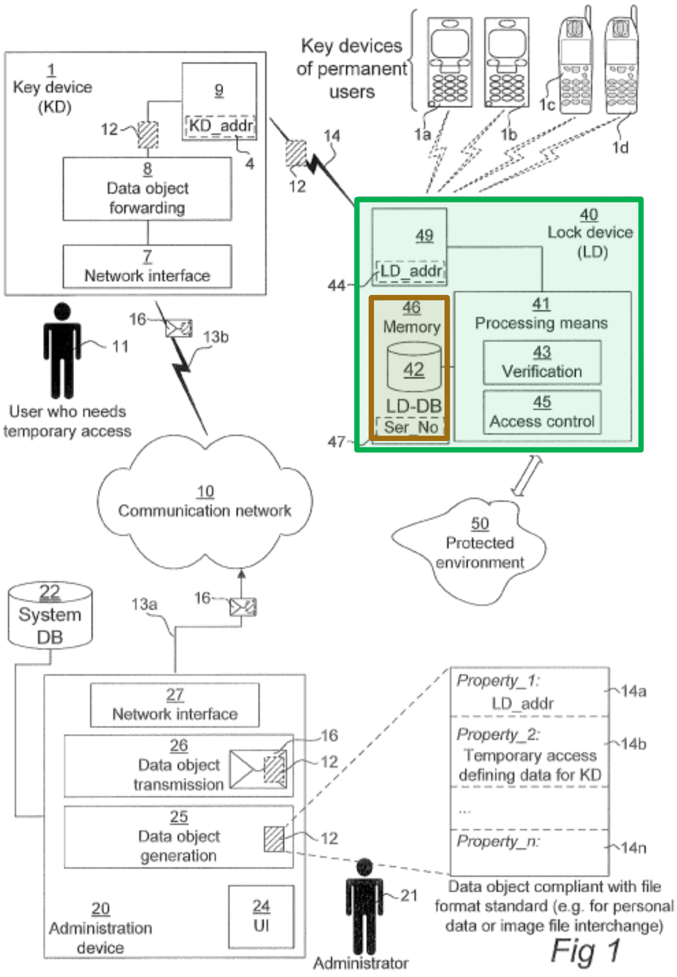
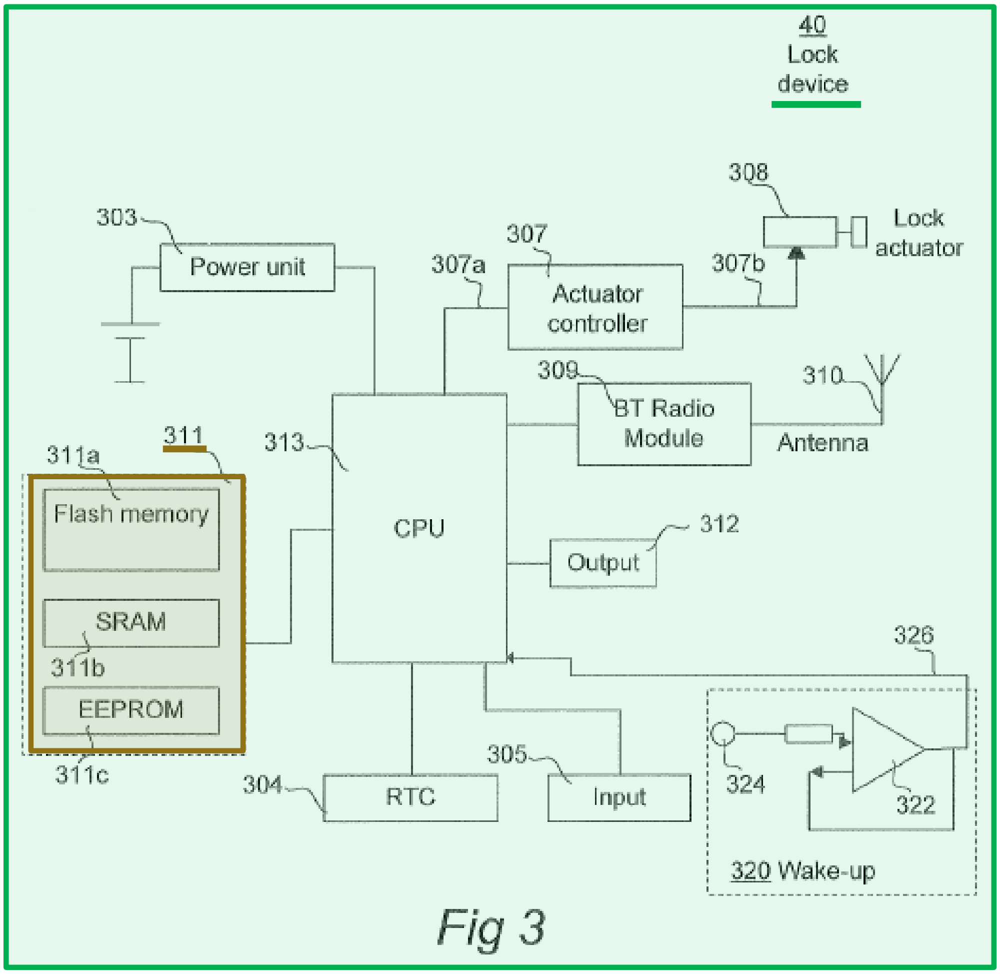

1
Key device
(KD)
9
KD_addr
12
4
8
Data object
forwarding
7
Network interface
Key devices
of permanent
users
1a
1b
1c
1d
14
12
40
Lock device
(LD)
49
LD_addr
44
46
Memory
42
LD-DB
Ser_No
47
41
Processing means
43
Verification
45
Access control
16
13b
11
User who needs
temporary access
10
Communication network
50
Protected
environment
22
System
DB
13a
16
27
Network interface
26
Data object
transmission
16
12
25
Data object
generation
12
20
Administration
device
24
UI
21
Administrator
Property_1:
LD_addr
14a
Property_2:
Temporary access
defining data for KD
14b
...
Property_n:
14n
Data object compliant with file
format standard (e.g. for personal
data or image file interchange)

Fig 1



Knutsson, FIGS. 1, 3.

As discussed above in Section VII.B, *Knutsson* discloses storing a communication address and serial number "in local memory of the lock device," *Knutsson*, 6:13-17, where they are used as an encryption/decryption key. *Id.*, 6:13-19. 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 would be stored on the lock device so that the received communication, such as *Knutsson*'s data object from a key device, is decrypted. Ex-1003, ¶137.

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 that, "[i]n a public key system, it is possible to communicate privately without transmitting any secret key." *DeBry*, 2:46-49. *DeBry* teaches that "[a]nyone desiring to communicate in private with a recipient merely encrypts the message under the recipient's public key .… [T]he **recipient** [i.e., the access device] … **retains the secret decrypting key** [and] … decipher[s] the transmitted message." *Id.*, 2:51-53. A POSA would have found it obvious that *Knutsson*'s memory 46 would be used to retain a private key in a public key system. Ex-1003, ¶138. A POSA would have found it obvious that *Knutsson*'s data object 12 would 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. *Id.*, ¶138; Section VII.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**."

[23B] "The method of claim 13 wherein at least a portion of the reservation certificate is **encrypted** by a server using a **public key** … the method further comprising the step of: d)

> **decrypting the portion**, by the processor, **with the private key**."

Knutsson in view of *DeBry* renders obvious [11B]/[23B] because *Knutsson* discloses encrypting/decrypting the reservation certificate and *DeBry* further discloses a specific encryption/decryption method using public and private keys. Ex-1003, ¶¶139, 142.

DeBry teaches "the encryption key is made public …. Anyone desiring to communicate in private with a recipient merely **encrypts** the message u[sing] the recipient's **public key** …. [T]he recipient …. retains the secret decrypting key" and "decipher[s] the … message," i.e., decrypts it with its private key. *DeBry*, 2:46-53; Ex-1003, ¶140. A POSA would have found it obvious to incorporate a known system of encrypting and decrypting using a public/private key pair as described by *DeBry* into *Knutsson*'s encrypting and decrypting system because *DeBry*'s system would have been an obvious existing use of encryption. Ex-1003, ¶¶139-140; Section VII.A.

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

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

As explained in Section III.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*. A POSA would have been motivated to implement *Woodard*'s access reporting system into *Knutsson*'s lock device 40 because *Woodard* discloses "automatically controlling access to an electronic lockbox utilizing showing appointment data maintained by a central showing management system." *Woodard*, [0010]; Ex-1003, ¶143. A POSA would have understood the importance of record keeping, particularly in hotels. Ex-1003, ¶143. A POSA would thus 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." *Woodard*, [0013]; Ex-1003, ¶143. Besides maintaining a complete record, 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." *Woodard*, [0068]; Ex-1003, ¶143.

A POSA would have had reasonable expectations of success combining *Woodard* and *Knutsson* because *Woodard* and *Knutsson* disclose similar key devices such as *Woodard*'s "electronic key device 104," a PDA or cell phone, *Woodard*, [0003], and *Knutsson*'s key device , also a PDA or a mobile phone, *Knutsson*, 4:32-5:4, to actuate access devices like *Woodard*'s lockbox 103 to "open" it, *Woodard*, [0048], or *Knutsson*'s lock device 40 to unlock a lock. *Knutsson*, 10:24-30; Ex-1003, ¶144. Commands in both cases are transmitted to an electronic lockbox or lock device (access device) to unlock a lock, and thus a

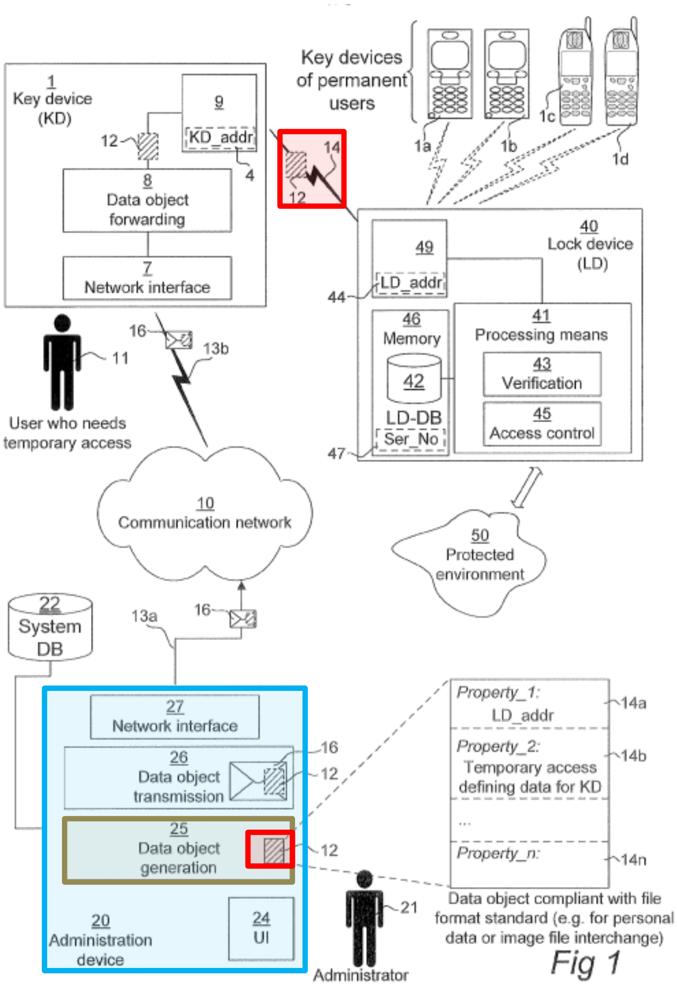
POSA would have implemented *Woodard*'s central management system with *Knutsson*'s lock devices. Ex-1003, ¶144.

B. Claims 12, 24

> **[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."
>
> **[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."

Knutsson in combination with *Woodard* renders obvious claims 12, 24. Ex-1003, ¶¶145-149.

Knutsson's administration device 20 can be a "server computer" and includes "data object generation module 25 [that] is configured to create a data object 12." *Id.*, 11:1-6, 11:24-26; Ex-1003, ¶146.



Id., FIG. 1.

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]. A POSA would have found it obvious to implement *Woodard*'s lockbox access records being reported to the system's servers via a communications link into *Knutsson*'s lock devices 40 and administration device 20. Ex-1003, ¶¶145-148. A POSA would have been motivated to combine *Woodard* and *Knutsson*, as discussed above in Section VIII.A. *Id.*

IX. 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*

As explained in Section III.B, *Elfström* discloses the majority of claim limitations. *Elfström*, however, does not expressly disclose comparing the interval of the reservation of the current reservation certificate to a current time accessible to the processor, determining the current time is within the interval of the reservation, and activating the door lock during the reservation interval. But *Woodard* does. Ex-1003, ¶149.

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]; Ex-1003, ¶150. A POSA would thus have incorporated *Woodard*'s automatic control concepts into *Elfström*'s access system to achieve a central management system. *Woodard*, [0012]; Ex-1003, ¶150.

A POSA would have further found it obvious to implement *Woodard*'s verification of an actual access time within a showing appointment time with *Elfström*'s access control module 116 to meet *Elfström*'s goal of confirming permissions. Ex-1003, ¶151. *Elfström*, 12:14-16. *Elfström* illustrates this point by explaining that "[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. A POSA would have been motivated to meet *Elfström*'s standards of "secure conditions" by verifying the time as disclosed in *Woodard*. Ex-1003, ¶151.

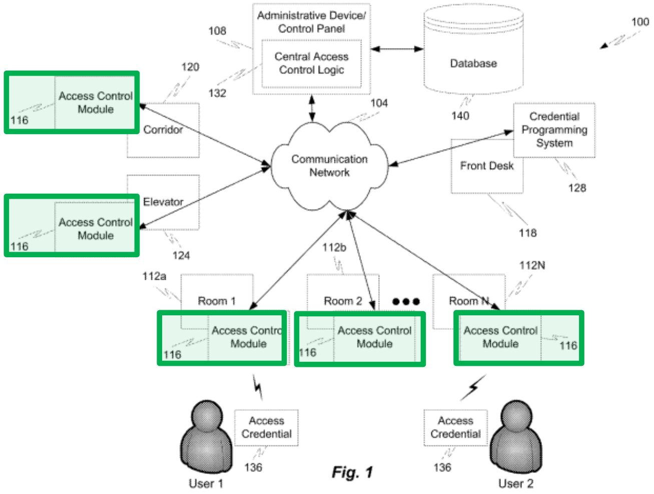
A POSA would have had reasonable expectations of implementing *Woodard*'s verification of an actual access time within a scheduled showing appointment time with *Elfström*'s access control module 116 because *Woodard* and *Elfström* disclose similar key devices such as *Woodard*'s "electronic key device 104, which can be a PDA, a cell phone," *Woodard*, [0003], and *Elfström*'s credential 136, also a PDA or a mobile phone, *Elfström*, 10:18-22, to actuate similar access devices like *Woodard*'s lockbox 103, *Woodard*, [0048], or *Elfström*'s access control device to open a lock. *Elfström*, 6:12-16; Ex-1003, ¶152.

B. Claims 1, 13

Elfström renders obvious claims 1, 13. Ex-1003, ¶¶153, 184.

1. [1p]/[13p]

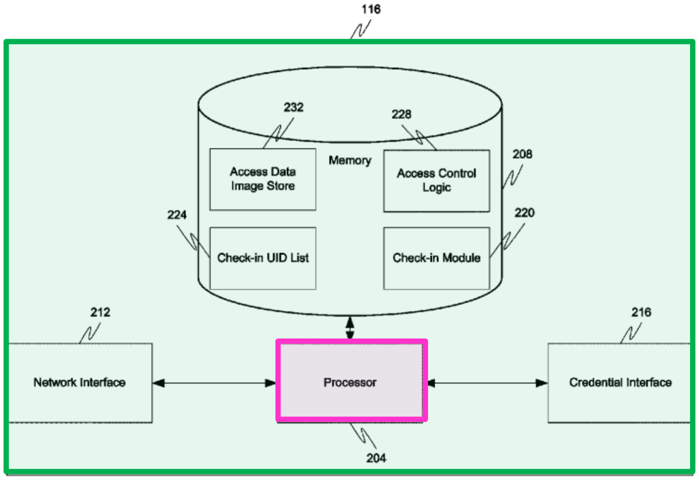
Elfström renders obvious [1p]/[13p] because *Elfström* discloses "**devices** for **controlling access** within a multi-facility room." *Elfström*, Abstract; Ex-1003, ¶¶154, 185. *Elfström* discloses its "**access control system** 100" includes "access control modules 116 [] adapted to communicate with access credentials 136 carried by users or guests of the multi-room facility." *Id.*, 4:58-65. *Elfström*'s access control module 116 includes a processor that controls an access control device including "an electronic lock … for a door." *Id.*, 5:60-61, 6:6-16; Ex-1003, ¶154.



Elfström, FIG. 1.

2. [1A]/[13A]

Elfström renders obvious [1A]/[13A]. Ex-1003, ¶¶155-156, 186. *Elfström* discloses "[c]onnected to the communication interface 216 is a controller or processor 204." *Elfström*, 5:60-61. "[P]rocessor 204 controls and determines how the access control module 116 behaves when a credential 136 is presented to it." *Id.*, 5:67-6:1; Ex-1003, ¶155.

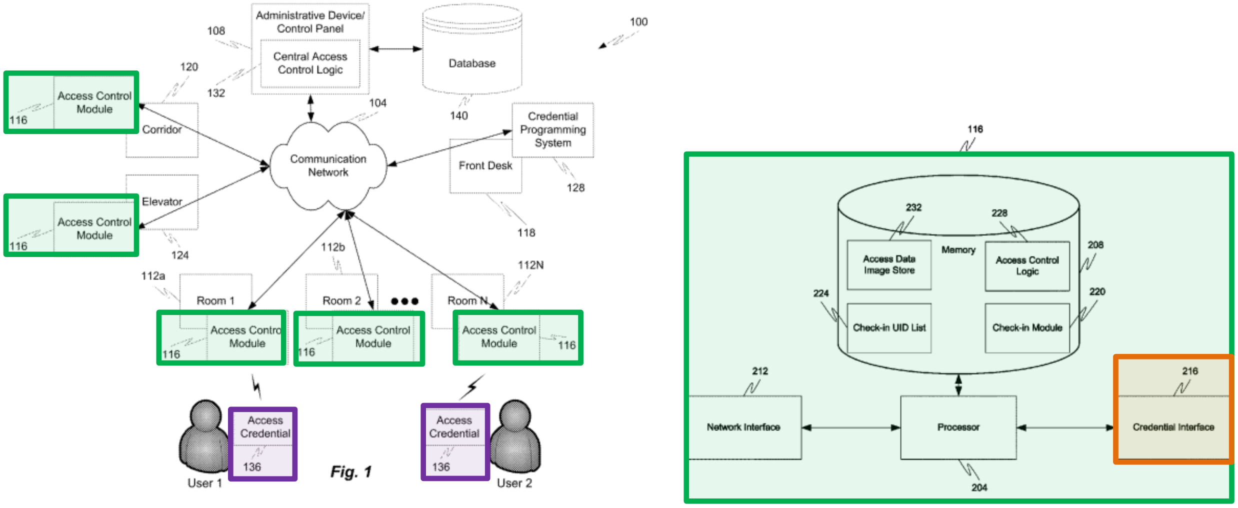


Knutsson, FIG. 2.

"The processor 204 is enabled to communicate with the access control device" that is "an electronic lock" and "access control modules 116 may be provided at access points to various physical assets" like "rooms 112 a-N." *Id.*, 4:32-35, 6:6-16; Ex-1003, ¶156.

3. [1B]/[13B]

Elfström renders obvious [1B]/[13B]. Ex-1003, ¶¶157-159. *Elfström* discloses its "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." *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.



Id., FIGS. 1, 2.

Elfström's access credential 136 may be "a **mobile phone**, PDA, … or the like." *Id.*, 10:19-22; Ex-1003, ¶158.

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; Ex-1003, ¶¶157-159.

4. [1C]/[13C]

Elfström renders obvious [1C]/[13C]. Ex-1003, ¶¶160, 188. *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 … at an access control module 116 enabled with a check-in module 220 (step 504)." *Elfström*, 11:54-56. *Elfström* discloses "access data images" are "written to a credential 136," and the "**access data may include … guest stay duration**." *Id.*, 8:7-9, 8:20-34, 12:29-36 ("stay duration (identifying either a departure date or an expiration date for the access data)"), claim 20.

5. [1D]/[13D]

Elfström renders obvious [1D]/[13D]. Ex-1003, ¶¶161, 189. *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 512, 516. *Elfström* discloses "access data images" of "a credential 136" that "may include … guest stay duration." *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, 6:16-20; Ex-1003, ¶¶161, 189.

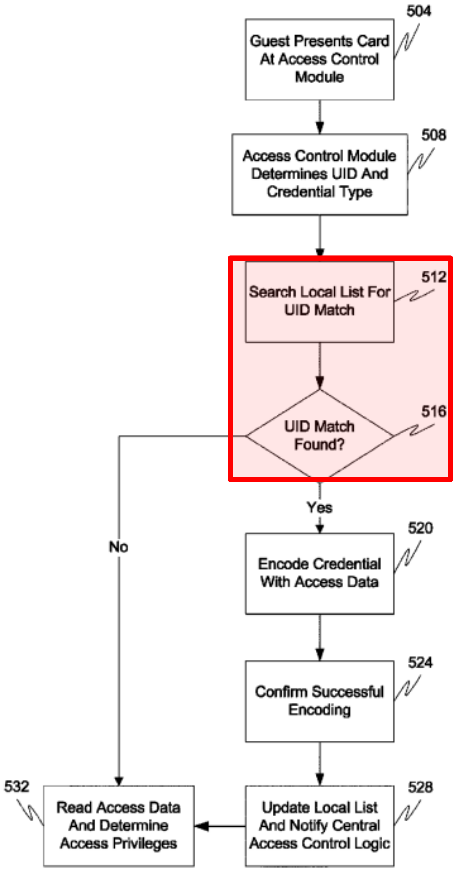

504
Guest Presents Card At Access Control Module
508
Access Control Module Determines UID And Credential Type
512
Search Local List For UID Match
516
UID Match Found?
Yes
No
520
Encode Credential With Access Data
524
Confirm Successful Encoding
528
Update Local List And Notify Central Access Control Logic
532
Read Access Data And Determine Access Privileges

Fig. 5

Id., FIG. 5.

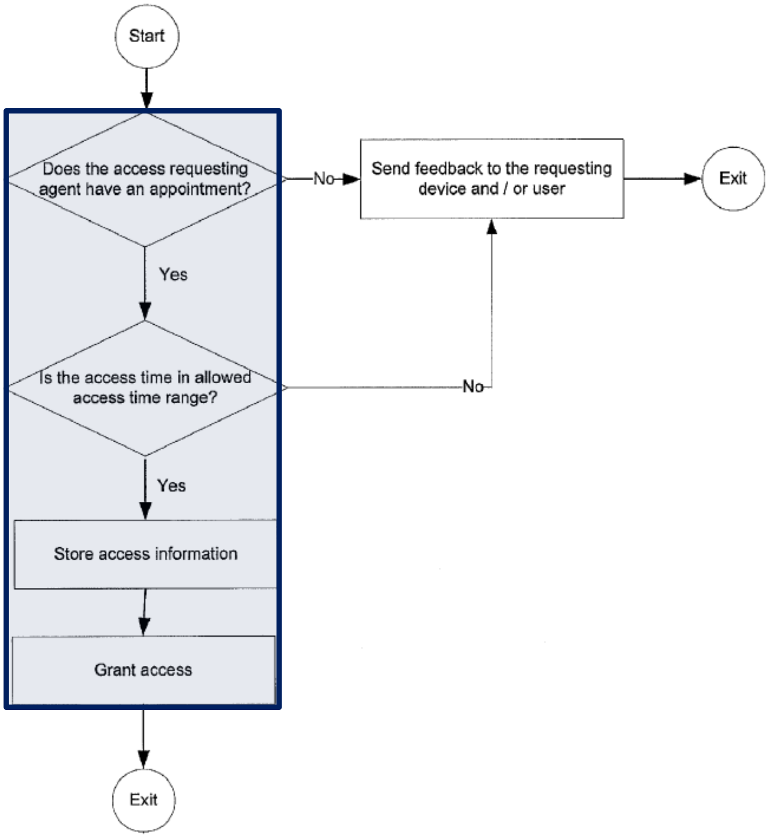
Elfström does not explicitly disclose "compar[ing] the interval of the reservation of the current reservation certificate to a current time accessible to the processor," but *Woodard* does. *Woodard* discloses "provid[ing] automatic access control to an electronic real estate lockbox utilizing showing 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*'s "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 include[s] … an internal controller [and] an accurate timer which may be capable of synchronization with a time server." *Id.*, [0051]. "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 appointment data (reservation certificate), including the data describing the showing time, is able to allow access (current). Ex-1003, ¶162. A POSA would have been motivated to combine *Elfström* and *Woodard*, as discussed above in Section IX.A. Ex-1003, ¶162.

6. [1E]/[13E]

Elfström renders obvious [1E]/[13E]. Ex-1003, ¶¶163, 190. *Elfström* discloses its access control module 116 includes processor 204 that controls an access control device including "an electronic lock … for a door." *Elfström*, 5:60-61, 6:6-16. "Thus, the access control logic 228 may facilitate … access data verification operations, and 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. One of those permissions is "duration," as discussed above in Section IX.B.4. *Elfström*, 8:7-9, 8:20-34, 12:29-36, claim 20. *Elfström* discloses "[i]f permissions are confirmed, then the access control module 116 will release … assets" like rooms. *Id.*, 12:14-16. *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 IX.B.5, "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. *Elfström*, 8:7-9, 8:20-34; Ex-1003, ¶163.

To the extent that *Elfström* does not disclose this limitation, *Woodard* does, as described above in Section IX.B.5, regarding *Woodard*'s disclosure of granting access "within the scheduled showing appointment time," *Woodard*, [0048], FIG. 9, corresponding to the claimed "during the interval of the reservation." Ex-1003, ¶164.

FIG. 9


Start
Does the access requesting agent have an appointment?
No
Send feedback to the requesting device and / or user
Exit
Yes
Is the access time in allowed access time range?
No
Yes
Store access information
Grant access
Exit

Woodard, FIG. 9.

A POSA would have been motivated to combine *Elfström* and *Woodard*, as discussed above in Section IX.A. Ex-1003, ¶165.

C. Claims 2, 14

1. [2A]/[14]

Elfström in view of *Woodard* renders obvious [2A]/14. Ex-1003, ¶¶166, 191. As discussed above in Section IX.B.5 for [1D]/[13D], *Woodard* discloses that "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 … and end exactly at the scheduled end time." *Id.*, [0012]. A POSA would have understood *Woodard*'s interval corresponds to the claimed "predetermined duration." Ex-1003, ¶166. 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." *Id.*

Woodard also teaches its "showing time period comprises a start time and one of a duration and an end time," thus disclosing that the data within *Elfström*'s access credential (certificate) is current from the start time to the "duration." *Woodard*, claim 2; Ex-1003, ¶167.

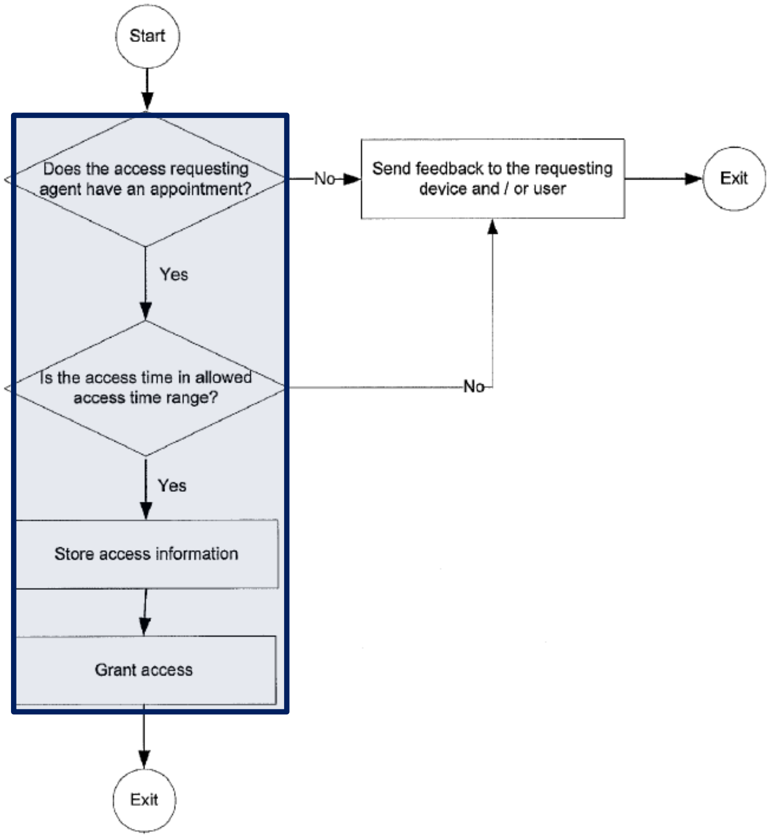
A POSA would have been motivated to combine *Elfström* and *Woodard*, as discussed above in Section IX.A. Ex-1003, ¶168.

2. [2B]

Elfström renders obvious [2B]. Ex-1003, ¶169. *Elfström* discloses its access control module 116 includes processor 204 that controls an access control device including "an electronic lock." *Elfström*, 5:60-61, 6:6-16. *Elfström* discloses unlocking a door if permissions are confirmed where one of those permissions is duration, as discussed above in Section IX.B.4. *Id.*, 8:7-9, 8:20-34, 12:29-36, claim 20. *Elfström* explains "[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*'s "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 IX.B.5, 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; Ex-1003, ¶169.

To the extent that *Elfström* does not disclose this limitation, *Woodard* does, as described above in Section IX.C.1, regarding *Woodard*'s disclosure of granting access "within the scheduled showing appointment time," corresponding to the claimed "from the start time up to the predetermined duration." *Woodard.*, [0048], FIG. 9; Ex-1003, ¶170.

FIG. 9


Start
Does the access requesting agent have an appointment?
No
Send feedback to the requesting device and / or user
Exit
Yes
Is the access time in allowed access time range?
No
Yes
Store access information
Grant access
Exit

Woodard, FIG. 9.

A POSA would have been motivated to combine *Elfström* and *Woodard*, as discussed above in Section IX.A. Ex-1003, ¶171.

D. Claims 3, 15

Elfström in view of *Woodard* renders obvious claims 3, 15. Ex-1003, ¶¶172, 192. As discussed above in Section IX.A.6, *Elfström* discloses its access control module 116 includes processor 204 that controls an access control device including "an electronic lock … for a door." *Elfström*, 5:60-61, 6:6-16. "If 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*'s "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; Ex-1003, ¶172.

As discussed above in Section IX.B.5, *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]. "The 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]. A POSA would have understood *Woodard*'s interval corresponds to the claimed "predetermined duration." Ex-1003, ¶173. 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." *Id.*

Woodard also discloses its "showing time period comprises a start time and one of a duration and an end time." *Woodard*, claim 2; Ex-1003, ¶174.

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. A POSA would have found it obvious that a "guest stay duration" in a hotel, as disclosed by *Elfström*, could be for one day as was commonly known, U.S. Patent Pub. No. 2010/0293011, [0025] (referring to "all available hotels having at least one day availability") corresponding to the claimed "all day." Ex-1003, ¶175.

E. Claims 4, 16

Claims 4, 16 are substantially similar to claims 2, 14 except that claims 2, 14 have additional limitations related to the "current time." For the same reasons discussed above in Section X.B, *Elfström*, alone or in view of *Woodard*, renders obvious claims 4, 16. Ex-1003, ¶¶176, 193.

F. Claims 6, 18

Elfström in view of *Woodard* renders obvious claims 6, 18. Ex-1003, ¶¶177, 196. *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]. "The 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]; Ex-1003, ¶177.

G. Claims 5, 17

Elfström in view of *Woodard* renders obvious claims 3, 15. Ex-1003, ¶¶178-179, 194-195. As discussed above for Section IX.F, *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]; Ex-1003, ¶178.

As discussed above in Section IX.B.6, *Elfström* discloses its access control module 116 includes processor 204 that controls an access control device including "an electronic lock … 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*'s "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. The *Elfström-Woodard* combination renders obvious actuating *Elfström*'s access control device within *Woodard*'s start time and end time. Ex-1003, ¶¶178-179.

H. Claims 9, 21

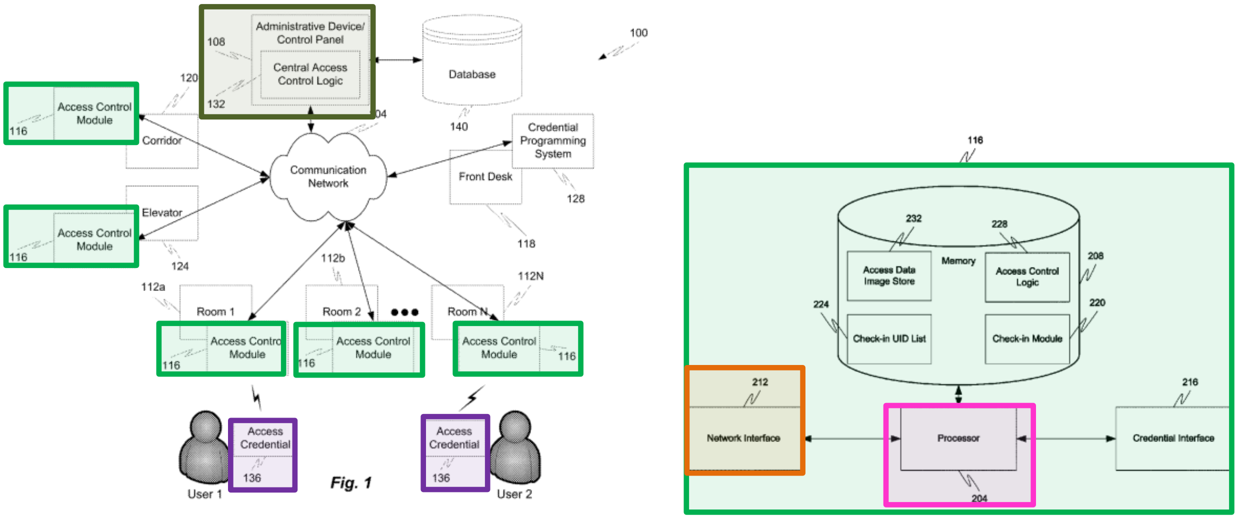
Elfström renders obvious claims 9, 21 because *Elfström* discloses "an instruction set (e.g., firmware, software, configuration data, and/or security data) is resident on the access control module 116 to support and control the functions of the access control module 116," *Elfström*, 4:54-57, and a POSA would have found it obvious that secure messages within *Elfström*'s secure access system 100 are verified as genuine. *Id.*, 3:51-54; Ex-1003, ¶¶180, 197. *Elfström* discloses its access control module 116 includes processor 204 that controls an access control device including "an electronic lock." *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. *Elfström* permits user access because 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; Ex-1003, ¶180.

I. Claims 10, 22

Elfström renders obvious claims 10, 22 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; Ex-1003, ¶¶181, 198.

J. Claims 12, 24

Elfström renders obvious claims 12, 24 because *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." *Id.*, 3:51-56. *Elfström* further discloses access control module 116's processor 204 communicates with other components in the network, such as administrative device 108, through network interface 212. *Id.*, 6:9-12; Ex-1003, ¶¶182, 199.



Elfström, FIGS. 1, 2.

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]. 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. Ex-1003, ¶183. A POSA would have been motivated to combine *Elfström* and *Woodard*, as discussed above in Section IX.A. *Id.*

X. 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*

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 IX.A. As explained in Section III.B, claims 7, 8, 11, 19, 20, and 23 further require encryption elements that are not expressly disclosed by *Elfström* and *Woodard*. Ex-1003, ¶200.

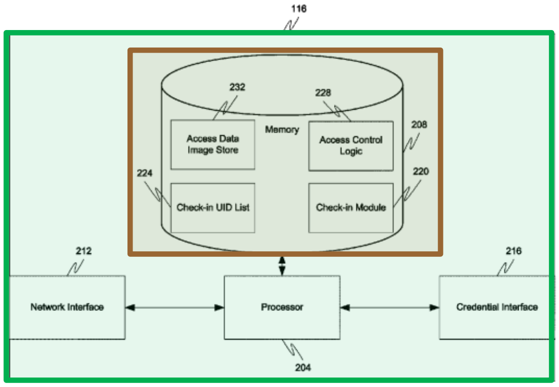
A POSA would have also been motivated to implement *DeBry*'s encryption methods into *Elfström*'s messages because *DeBry* discloses "[s]ome files must be encrypted at the sending end and decrypted at the receiving end to ensure that the file contents are not intercepted by an unauthorized entity during the transmission." *DeBry*, 1:54-57; Ex-1003, ¶201. A POSA would have found it obvious to incorporate a known system 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. Ex-1003, ¶201. A POSA would thus have incorporated *DeBry*'s encryption methods to avoid unauthorized interceptions. *Id.* Further, to meet *Elfström*'s goals of secure communication managed by administrative device 108, a POSA would have been motivated to implement *DeBry*'s method of ensuring authorized users through encryption. *Id.*

A POSA would have had reasonable expectations of success combining *DeBry* and *Elfström* because *DeBry*'s encryption methods are known methods of encrypting communications between one device to another, such as *DeBry*'s client system communicating with an electrical-mechanical system such as a printer, *DeBry*, 5:34-36, and *Elfström*'s credentials 136 that is a PDA or a mobile phone, *Elfström*, 10:19-22, communicating with *Elfström*'s access control module 116 to actuate *Elfström*'s door lock to open a lock. *Id.*, 5:60-61, 6:6-16; Ex-1003, ¶202.

B. Claims 7, 19

1. [7A]/[19A]

Elfström discloses "a memory to which the processor has access." *Elfström*'s "memory 208 and … 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." *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.

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; Ex-1003, ¶¶203-205.

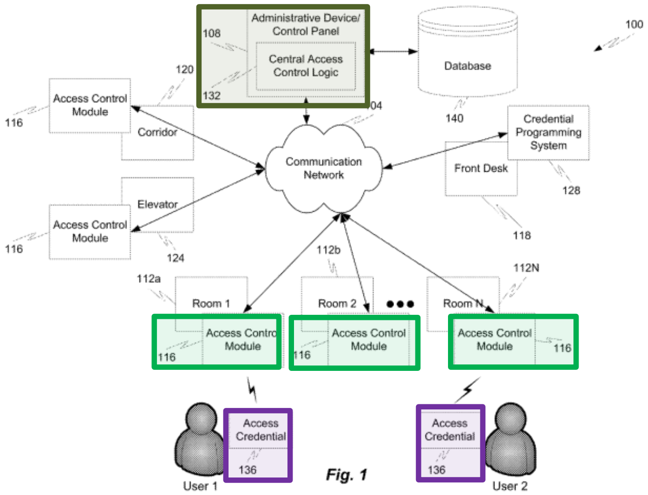


Fig. 1

Elfström, FIG. 1.

Elfström does not expressly disclose a public key, but *DeBry* does. *DeBry* teaches that, "[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 *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; Ex-1003, ¶206. A POSA would have been motivated to combine *DeBry* and the *Elfström-Woodard* combination, as disclosed above in Section X.A. Ex-1003, ¶206.

2. [7B]/[19B]

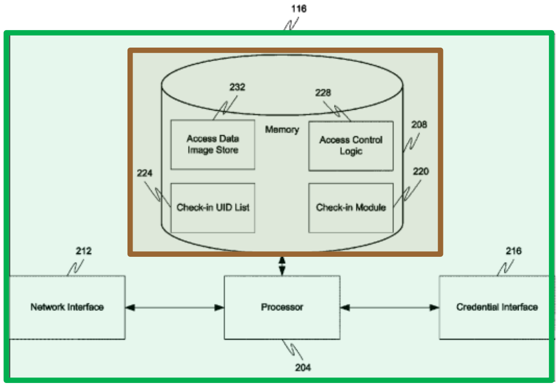
Elfström in view of *DeBry* renders obvious [7B]/[19B] because *DeBry* discloses a specific encryption method using both public and private keys. Ex-1003, ¶¶207, 220.

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* explains that "[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. *Elfström* discloses access to “an electronic lock” and that “[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,” *Elfström*, 12:14-16, such as determining that identification information matches the locally maintained list. *Id.*, 13:20-31. 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. Ex-1003, ¶208. A POSA would have been motivated to combine *DeBry* and the *Elfström-Woodard* combination, as disclosed above in Section X.A. *Id.*

C. Claims 8, 20

1. [8A]/[20A]

Elfström in view of *DeBry* renders obvious [7B]/[19B]. Ex-1003, ¶209. *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; Ex-1003, ¶¶209-210, 221. *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.

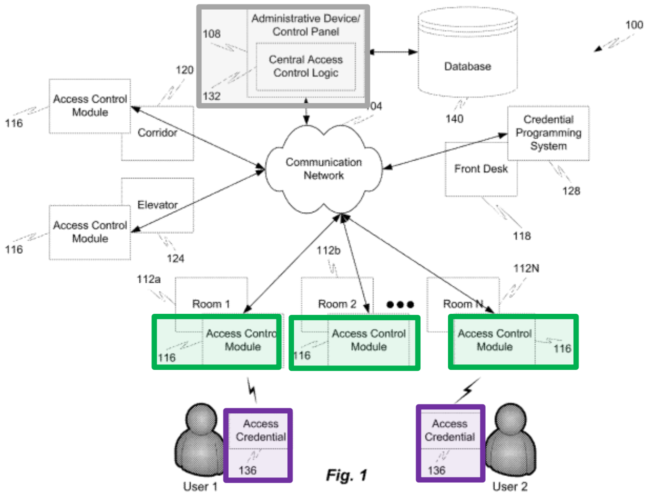
While *Elfström* discloses encryption, it does not expressly disclose a symmetrical key, but *DeBry* does. *DeBry* discloses "[c]onventional cryptography, or in other words traditional symmetric cryptography, is used to maintain the privacy of the information contents. Conventional cryptography requires 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 explained above in Section X.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. Ex-1003, ¶211. 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; Ex-1003, ¶211. A POSA would have been motivated to combine *DeBry* and the *Elfström-Woodard* combination, as disclosed above in Section X.A. Ex-1003, ¶211.

2. [8B]/[20B]

Elfström in combination with *Woodard* and *DeBry* renders obvious [8B]/20B. Ex-1003, ¶¶212, 221.

Elfström's use of encryption would occur with *Elfström*'s messages from credential 136 and/or administration device 106 that originates with *Elfström*'s administration device 106 which "an administrative device 108, which may also be referred to as a control panel." *Elfström*, 3:46-50. *Elfström*'s administration device 108 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.*, 3:51-56; Ex-1003, ¶¶212-213. *Elfström* discloses access to "an electronic lock" and that "[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,” *Elfström*, 12:14-16, such as determining that identification information matches the locally maintained list. *Id.*, 13:20-31.



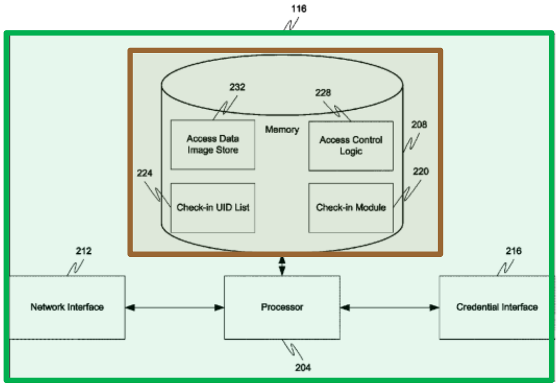
Id., FIG. 1.

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. Ex-1003, ¶¶213-214. A POSA would have been motivated to combine *DeBry* and the *Elfström-Woodard* combination, as disclosed above in Section X.A. *Id.*

D. Claims 11, 23

1. [11A]/[23A]

Elfström in combination with *Woodard* and *DeBry* renders obvious [11A]/[23A]. Ex-1003, ¶215. *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; Ex-1003, ¶¶215-216, 222. *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.

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. 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; Ex-1003, ¶217.

2. [11B]/[23B]

Elfström in combination with *Woodard* and *DeBry* renders obvious [11B]/[23B]. Ex-1003, ¶¶218, 222.

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. 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. Ex-1003, ¶219. A POSA would have been motivated to combine *DeBry* and the *Elfström-Woodard* combination, as disclosed above in Section X.A. *Id.*

XI. 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*

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 IX.A. As explained in Section III.B, claims 3 and 15 further require the reservation certificate to be valid for an interval of a predetermined duration that is all day. Ex-1003, ¶223.

A POSA, however, 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; Ex-1003, ¶224. *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; Ex-1003, ¶224. A POSA would thus have incorporated *Micali*'s duration of a certificate to improve security for smart doors and ensure credentials are valid. Ex-1003, ¶224.

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, *Micali*, 8:13-16, just like *Woodard*'s key device and *Elfström*'s credentials 136. Ex-1003, ¶225. Further, *Micali* describes known methods of use of digital certificates with a unique serial number, *Micali*, 4:62-63; 9:45-47, such as *Elfström*'s messages that include a unique identifier. *Elfström*, 8:25-27; Ex-1003, ¶225.

B. Claims 3, 15

Elfström in combination with *Woodard* and *DeBry* renders obvious claims 3, 15, because, as explained in Section IX.B.6, *Elfström* discloses its access control module 116 includes processor 204 that controls an access control device including "an electronic lock … for a door." *Elfström*, 5:60-61, 6:6-16; Ex-1003, ¶¶226, 229.

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.

As discussed above in Section IX.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." *Id.*, [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]. A POSA would have understood *Woodard*'s interval corresponds to the claimed "predetermined duration." Ex-1003, ¶227. 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." *Id.* *Woodard* also discloses "said showing time period comprises a start time and one of a duration and an end time." *Woodard*, claim 2; Ex-1003, ¶227.

To the extent that *Elfström* and *Woodard* do not disclose a "predetermined duration that is all day," *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, D1." *Micali*, 15:57-62. A POSA would have understood that a certificate could be issued for a day, as disclosed by *Micali*. Ex-1003, ¶¶228-229. 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," *Micali*, 18:17-19, corresponding to the claimed "reservation from the start time up to the predetermined duration that is all day." Ex-1003, ¶¶228-229. A POSA would have been motivated to combine *Micali* and the *Elfström-Woodard* combination, as disclosed above in Section XI.A. *Id.*

XII. DISCRETIONARY DENIAL IS IMPROPER

Non-institution under § 314(a) would be improper because no factors articulated in *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 5-6 (PTAB Mar. 20, 2020), weigh in favor of non-institution. No effective trial date has been set in either *Liberty Access Technologies Licensing LLC v. ASSA ABLOY AB et al.*, 2:22-cv-00507 (E.D. Tex.) ("the -00507 case") or *ASSA ABLOY Global Solutions, Inc. v. Liberty Access Technologies Licensing LLC*, 1:23-cv-00756 (N.D. Ill.) ("the -00756 case"). Ex-1016; Ex-1017. These cases are in their infancy. No invalidity contentions have been asserted and no Markman hearing date has been set. Petitioners filed counterclaims asserting invalidity in the -00756 case, but those counterclaims do not create a bar to institution. 35 U.S.C. § 315(a)(3); *Canfield Scientific, Inc. v. Melanoscan, LLC*, IPR2017-02125, Paper 7 (P.T.A.B. Mar. 30, 2018). Petitioners intend to seek a stay of these cases and, there is a high likelihood that a stay will be granted in the co-pending case because there has been virtually no investment in the parallel proceeding. Moreover, as invalidity contentions have not been asserted, there are no overlap of issues with this Petition.

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

Non-institution under § 325(d) would also be improper under the factors set forth in *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 (PTAB Dec. 15, 2017). The asserted combinations are materially different and not cumulative of the prior art involved during the examination of the challenged claims. During prosecution, no references were applied by the Office and the claims were issued only a double patenting rejection, Ex-1002 at 55-58, before being allowed barely a year after being filed. *Id.*, 90. During a supplemental examination initiated by the Patent Owner, U.S. Patent Publication No. 2003/0208386 to Bröndrup and WO Publication No. 2005/017840 to Rankl was considered with regards to the patentability of claims 1-24. Ex-1010 at 199. The Office ultimately allowed amended claims, noting that *Bröndrup* does not "1) receive a reservation interval [from] the phone requesting entry into the room, 2) have access to the current time and 3) compare a received interval to the current time." *Id.* at 275. The Office also stated that *Rankl* "does not send a reservation interval to the lock requested to be opened." *Id.* at 276.

The prior art references presented in this Petition were never listed by the Patent Owner nor cited by any examiner. They were never discussed or applied by an examiner to reject any claims. The cited references are materially different from and not cumulative of the earlier references at least because they describe (1) receiving a reservation certificate from a phone requesting entry into a room; (2) having access to the current time; and (3) comparing a received interval to the current time—elements that the Supplemental Examination stated were missing from *Bröndrup*. There is thus little to no overlap between the current and prior arguments. *Becton*, Paper 8, 23. As explained in this Petition, the cited references render obvious these limitations, making denial under § 325(d) improper.

XIII. MANDATORY NOTICES

A. Real Parties-in-Interest

The real parties-in-interest are ASSA ABLOY AB, ASSA ABLOY Mobile Services AB,[4] ASSA ABLOY Global Solutions, Inc., ASSA ABLOY Global Solutions AB, ASSA ABLOY Inc., HID Global Corp., and Marriott International, Inc.

B. Related Matters

Patent Owner has asserted the ’205 patent in litigation filed on May 23, 2018, *Liberty Access Technologies Licensing LLC v. Hilton Worldwide Holdings Inc. et al.*, 1:18-cv-03627 (N.D. Ill.).

Patent Owner has asserted the ’205 patent in litigation filed on August 18, 2022, *Liberty Access Technologies Licensing LLC v. Marriott International, Inc.*, 2:22-cv-00318 (E.D. Tex.).

Patent Owner has asserted the ’205 patent in litigation filed on December 30, 2022, *Liberty Access Technologies Licensing LLC v. ASSA ABLOY AB et al.*, 2:22-cv-00507 (E.D. Tex.).

[4] ASSA ABLOY Mobile Services AB was named as a party in the 2:22-cv-00507 E.D. Tex. litigation, but this entity does not exist.

ASSA ABLOY Global Solutions, Inc. has asserted non-infringement of the ’205 patent in a declaratory judgment action filed on February 7, 2023, *ASSA ABLOY Global Solutions, Inc. v. Liberty Access Technologies Licensing LLC*, 1:23-cv-00756 (N.D. Ill.).

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

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

XIV. GROUNDS FOR STANDING

Petitioners certify the ’205 patent is available for IPR, and Petitioners are not barred or estopped from requesting IPR challenging the patent claims on the grounds identified in this Petition.

XV. CONCLUSION

Petitioners have established a reasonable likelihood of prevailing with respect to each of the challenged claims 1-24 of the ’205 patent. Petitioners therefore request the Board institute *inter partes* review and cancel each of these claims as unpatentable.

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

Date: May 23, 2023

Respectfully Submitted,

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

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

Pursuant to 37 C.F.R. § 42.24(a)(1)(i), the undersigned hereby certifies that the foregoing PETITION FOR *INTER PARTES* REVIEW contains 13,656 words, excluding the parts of this Petition that are exempted under 37 C.F.R. § 42.24(a), as measured by the word-processing system used to prepare this paper.

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

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(a), the undersigned certifies that the foregoing **Petition for *Inter Partes* Review, the associated Power of Attorneys, and Exhibits 1001-1012, 1014, and 1016-1017** are being served on May 23, 2023, by FedEx Priority Overnight on the correspondence address of record indicated in the Patent Office's Patent Center system for U.S. Patent No. 9,373,205.

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

A courtesy copy has been served on litigation counsel at:

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

Date: May 23, 2023

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

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP