

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

<i>In re</i> patent of Chris Outwater et. al.	§	Attorney Docket: T4172-00009
	§	
U.S. Patent 11,373,474	§	
	§	
Issue Date: 2022-06-28	§	Customer No.: 39290
	§	
Filing Date: 2022-01-03	§	Real Party in Interest:
	§	
For: ACCESS CONTROL SYSTEM	§	Unified Patents LLC
AND METHOD FOR USE BY	§	
AN ACCESS DEVICE.	§	

**REQUEST FOR *EX PARTE* REEXAMINATION OF
U.S. PATENT 11,373,474**

Mail Stop “*Ex Parte* Reexam”
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

Pursuant to 35 U.S.C. §§ 301-307, Unified Patents, LLC (“Requester”) hereby requests an *ex parte* reexamination of Claims 1, 2, 5-9, 14-16, 19-20, 24, 26-27, 30, and 35 of U.S. Patent 11,373,474 (“the ’474 Patent,” EX-1001), which issued on June 28, 2022 to Chris Outwater and William Gibbens Redmann,

resulting from U.S. Patent Application 17/646,837, filed on January 3, 2022 as a continuation from several applications dating back to March 2, 2010.¹

This Request presents prior art references and analyses that were never presented before the Examiner during the original prosecution of the '474 Patent and demonstrates that Claims 1, 2, 5-9, 14-16, 19-20, 24, 26-27, 30, and 35 (“the Challenged Claims”) of the '474 Patent are invalid over these references.

Requester therefore requests that an order for reexamination and an Office Action rejecting Claims 1, 2, 5-9, 14-16, 19-20, 24, 26-27, 30, and 35 be issued.

¹ Because the '474 Patent's earliest possible effective filing date is before March 16, 2013, it is subject to the pre-AIA provisions of 35 U.S.C. et seq.

Ex Parte Patent Reexamination Filing Requirements

Pursuant to 37 C.F.R. § 1.510(b)(1), statements pointing out at least one substantial new question of patentability based on material, non-cumulative references for Claims 1, 2, 5-9, 14-16, 19-20, 24, 26-27, 30, and 35 of the '474 Patent are provided in Section III of this Request.

Pursuant to 37 C.F.R. § 1.510(b)(2), reexamination of Claims 1, 2, 5-9, 14-16, 19-20, 24, 26-27, 30, and 35 is requested, and a detailed explanation of the pertinence and manner of applying the cited references to Claims 1, 2, 5-9, 14-16, 19-20, 24, 26-27, 30, and 35 is provided in Section IV of this Request. The material and analysis in the request is fully supported by the expert testimony of Dr. Nick Feamster (Ex-1003). Additionally, the claim charts at Exhibits AA, BB and CC provide further support for the issues analyzed in this request, including more fulsome reproductions of the cited portions of the references relied upon herein.

Pursuant to 37 C.F.R. § 1.510(b)(3), copies of every patent or printed publication relied upon or referred to in the statement pointing out each substantial new question of patentability or in the detailed explanation of the pertinence and manner of applying the cited references are provided as Exhibits 1004-1008 of this Request.

Pursuant to 37 C.F.R. § 1.510(b)(4), a copy of the '474 Patent is provided as EX-1001 of this Request, along with a copy of any disclaimer, certificate of correction, and reexamination certificate issued corresponding to the patent.

Pursuant to 37 C.F.R. § 1.510(b)(5), the attached Certificate of Service indicates that a copy of this Request, in its entirety, has been served on the Patent Owner at its correspondence address of record in the patent file of the '474 Patent, in accordance with 37 C.F.R. § 1.33(a) and (c):

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

Also submitted herewith is the fee set forth in 37 C.F.R. § 1.20(c)(2).

Pursuant to 37 C.F.R. § 1.510(b)(6), Requester hereby certifies that the statutory estoppel provisions of 35 U.S.C. § 315(e)(1) and 35 U.S.C. § 325(e)(1) do not prohibit Requester from filing this *ex parte* patent reexamination request.

TABLE OF CONTENTS

	Page
I. SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY	1
II. OVERVIEW	1
A. Summary of the '474 Patent	2
B. Prosecution History	10
C. Claim Construction	11
D. Priority Date of the Challenged Claims	12
E. Person of Ordinary Skill in the Art	12
F. State of the Art	13
1. Access Devices	13
2. Applications on a Portable Terminal	14
3. Server	15
4. Reservation Certificate	15
5. Communication Settings	16
III. SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY	17
A. Prior Art	19
1. <i>Nielsen</i> (EX-1004)	19
2. <i>Kung</i> (EX-1005)	20
3. <i>Buckingham</i> (EX-1006)	20
4. <i>Ullmann</i> (EX-1007)	20
5. <i>Barnes</i> (EX-1008)	21

B.	Grounds 1 and 2: Anticipation and/or obviousness over <i>Nielsen</i> Presents Substantial New Questions of Patentability (Claims 8, 9, 14, 26, 27, 30 and 35).....	21
1.	<i>Nielsen</i>	21
C.	Ground 3: <i>Nielsen</i> in view of <i>Kung</i> and <i>Buckingham</i> Presents Substantial New Questions of Patentability (Claims 1, 2, 5-7, 15-16, 19-20 and 24)	23
1.	<i>Kung</i>	23
2.	<i>Buckingham</i>	26
3.	Motivation to combine.....	28
D.	Ground 4: <i>Ullmann</i> in view of <i>Barnes</i> Presents Substantial New Questions of Patentability (Claims 1, 8, 15, 26, 27 and 30)	30
1.	<i>Ullmann</i>	30
2.	<i>Barnes</i>	32
3.	Motivation to Combine	33
IV.	IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE	35
A.	Proposed rejections.....	35
B.	Proposed Rejection 1: Claims 8, 9, 14, 26, 27, 30 and 35 are anticipated by <i>Nielsen</i>	35
C.	Proposed Rejection 2, Claims 8, 9, 14, 26, 27, 30 and 35 are unpatentable over <i>Nielsen</i> in view of knowledge of a POSA.....	42
D.	Proposed Rejection 3, Claims 1, 2, 5-7, 15-16, 19-20 and 24 are unpatentable over <i>Nielsen</i> in view of <i>Kung</i> and <i>Buckingham</i>	52
E.	Proposed Rejection 4, Claims 1, 8, 15, 26, 27 and 30 are unpatentable over <i>Ullmann</i> in view of <i>Barnes</i>	67
F.	Secondary Considerations	84

V. DISCLOSURE OF CONCURRENT LITIGATION AND ADMINISTRATIVE PROCEEDINGS.....85

VI. CONCLUSION 85

Requester's Exhibit List

<i>Exhibit #</i>	<i>Description</i>
1001	U.S. Patent 11,373,474 ("the '474 Patent")
1002	Prosecution history of the '474 Patent ("File History")
1003	Declaration of Requester's Expert Nick Feamster, Ph.D.
1004	U.S. Patent 7,012,503 (" <i>Nielsen</i> ")
1005	US 2005/0021954 A1 (" <i>Kung</i> ")
1006	International Published Application WO 2006/101614 A1 (" <i>Buckingham</i> ")
1007	U.S. Patent 8,635,462 (" <i>Ullmann</i> ")
1008	U.S. Pub. No. 2007/0173266 (" <i>Barnes</i> ")
1009	U.S. Pub. No. 2009/0051486 (" <i>Denison</i> ")
1010	Prosecution history of U.S. Patent ("File history of the '258 Patent")
1011	Prosecution history of U.S. Patent ("File history of the '205 Patent")
1012	Prosecution history of U.S. Patent ("File history of the '876 Patent")
1013	Kerberos: An Authentication Service for Open Network Systems, Steiner, Newman, Schiller (1988) ("Steiner")
1014	The Bluetooth Radio System, Haartsen (2000) ("Haartsen")
1015	Neil Rhodes & Julie McKeehan, <i>Palm OS Programming: The Developer's Guide</i> , (Troy Mott ed., 2d ed. 2002) ("Palm OS")
1016	Chang-Seop Park, <i>On Certificate-Based Security Protocols for Wireless Mobile Communication Systems</i> , IEEE Network, Sept./Oct. 1997 ("Park")
AA	Claim Charts - Claims anticipated/obvious over Nielsen
BB	Claim Charts - Claims obvious over Nielsen in view of Kung and Buckingham
CC	Claim Charts - Claims obvious over Ullmann in view of Barnes

I. SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

Prior to describing the substantial new questions of patentability presented in this Request, provided below is an overview of the '474 Patent, its prosecution history, a discussion of claim construction, a summary of the prior art used in the present Request, and a summary of the state of technology relevant to the '474 Patent.

II. OVERVIEW

The Challenged Claims are unpatentable as anticipated or obvious over the prior art. The claims are directed to prior art systems and combinations of conventional components that perform conventional functions regarding wireless control of electronic locks, all of which was well known in the art. EX-1003 ¶ 32. At least the prior art references *Nielsen*, *Kung*, *Buckingham*, *Ullmann*, and *Barnes* as discussed in detail below, alone or in combination disclose each of the claimed limitations.

Because these references are all directed to the same problem and describe different levels of detail regarding the same set of solutions, these references are naturally combined together, and the combination discloses each limitation recited in the Challenged Claims. EX-1003 ¶ 33.

A. Summary of the '474 Patent

The '474 Patent is directed to systems and methods to allow a smartphone or any terminal to activate a door lock using a web site or server computer system.

The present invention relates to the use of a web site and a cellular telephone, preferably a smart phone, to reserve and activate an electric vehicle charger or to activate and allow access to any access device such as a hotel room lock or the like.

EX-1001 2:9-13; EX-1003 ¶ 34.

In particular the '474 Patent describes the use of a reservation certificate received at the smartphone from a server. EX-1001 4:17-22; EX-1003 ¶ 35. The smartphone may then activate the door lock by transmitting the certificate to the lock. EX-1001 6:21-26; EX-1003 ¶ 35. The certificate is described as including an “interval of the reservation.” As described in the claims, this interval of the reservation is compared to the current time in order to determine if the certificate is “current” (i.e., valid). EX-1001 Claim 1; EX-1003 ¶ 35. Two different embodiments are claimed: one in which a processor in the lock performs the comparison of the reservation certificate with the current time (Claims 8-13 and Claims 26-36), and a second in which the comparison is performed by an application on the smartphone (Claims 1-7 and Claims 15-25).

The claimed components of the system include a lock, an access device controlling a lock, an application running on a smartphone, a server and a reservation certificate

Claim 8 is representative:

8. *[pre]* An access control system comprising:

[a] an access device comprising a communication module connected to a processor having control of a door lock;

[b] an application on a portable terminal; and

[c] a server to provide a communication setting and a reservation certificate to the application, the communication setting corresponding to the access device, and the reservation certificate comprising an interval of a reservation,

[d] wherein the processor receives the reservation certificate from the application based on use by the application of the communications setting, and

[e] wherein the processor compares the interval of the reservation to a current time accessible to the processor to determine if the reservation certificate is current and

[f] wherein the processor activates the door lock when the processor determines that the reservation certificate is current.

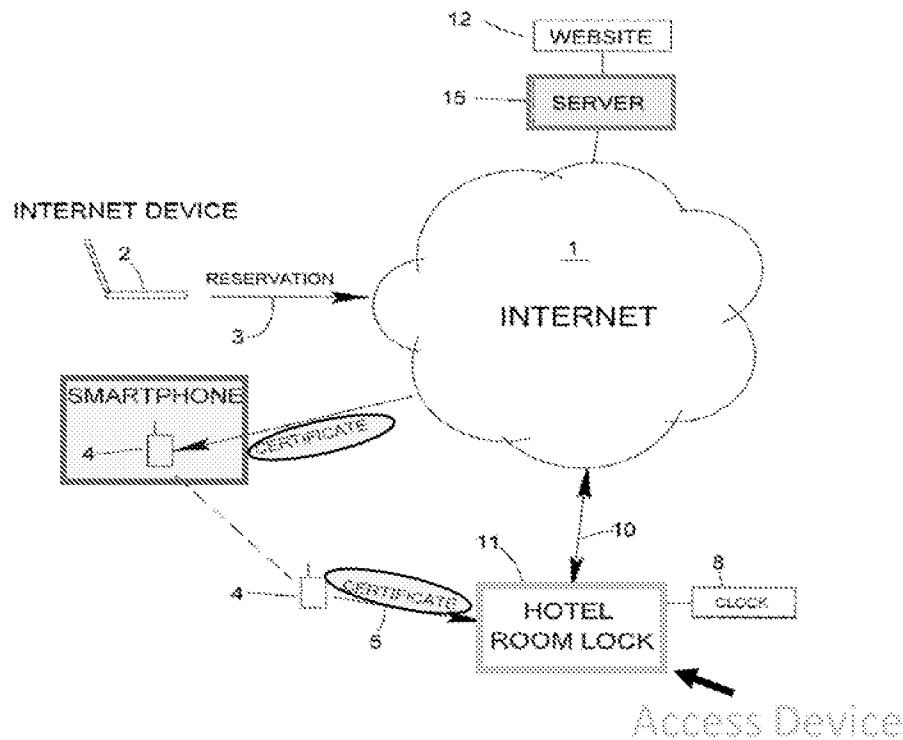


FIG. 4

EX-1001 Fig. 4 (annotated); EX-1003 ¶ 36.

Access device

The '474 Patent describes the components of the access device with respect to the charger 60 in Fig. 6. The access system includes a communication module (long range communication module 18 and/or Short Range Communication module 17) and a processor.

FIG. 6 shows a block diagram of a charger system 60 that is an embodiment of the charger of the present invention. A processor 16 is tied to a communication module 17 that performs short-range communication with a cellular telephone or smart phone...

EX-1001 6:30-34; EX-1003 ¶ 37.

An optional long-range communication module 18 can communicate with the Internet either by placing a cellular telephone call or with Wi-Fi or the like.

EX-1001 6:46-48; EX-1003 ¶ 37.

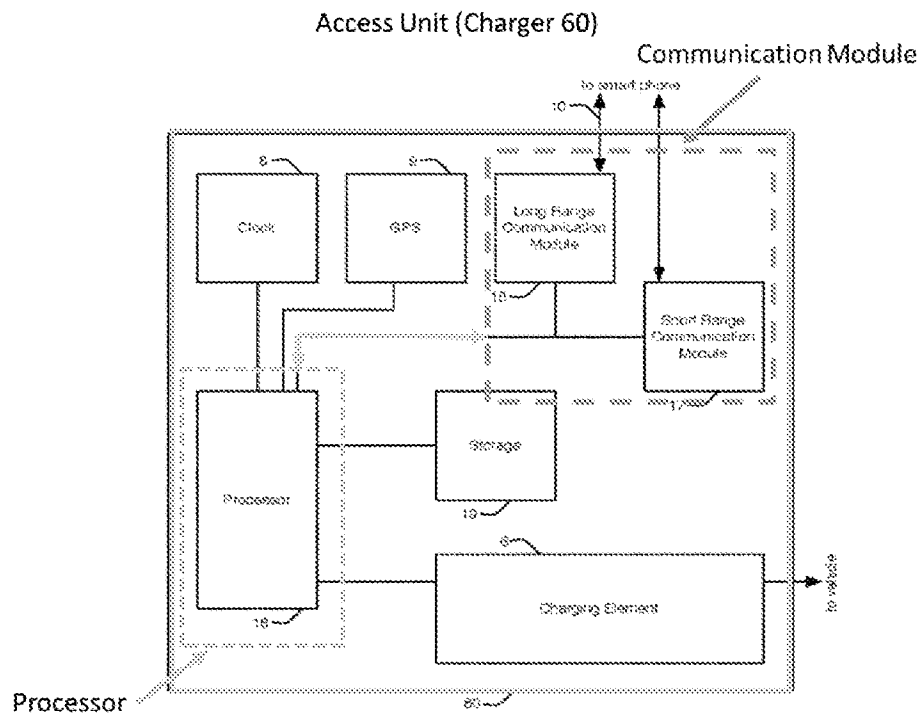


FIG. 6

EX-1001 Fig. 6 (annotated); EX-1003 ¶ 37.

The '474 Patent describes that the access device may or may not be Internet capable, and the access device communicates with the smartphone via a wireless technology.

The charger 6 (or access device 11, shown in FIG. 4) may be Internet capable, having connection 10 to Internet 1, or optionally it may be unconnected to the Internet 1 (as shown in FIG. 3 and FIG. 5 with no connection 10). As the cellular telephone 4 approaches the charger 6 (or access device 11, shown in FIGS. 4 & 5), a wireless technology such as BLUETOOTH, Wi-Fi, Zigbee, infrared, or other wireless technique can be used to communicate with the charger or access device.

EX-1001 4:51-59; EX-1003 ¶ 38.

Application on a portable terminal

The '474 Patent describes the application as running on a wireless device such as a smartphone or any portable computer with wireless communication ability.

If a wireless device, such as a laptop or smart phone, is used to carry the certificate, it can be running an application that turns on short-range wireless capability as the reservation time approaches. For simplicity in the following discussion, the term 'smart phone' is used, but will be understood to include any portable computer or PDA, having a wireless communication ability.

EX-1001 2:43-49; EX-1003 ¶ 39.

Server

The '474 Patent describes several functions of the server. Specifically, the server communicates with the smartphone or other internet terminal (3:62-67), it provides the certificate to the smartphone and in some embodiments provides the certificate to the access device (4:17-22). EX-1003 ¶ 40. The server may also encrypt the certificate (4:27-31) and host the website (3:62-64). EX-1003 ¶ 40.

Reservation Certificate

The '474 Patent describes the content of the certificate and how the certificate is passed through the system. The '474 Patent describes that the certificate is transferred from the server to the access device via the smartphone as shown Figs. 4 and 5. The certificate may include a unique ID, date/time stamp, start time, duration, and digital signature. The certificate may be encrypted.

The certificate generally has an ID referring to the final access device (for example, a charger), or is encoded in such a way that only the final access device can read and/or verify the message (e.g., the certificate may be encrypted with or signed with a public key for the final access device); whereby the final access device can recognize that the certificate is intended for it. The certificate generally has a start time and duration (or end time), describing the interval during which the final access device has been reserved. Additional options may also be included.

EX-1001 2:24-33; EX-1003 ¶ 41.

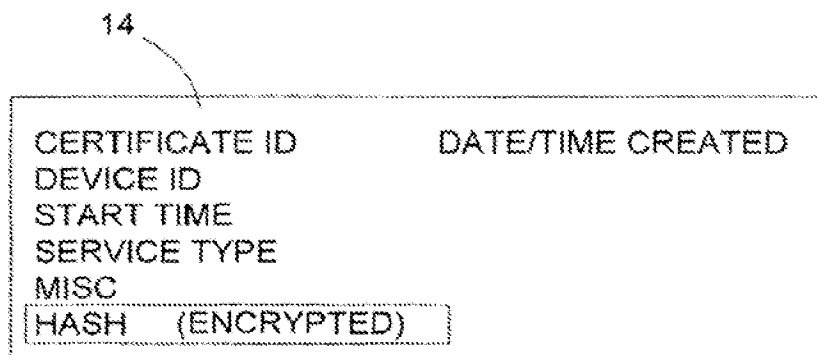


FIG. 2

EX-1001 Fig. 2; EX-1003 ¶ 41.

Communication Setting

The '474 Patent describes the application on the smartphone uses a predetermined communication setting or obtains one and provides examples “such as a Network SSID, IP addresses, Bluetooth ID, etc.” that “allow the application to identify and communicate” with a specific access device. EX-1001 4:60-5:3; EX-1003 ¶ 42. The '474 Patent describes the communication setting being part of the reservation certificate “wherein the reservation certificate comprises the communication setting.” EX-1001 Claim 7; EX-1003 ¶ 42.

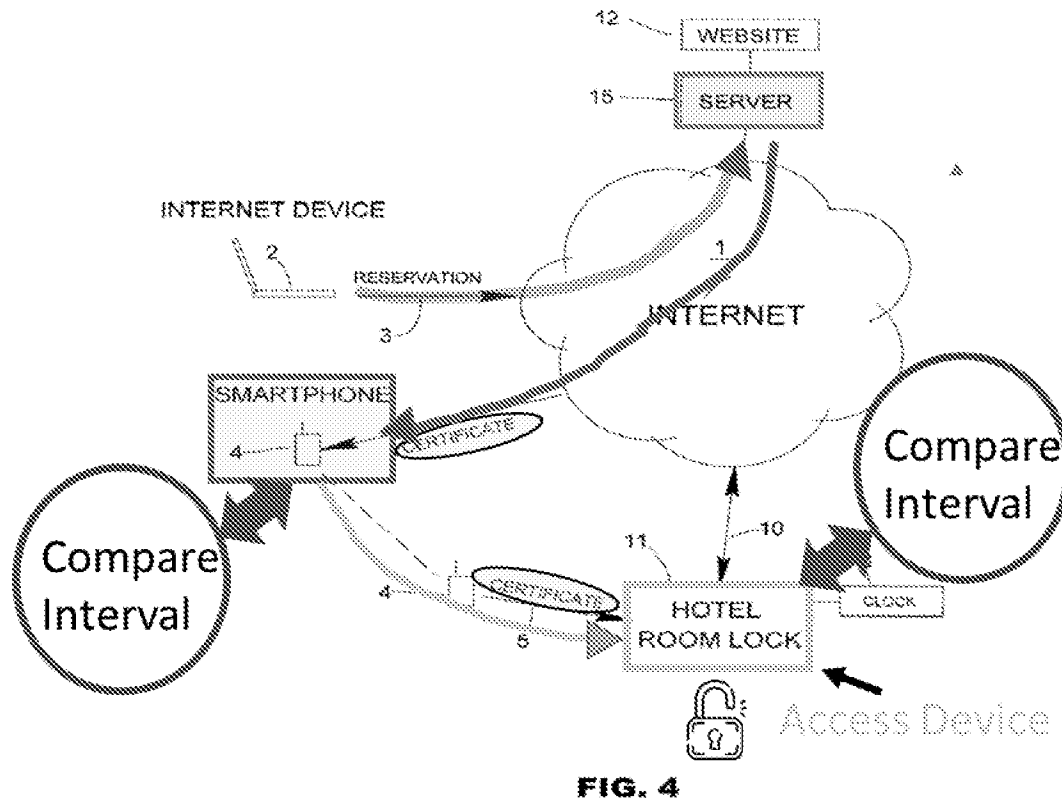
Operation

As shown below, the '474 Patent describes the process by which a user accesses the locked door. EX-1003 ¶ 43. A user places a reservation via a

browser, the server sends a certificate to a smartphone, and the smartphone sends the certificate to the lock device by way of a short range wireless technique. If the reservation period provided in the certificate corresponds with the current time as determined by the application or the access unit, access is granted (door unlocked).

In the case of a hotel room, a room reservation can be made using an Internet-enabled cellular telephone 4, laptop 2, computer or other Internet device. The room can be paid for in the usually e-commerce way by credit card or by any other payment method. The digital token or certificate is sent to the smart phone 4, and the user is told the external room number. As the guest approaches the hotel room door, the smart phone 4 sends the certificate 5 to the lock device by way of short-range wireless like BLUETOOTH. The user can then unlock the door at any time during the stay period by pressing a particular button on the phone or by other technique.

EX-1001 6:15-26; EX-1003 ¶ 43.



EX-1001 Fig. 4 (annotated); EX-1003 ¶ 43.

All of these limitations, however, were also well known in the art and were commonly used long before the '474 Patent, as demonstrated below. EX-1003 ¶ 44.

B. Prosecution History

The '474 Patent obtained allowance through a series of terminal disclaimers. The '474 Patent having a terminal disclaimer with respect to U.S. Pat. 9,911,258 ("the '258 Patent") (EX-1002 pp. 28-29), the '258 Patent having a terminal disclaimer with respect to U.S. Pat. 9,373,205 ("the '205 Patent") (EX-1010 pp.

55-56), and the '205 Patent having a terminal disclaimer with respect to U.S. Pat. 8,996,876 ("the '876 Patent") (EX-1011 pp. 24-25). The only art rejection in the string of continuations was with respect to the original claim set² (claiming a generic reservation system), which was subsequently cancelled and replaced with a claim set directed to electric vehicle charging. The applicant stated:

In particular, the feature of an electric vehicle charger has been incorporated into each of new independent claims 22 and 34, further differentiating them from the proposed combination of Yanai and Tanimoto.

EX-1012 p. 53.

The Office did not apply any prior art rejections to the current claims.

C. Claim Construction

The claims must be given their "broadest reasonable interpretation consistent with the specification." *See* MPEP § 2258; *In re Yamamoto*, 740 F.2d 1569, 222

² Original Claim 1 "1. A reservation system comprising: a server able to receive a reservation request from a first terminal and provide a reservation certificate to a portable second terminal in response to the reservation request; and, an access device able to receive and validate the reservation certificate from the portable second terminal and allow access in response." EX-1012 p. 170

USPQ 934 (Fed. Cir. 1984). This Request presents its claim analysis in a manner that is consistent with the broadest reasonable interpretation consistent with the specification.

Requester proposes that each claim term in the Challenged Claims be given its plain and ordinary meaning in this proceeding, and that no specific construction of any claim term is required because the prior art relied on in this Request meets each of the claim terms under any reasonable construction.

D. Priority Date of the Challenged Claims

The application that issued as the '474 Patent claims priority to provisional application number 61/309,813, filed on March 2, 2010. Requester does not concede that the '474 Patent is entitled to the March 2, 2010, earliest possible priority date. Nonetheless, because all of the prior art relied on herein antedates Mar. 2, 2010, a priority analysis is not necessary to find the Challenged Claims unpatentable.

E. Person of Ordinary Skill in the Art

At the time of the purported invention of the '474 Patent, a POSA would have been familiar with computer programming and wireless communications. EX-1003 ¶ 22. A POSA would have had a working knowledge of near-field and cellular communications and the Internet of Things (IoT). EX-1003 ¶ 22. A POSA would have gained knowledge of these concepts through a mixture of

training and work experience, such as by having a Bachelor's degree in computer science, computer programming, or electrical engineering, and two years of work experience in computer science, computer programming, or electrical engineering. A POSA may have more work experience with less formal education (e.g., four years of work experience without a Bachelor's degree) and vice versa (e.g., an advanced degree with no work experience). EX-1003 ¶ 22.

F. State of the Art

The following section describes the state of the art for wireless systems for physical access as of the filing date. EX-1003 ¶ 47. The prior art references, and the discussions of what was known to a POSA, provide the factual support for the general description of the state of the art at the time of the invention and provide additional motivation to modify or combine the references.

1. ACCESS DEVICES

Electromechanical devices for providing access were well known at the time of the purported invention of the '474 Patent. EX-1009 [0066]; EX-1003 ¶ 48. Examples of access devices that were well known include wireless controlled door locking systems, gate-locking systems, and building access systems. EX-1003 ¶ 48. Techniques for wirelessly controlling such devices to provide selective access to authorized individuals at authorized times were well known to a POSA. EX-1009 [0091, 92]; EX-1003 ¶ 48. Varying the implementation details of these

techniques was within the ordinary skill and general knowledge of a POSA, and was entirely predictable. EX-1003 ¶ 48. A POSA at the time of the purported invention would not have found anything new, surprising, counterintuitive, unpredictable, or technologically challenging about the access devices and access device operations described in the '474 Patent. EX-1003 ¶ 48.

2. APPLICATIONS ON A PORTABLE TERMINAL

The use of applications on portable terminals, such as the apps on a Palm OS device, as well as Apple or Android smartphones, were well known at the time of the purported invention of the '474 Patent. EX-1015 pp. xii-xiv, 3; EX-1003 ¶ 49. It was common and generally known in the art to use such applications for a wide variety of security purposes, including apps for gaining access to a door. EX-1003 ¶ 49. Techniques for using an application on a portable terminal for wirelessly controlling an access device were well known to a POSA. EX-1003 ¶ 49. Varying the implementation details of these techniques was within the ordinary skill and general knowledge of a POSA, and was entirely predictable. EX-1003 ¶ 49. A POSA at the time of the purported invention would not have found anything new, surprising, counterintuitive, unpredictable, or technologically challenging about the applications and application operations described in the '474 Patent. EX-1003 ¶ 49.

3. SERVER

The use of servers to hold or coordinate security information was well known at the time of the purported invention of the '474 Patent. EX-1016, p. 51 (describing, "Each mobile network has an authentication server (AS) which may be colocated with a location register. The AS (not shown in the figure) stores security-related parameters such as secret keys of mobile users"); EX-1003 ¶ 50. It was common and generally known in the art to use a server for a wide variety of security purposes, including selectively providing security information for use in obtaining access to a door. EX-1003 ¶ 50. Techniques for using such servers were well known to a POSA. EX-1003 ¶ 50. Varying the implementation details of these techniques was within the ordinary skill and general knowledge of a POSA, and was entirely predictable. EX-1003 ¶ 50. A POSA at the time of the purported invention would not have found anything new, surprising, counterintuitive, or technologically challenging about the servers and server operations described in the '474 Patent. EX-1003 ¶ 50.

4. RESERVATION CERTIFICATE

Using a reservation certificate to provide the secure details of a reservation was well known at the time of the purported invention of the '474 Patent. EX-1013 pp. 5-8; EX-1003 ¶ 51. It was common and generally known in the art to use a reservation certificate to selectively validate an access attempt for a particular

authorized entity for a specified validity time, such as is done to provide selective, valid access to a guest of a hotel or car reservation only during the time of the reservation. EX-1013 pp. 5-8; EX-1008 [0185-0191, 0194]; EX-1003 ¶ 51.

Providing security details of such a reservation certificate and validation was well known to a POSA. EX-1003 ¶ 51. Varying the implementation details of these techniques was within the ordinary skill and general knowledge of a POSA, and was entirely predictable. EX-1003 ¶ 51. A POSA at the time of the purported invention would not have found anything new, surprising, counterintuitive, unpredictable or technologically challenging about the reservation certificate and reservation certificate operations described in the '474 Patent. EX-1003 ¶ 51.

5. COMMUNICATION SETTINGS

Providing communication settings such as an ID to identify a device with which to communicate was well known at the time of the purported invention of the '474 Patent. EX-1014 pp. 28-36; EX-1003 ¶ 52. For example, Bluetooth ID and SSID were both well known IDs that identify a Bluetooth device and a Wi-Fi network respectively. It was common and generally known in the art to use such identifiers to identify a target of a transmission, and/or the medium by which it could be reached. Providing the settings identifying who and/or by what manner communications may be engaged was well known to a POSA. Varying the implementation details of these techniques was within the ordinary skill and

general knowledge of a POSA, and was entirely predictable. EX-1003 ¶ 52. A POSA at the time of the purported invention would not have found anything new, surprising, counterintuitive, unpredictable, or technologically challenging about providing a communication setting as described in the '474 Patent. EX-1003 ¶ 52.

III. SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

Requester submits that the *Nielsen*, *Kung*, *Buckingham*, *Ullmann*, and *Barnes* references cited herein raise a new “substantial question of patentability” because “the teaching of the (prior art) patents and printed publications is such that a reasonable examiner would consider the teaching to be important in deciding whether or not the claim is patentable.” *See* MPEP 2242. For example, the references introduced and discussed in further detail below and in the attached charts, when considered by themselves or as an ordered combination, teach each of the elements of the claims.

Table 1 is an overview generally illustrating the disclosures in each reference relative to the claim elements, with respect to representative Claim 8 of the '474 Patent:

8. *[pre]* An access control system comprising:

[a] an access device comprising a communication module connected to a processor having control of a door lock;

[b] an application on a portable terminal; and

[c] a server to provide a communication setting and a reservation certificate to the application, the communication setting corresponding to the access device, and the reservation certificate comprising an interval of a reservation,

[d] wherein the processor receives the reservation certificate from the application based on use by the application of the communications setting, and

[e] wherein the processor compares the interval of the reservation to a current time accessible to the processor to determine if the reservation certificate is current and

[f] wherein the processor activates the door lock when the processor determines that the reservation certificate is current.

TABLE 1

Claim Elements	Nielsen	Kung	Buckingham	Ullmann	Barnes
Access Device	Lock Control Unit	Wireless Door Lock	Electronic Lock	Locking Unit	Lock Unit
Application on Portable Terminal	Electronic Key Device	PAD	Primary Access Control Electronics	Mobile Device	Device With PAN
Server	Management System		Network Server	Central Processor	Hotel Computer System
Reservation Certificate With Interval	Access Code with Validity Period	Digital Certificate/ Service Key	Wireless Control And Data Communications	Authorization Information	Guest entry code/Data with

of Reservation					Temporal Data
Comparison of Interval of Reservation	Validation of Validity Period	Authentication	Processing Data Locally	Comparator Circuit	Determine Satisfaction of Temporal Criteria

Further, these references were never cited nor applied in an Office Action during prosecution of the '474 Patent; the “same question of patentability as to the claim has not been decided by the Office in an earlier concluded examination or review of the patent” (*MPEP 2242, Section I*) at least because there is no evidence that the art referenced in this request was considered by the Office during prosecution of the '474 Patent.

Further, to Requester’s knowledge, there has never been a prior post-grant proceeding challenging any claim of the '474 Patent, much less based on the prior art references of *Nielsen*, *Kung*, *Buckingham*, *Ullmann*, and *Barnes*.

A. Prior Art

I. NIELSEN (EX-1004)

U.S. Patent 7,012,503 (“*Nielsen*”) is titled ELECTRONIC KEY DEVICE A SYSTEM AND A METHOD OF MANAGING ELECTRONIC KEY INFORMATION. It issued on March 14, 2006, from an application filed on May 21, 2002. *Nielsen* qualifies as prior art under §102(b) (Pre-AIA). *Nielsen* was not cited or applied by the examiner during prosecution.

2. *KUNG (EX-1005)*

U.S. Patent Publication US 2005/0021954 A1 (“*Kung*”) is titled PERSONAL AUTHENTICATION DEVICE AND SYSTEM AND METHOD THEREOF. It published on January 27, 2005, from an application filed on July 1, 2003. *Kung* qualifies as prior art under §102(b) (Pre-AIA). *Kung* was not cited or applied by the examiner during prosecution.

3. *BUCKINGHAM (EX-1006)*

International Published Application WO 2006/101614 A1 (“*Buckingham*”) is titled REDUCED POWER ELECTRONIC LOCK SYSTEM. It published on September 28, 2006, from an application filed on February 7, 2006. *Buckingham* qualifies as prior art under §102(b) (Pre-AIA). *Buckingham* was not cited or applied by the examiner during prosecution.

4. *ULLMANN (EX-1007)*

U.S. Patent 8,635,462 (“*Ullmann*”) is titled METHOD AND DEVICE FOR MANAGING ACCESS CONTROL. It issued on January 21, 2014, from a PCT application filed on January 30, 2009, which entered the National Stage on July 28, 2010. *Ullmann* qualifies as prior art under §102(e) (Pre-AIA). *Ullmann* was not cited or applied by the examiner during prosecution.

5. BARNES (EX-1008)

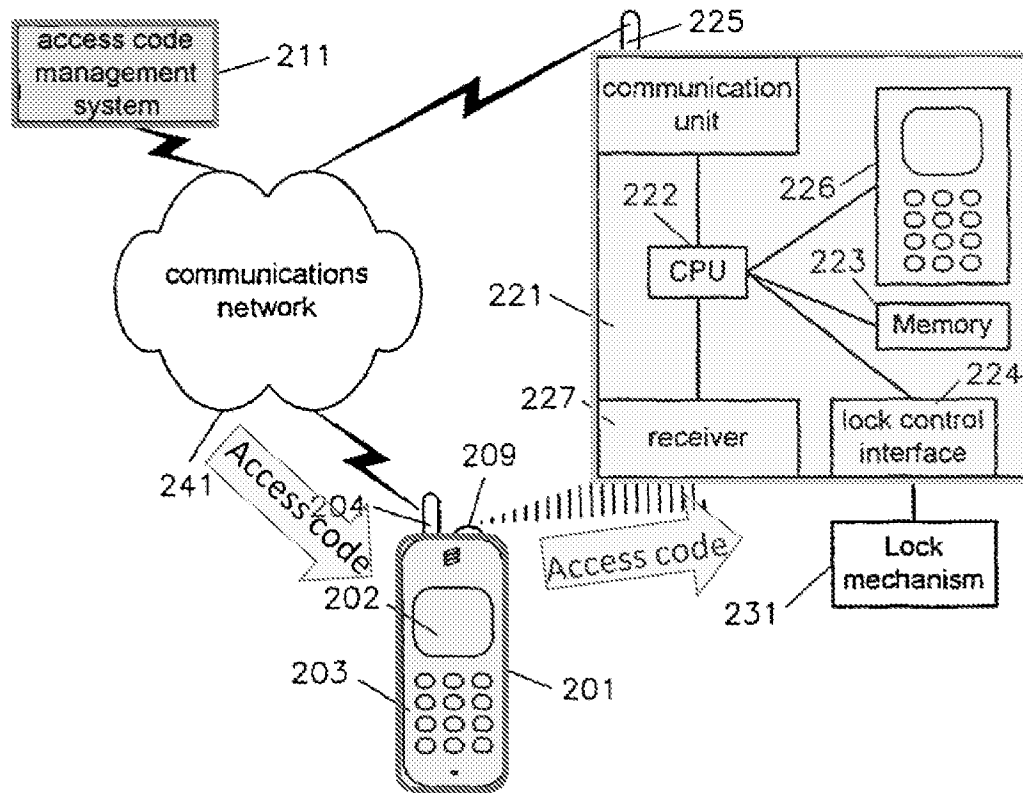
U.S. Patent Application Publication 2007/0173266 (“*Barnes*”) is titled PORTABLE COMMUNICATIONS DEVICE AND METHOD. It published on July 26, 2007, from application 11/696,387 filed on April 4, 2007. *Barnes* qualifies as prior art under at least §102(b) (Pre-AIA). *Barnes* was not cited or applied by the examiner during prosecution.

B. Grounds 1 and 2: Anticipation and/or obviousness over *Nielsen* Presents Substantial New Questions of Patentability (Claims 8, 9, 14, 26, 27, 30 and 35)

1. NIELSEN

Nielsen discloses a method and a system for controlling access to a location secured by a lock mechanism 231 controlled by a lock control unit 221 (*access device*). The method includes receiving a plurality of access codes including an access code (*reservation certificate*) from an access code management system 211 (*server*) at an electronic key device 201 (*application on portable terminal*). The access code of *Nielsen*, like the reservation certificate of the ’474 Patent, includes a device ID and a validity period. Using the electronic key device, access to the location is requested by initiating transmission of the access code (*reservation certificate*) to the lock control unit where the transmitted access code is validated, and if valid, operation of the lock mechanism is initiated. EX-1004 10:25-44, 11:44-49, 16:38-65; EX-1003 ¶ 54.

FIG. 2b



EX-1004 Fig 2b (annotated); EX-1003 ¶ 54.

Nielsen also discloses that the access code management system provides application software and communications software components and lock control unit ID (*communication settings*) along with the access codes to the application, “in order to enable the electronic key device 601 to perform the operations of storing, retrieving, selecting and transmitting access codes.” EX-1004 14:57-15:22, 17:18-24; EX-1003 ¶ 55.

All of the limitations of Claims 8, 9, 14, 26, 27, 30, and 35 are disclosed or obvious as shown in the Proposed Rejections 1 and 2, below and in the Claim Charts of Exhibit AA. EX-1003 ¶ 56.

C. Ground 3: *Nielsen* in view of *Kung* and *Buckingham* Presents Substantial New Questions of Patentability (Claims 1, 2, 5-7, 15-16, 19-20 and 24)

1. *KUNG*

Kung describes a flexible, tamper-resistant authentication system, or personal authentication device (PAD) (*portable terminal*), which can support applications in authentication, authorization, and accounting. EX-1005 Abstract; EX-1003 ¶ 57.

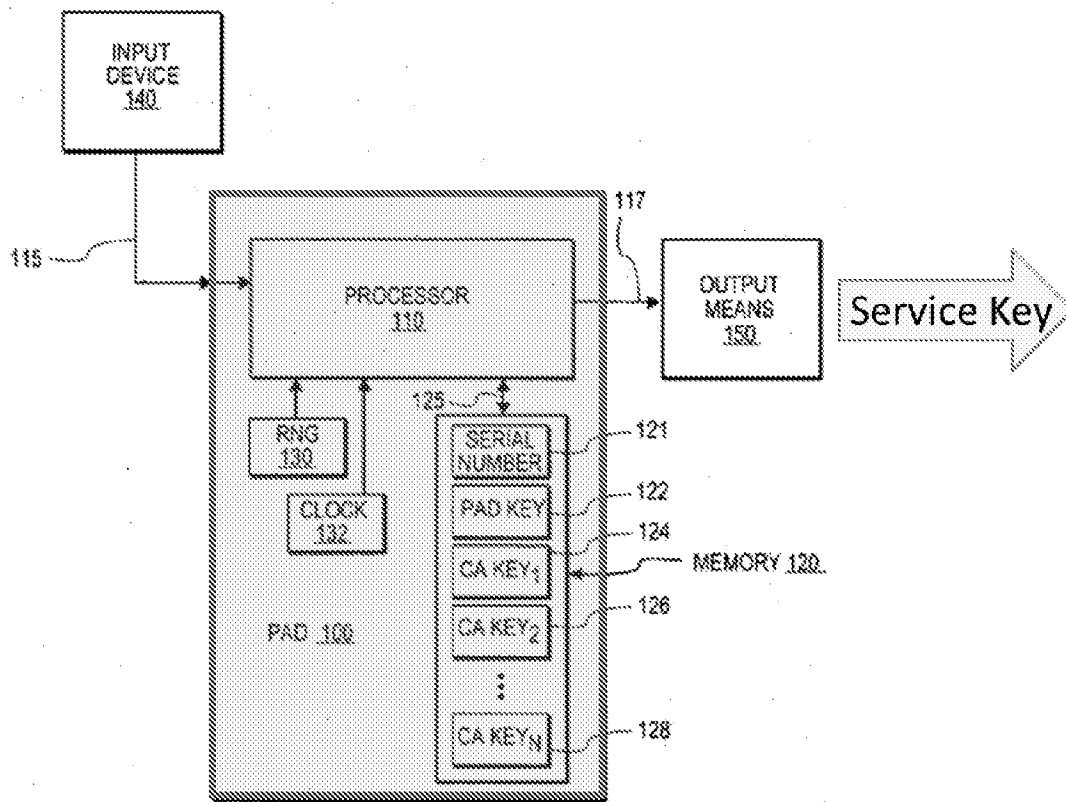


FIG. 1

EX-1005 Fig. 1 (annotated).

Kung's PAD 100 comprises an output device 150, as shown in Fig. 1, which is operatively connected to another device such as a door lock (*access device*).

Output device 150 may be any device capable of **outputting a service key** to any other devices such as a display, printer, card reader, USB device, **door lock**, handset or handheld device, personal digital assistant (PDA), personal computer, server, and/or Internet connection. Output device 150 may be used, for example, to wirelessly output a

service key to a door lock for opening a door, to a printer for printing a service coupon, or to a monitor for displaying a service number.

EX-1005 [0031] (emphasis added); EX-1003 ¶ 58.

Kung describes performing the validation of the certificate at the PAD:

[A]ll authentication operations may be performed at PAD 100 without needing Internet or network connections.

EX-1005 [0039]; EX-1003 ¶ 59.

Kung describes the validation of the certificate includes determining if it is still valid:

One or more of the digital certificates received in step 215 may be authenticated in step 220. Authentication of digital certificates may involve, for example, **checking whether the digital certificate is still valid**. As described above, a digital certificate may comprise information indicating a period of validity. If so, the process of authentication may involve checking the current date and time (which may be obtained, for example, from clock 132) against the validity period of the digital certificate.

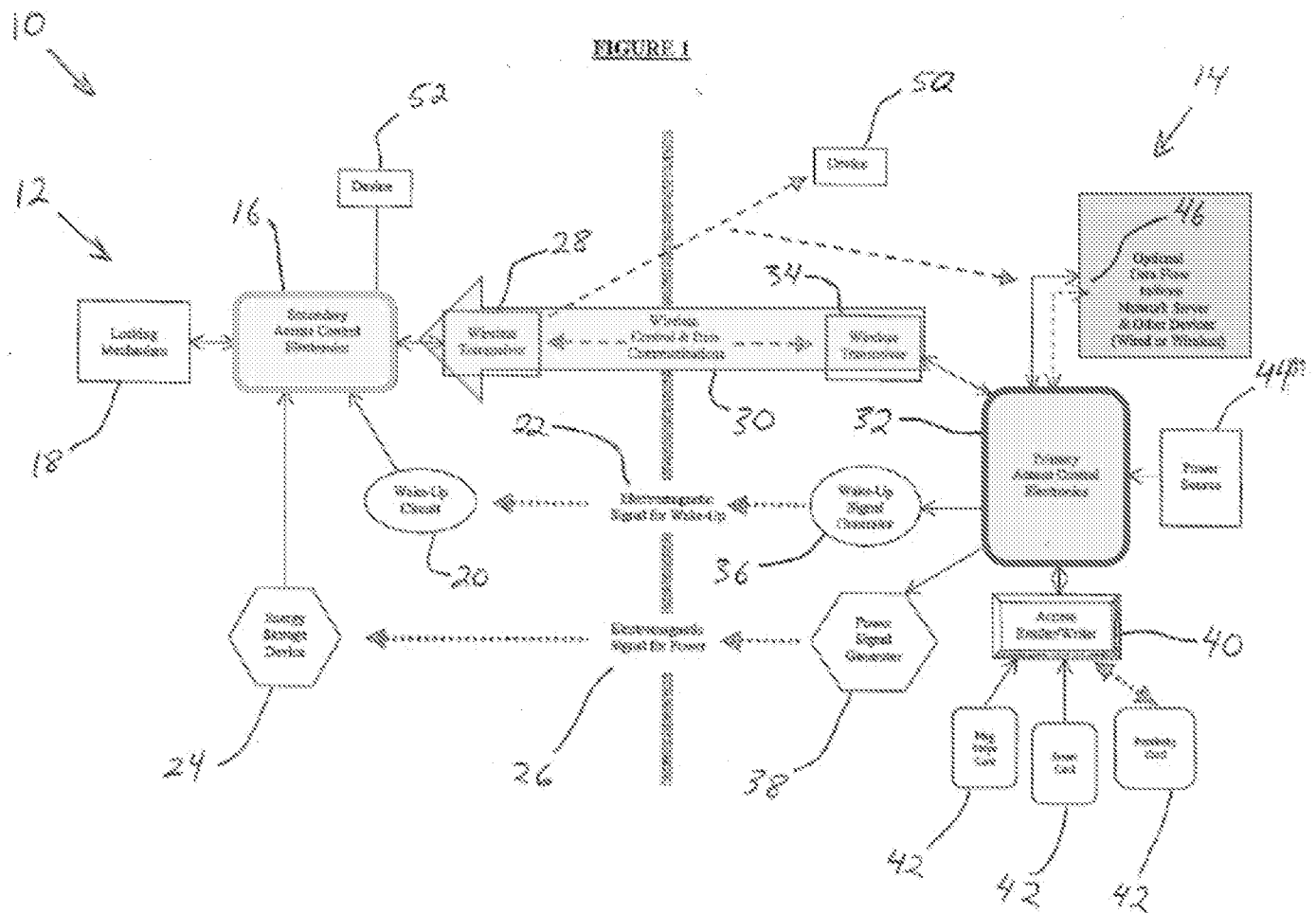
EX-1005 [0040] (emphasis added); EX-1003 ¶ 60.

2. *BUCKINGHAM*

Buckingham provides motivation to perform authentication or validation at the primary access control electronics (*portable terminal*) rather than the secondary access control electronics (*access device*). EX-1006 [0026]; EX-1003 ¶ 61.

Buckingham describes problems with both battery-powered locks and hard wired electronic locks. Specifically, for hotels with standalone electronic lock systems, battery replacement scheduling must be performed on the basis of “shortest expected battery life span”, regardless of whether some batteries may have continued functioning for several months or even a year beyond the replacement point in time, resulting in “significant expense.” EX-1006 [0003]; EX-1003 ¶ 62. *Buckingham* also describes wired electronic locks as having “very significant initial installation costs.” EX-1006 [0004]; EX-1003 ¶ 62.

Buckingham further describes that most of the energy required is a result of electronic functions other than physically operating the lock. EX-1006 [0005, 0006]; EX-1003 ¶ 63. *Buckingham* proposes a lock system which “uses reduced power,” and “fewer components.” EX-1006 [0008]; EX-1003 ¶ 63.



EX-1006 Fig. 1 (annotated); EX-1003 ¶ 63.

Buckingham describes a controller that processes identification data locally (or via network connection) and generating a wireless activation signal (*certificate*) at the controller (processor/remote device) transmitting the activation signal to the electronic lock (*access device*) and operating the electronic lock in response to the activation signal. EX-1006 [0012]; EX-1003 ¶ 64.

3. MOTIVATION TO COMBINE

Nielsen, *Kung*, and *Buckingham* as described above are each directed to controlling physical access via transfer of an access code to an electronic lock and thus are analogous art. EX-1003 ¶ 65.

Nielsen as described above discloses a method and a system for controlling access to a location, wherein an access code is received from a management system at an application on electronic device, which transfers the access codes to the lock unit. The access code including a validity period is validated by the lock control unit, and access is granted based upon the validation. However, *Nielsen* while explicitly disclosing the comparison of the validity period, does not provide and exhaustive recitation of the other components of the system that may also perform the comparison of the validity period. EX-1003 ¶ 66.

Kung provides an additional teaching that the authentication (*comparing*) of certificate information may be performed remotely from the lock control unit. Specifically, *Kung* discloses that the digital certificate information (*reservation certificate*) is received and may be authenticated at an application on a PAD. EX-1005 [0039]; EX-1003 ¶ 67. The process of authentication may involve checking the current date and time (which may be obtained, for example, from clock 132) against the validity period of the digital certificate. EX-1005 [0040]; EX-1003 ¶ 67.

Buckingham provides an explicit motivation to combine. *Buckingham* describes moving processing and functions from the access device to reduce power consumption from processing tasks and reduce costs. *Buckingham* describes that maintaining electronic circuitry accounts for a large amount of the power consumption in battery-powered electronic lock and it is desirably for a lock system to minimize the functions and components at the electronic locks. EX-1006 [0006, 0008]; EX-1003 ¶ 68.

Therefore, it would have been obvious to modify the system of *Nielsen* as described above to perform the authentication of the validity period at the PAD (application on a portable terminal) as taught by *Kung*. EX-1003 ¶ 69. A POSA would have been motivated to make the modification to reduce power consumption of the electronic lock (access unit) as well as costs associated with installment and maintenance of the electronic locks as taught by *Buckingham*. EX-1003 ¶ 69.

A POSA would have expected that the combination would have had a reasonable expectation of success because each of *Nielsen*, *Kung*, and *Buckingham* are directed to the same problem of selectively providing access to secure locations via the use of electronic locks and transmission of access codes. Electronic locks, wireless transmission of codes, distribution of information via a server, and subsequent authorization of those codes were well known and developed

techniques that were routinely used in various common applications (e.g., key cards, electronic automobile locks, contactless payments etc.). EX-1003 ¶ 70.

All the limitations of Claims 1, 2, 5-7, 15-16, 19-20 and 24 are disclosed and rendered obvious by *Nielsen*, *Kung* and *Buckingham* as shown in the Proposed Rejection 3, below and in the Claim Charts of Exhibit BB. EX-1003 ¶ 71.

D. Ground 4: *Ullmann* in view of *Barnes* Presents Substantial New Questions of Patentability (Claims 1, 8, 15, 16, 19, 26, 27 and 30)

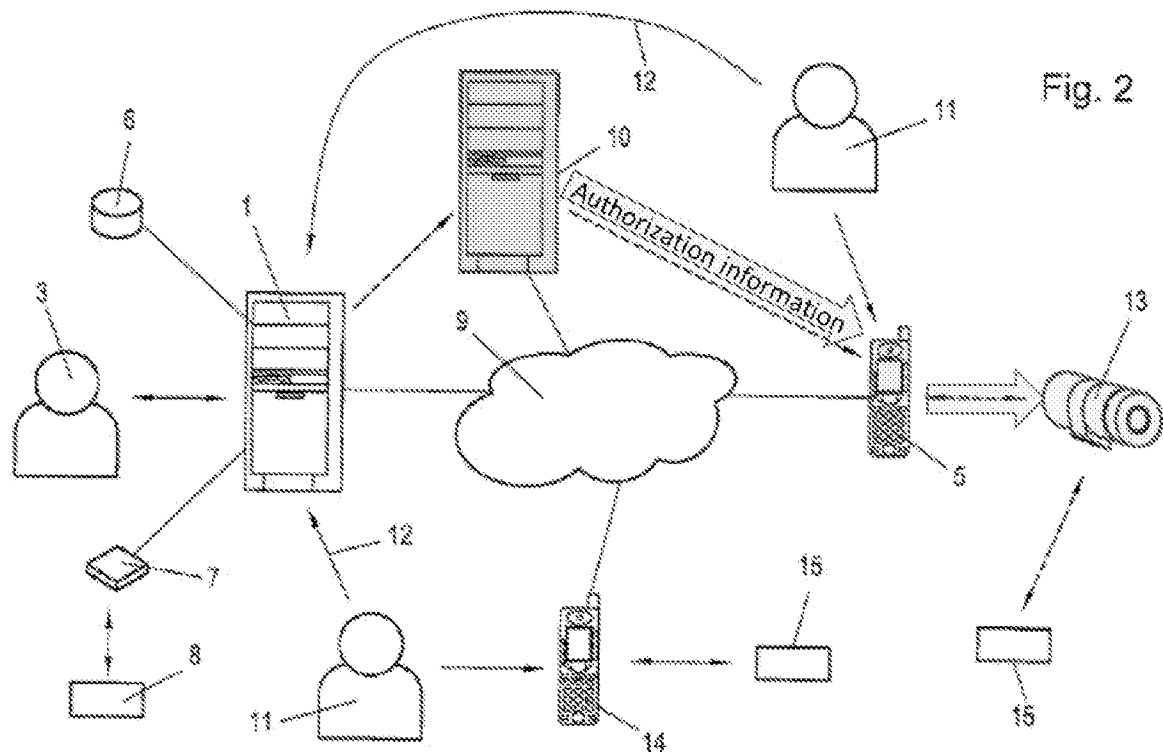
1. ULLMANN

Ullmann discloses a method for managing access control with locking units, particularly locks (*access device*), and electronic keys (*application on portable terminal*). *Ullmann* discloses access authorizations are stored and managed in a central processor, the keys are programmed with authorization information (*reservation certificate*) for a pre-specified given selection of locking units as a function of the respective access authorization. The authorization information is wirelessly sent from a key to a locking unit in the event of an access request, and the access authorization is determined in the locking unit as a function of the received authorization information. The programming of a key comprises the sending of the authorization information from a central processor (*server*) via a wireless telecommunication network to a wireless mobile telecommunication device and the transmitting of the authorization information received by the mobile

telecommunication device to a memory of the key. EX-1007 (Abstract); EX-1003

¶ 72.

Fig. 2 as annotated below shows the server (10), portable terminal (5) with an application, access device (13), and certificate (authorization information).



EX-1007 Fig. 2 (annotated); EX-1003 ¶ 73.

Ullmann also describes providing “a lock identification 101” in the authorization information to enable the mobile telecommunication device to communicate with the locking unit. EX-1007 8:24-44; EX-1003 ¶ 74.

Ullmann discloses broadly the use of authorization information (*reservation certificate*) to activate the locks (*access device*). However, *Barnes* provides

additional teachings with respect to the information contained within and the processing of check in information (*reservation certificate*). EX-1003 ¶ 75.

2. BARNES

Barnes describes the operation of portable communication device (*portable terminal*) allowing a guest to gain access to a hotel room. The hotel computer system (*server*) provides check in information to the device, which includes a room number identifying the hotel room to be communicated with (*communication setting*) and the guest's entry code (*reservation certificate*). The guest's entry code is wirelessly transmitted (preferably along with user or device authenticating data) from the device to the lock unit (*access device*) to unlock the door via a wireless personal area network (PAN). *Barnes* describes the transmission of the check in information is controlled by software (*application on the portable terminal*). EX-1008 [0005], [0027] [0122], [0185-0191].

Barnes describes that the wireless transmissions from the portable communication device are generated and sent only after certain criteria is determined to be satisfied. *Barnes* further discloses the criteria may include temporal data (validity period) and may be supplied to the portable communication device by the hotel. EX-1008 [0365], [0366], [0185-0191]; EX-1003 ¶ 77.

3. MOTIVATION TO COMBINE

Like *Nielsen*, *Kung*, and *Buckingham*, the prior art references *Ullmann* and *Barnes* as described above are directed to the same field of endeavor of controlling physical access via transfer of an access code to an electronic lock, specifically a home (*Ullmann* Fig. 1) and hotel room (*Barnes* [0024]), and thus are analogous art. EX-1003 ¶ 78.

Ullman also discloses, as described above, a method and a system for controlling physical access to a location, wherein an access code is received from a management system at an application on electronic device, which transfers the access codes to the lock unit, where the access code is validated and access is subject to the validation. Claims 1 and 8 respectively recited the access code includes a validity period and the validation is performed at the mobile (“reservation certificate comprising an interval of a reservation” and “wherein the application compares the interval of the reservation to a current time accessible to the application to determine if the reservation certificate is current.”). EX-1003 ¶ 79.

Barnes provides additional teachings regarding the inclusion of temporal criteria (*interval of a reservation*) in the transmission (*reservation certificate*) to the lock unit, as well as determining at the mobile device (*application on a portable terminal*) if the temporal criteria is satisfied prior to the transmission of

the guest's entry code. *Barnes* describes authentication based upon temporal and other criteria at the PAN. Specifically, in *Barnes* the device 101 can, at the election of the user, perform a desired action when one or more of location data, temporal data, activity data, and sensed input data satisfy criteria. EX-1008 [0366]; EX-1003 ¶ 80.

Therefore, it would have been obvious to modify the system of *Ullmann* as described above to include temporal data and determine if the temporal criteria (*interval of reservation*) supplied by the server is satisfied via the software on the portable terminal as taught by *Barnes*. EX-1003 ¶ 81. A POSA would have been motivated to include the temporal data taught by *Barnes* in the Authorization information of *Ullmann* in order to more precisely manage access and add another layer of security in preventing unauthorized access. EX-1003 ¶ 81. A POSA would have also been motivated to determine whether the criteria is satisfied via the application as taught by *Barnes* in order to leverage the processing assets of the user's portable terminal rather than expending the cost (in expense and energy usage) to incorporate the technology in the lock unit. EX-1003 ¶ 81.

IV. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Proposed rejections

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

B. Proposed Rejection 1: Claims 8, 9, 14, 26, 27, 30 and 35 are anticipated by *Nielsen*

Claims 8, 9, 14, 26, 27, 30, and 35 are anticipated under § 102 by U.S.

Patent 7,012,503 (“*Nielsen*.”). EX-1003 ¶ 82.

Claim 8³

Nielsen anticipates **an access control system** (See *Nielsen* “[a]n efficient method and a system for controlling access to a location secured by a lock mechanism controlled by a lock control unit,” Abstract; EX-1003 ¶¶ 83-84.)

comprising: an access device (See *Nielsen*, “lock control unit 221,” 10:55-11:27, 12: 42-54, Figs. 2a and 2b; EX-1003 ¶ 85.) **comprising a communication**

³ Claim language in Bold

module connected to a processor having control of a door lock (*See Nielsen*, the lock control unit 221 comprises a receiver 227 and a processing unit 222 connected to a lock control interface 224 which is adapted to control a lock mechanism 231, 10:55-11:27, 12:42-54, Figs. 2a and 2b; EX-1003 ¶ 85.);

an application on a portable terminal; (*See Nielsen*, “software application on electronic key device 201,” 10:34-41, 13:1-13, 17:18-28, Figs. 2a and 2b; EX-1003 ¶ 86) **and**

a server to provide a communication setting and a reservation certificate to the application, the communication setting corresponding to the access device (*See Nielsen*, Access code management system 211 includes a server that provides access codes including communications software components and device IDs to the software application to enable communication, e.g., “lock control unit ID 402,” 12:21-31, 14:57-15:22, 17:18-28, Figs 2a and 2b, Fig. 4; EX-1003 ¶ 87), **and the reservation certificate comprising an interval of a reservation,** (*See Nielsen*, “The access code illustrated in FIG. 4 further comprises additional optional fields, comprising information about the type of access rights” and these access rights include “additional parameters, e.g., validity period 410,” indicating a period of time for which the access code is valid, 14:57-15:22; EX-1003 ¶ 87).

wherein the processor receives the reservation certificate from the application based on use by the application of the communications setting,

(See *Nielsen*, “The lock control unit 221 comprises a receiver 227 for receiving the signal with the access code transmitted by the communications port 209 of the electronic key device 201,” and “[t]he receiver 227 is connected to a processing unit 222” (10:55-66); software applications/components and/or the identification of the lock control unit received from the access code management system enables transmission of access codes by the electronic key device, 17:18-28; EX-1003 ¶ 88,) and

wherein the processor compares the interval of the reservation to a current time accessible to the processor to determine if the reservation certificate is current (See *Nielsen*, “Block 689,” the lock control unit verifies the received access codes which include determining the applicability of the limited access rights, e.g., determining if the current time corresponds with the validity period 410, 14:57-15:22, 16:60-17:6, Fig. 6a; EX-1003 ¶ 89.) and

wherein the processor activates the door lock when the processor determines that the reservation certificate is current. (See *Nielsen*, “Block 690,” upon verification of the access codes including the validity period, “the lock mechanism is operated in step 690, thereby granting access to the location. The operation may comprise unlocking and/or locking the lock mechanism,... If the verification 689 of the access code fails, the lock mechanism is not operated,” 14:57-15:22, 16:60-17:6, Fig. 6a; EX-1003 ¶ 90).

Claim 9

Nielsen discloses **the access control system of claim 1 [8], wherein the communication setting is specific to the access device.** (See *Nielsen*, the communication setting includes “A lock control unit ID 402, which identifies the lock control unit” enabling the electronic key to communicate with the identified lock control unit, 14:57-15:22; EX-1003 ¶ 91).

Claim 14

Nielsen discloses **the access control system of claim 8, wherein the reservation certificate comprises the communication setting** (See *Nielsen*, “lock control unit ID 402” included in the access code provided to the electronic key devices and enables the transmission of access codes from the electronic key device to the respective lock control unit, 14:57-15:22, Fig. 4; EX-1003 ¶ 92).

Claim 26

Nielsen anticipates **an access control system** (See *Nielsen* “[a]n efficient method and a system for controlling access to a location secured by a lock mechanism controlled by a lock control unit,” Abstract; EX-1003 ¶¶ 93-94.)

comprising:

an access device (See *Nielsen*, “lock control unit 221,” 10:55-11:27, 12:42-54, Figs. 2a and 2b; EX-1003 ¶ 95.) **comprising a communication module connected to a processor having control of a door lock** (See *Nielsen*, the lock

control unit 221 comprises a receiver 227 and a processing unit 222 connected to a lock control interface 224 which is adapted to control a lock mechanism 231, 10:55-11:27, 12:42-54, Figs. 2a and 2b; EX-1003 ¶ 95.);

an application on a portable terminal (*See Nielsen*, “software application on electronic key device 201,” 10:34-41, 13:1-13, 16:19-27 and 17:18-28, Figs. 2a, 2b, 5a and 5b; EX-1003 ¶ 96); **and**

a server to provide a communication setting to the application, the communication setting corresponding to the access device (*See Nielsen*, Access code management system 211 includes a server that provides access codes including communications software components and device IDs to the software application to enable communication, e.g., “lock control unit ID 402,” 12:21-31, 14:57-15:22, 17:18-28, Figs 2a and 2b, Fig. 4; EX-1003 ¶ 97), **and further to provide, via a first communication protocol** (*See Nielsen*, a standard communications network 241 e.g., mobile telephone network, 12:3-21; EX-1003 ¶ 97), **a reservation certificate to the application**, (*See Nielsen*, Access code management system 211 provides access codes to the software application, 12:21-31, 17:18-28, Figs 2a and 2b, Fig. 4; EX-1003 ¶ 97) **the reservation certificate comprising an interval of a reservation** (*See Nielsen*, “The access code illustrated in FIG. 4 further comprises additional optional fields, comprising information about the type of access rights” including “additional parameters, e.g.,

validity period 410,” indicating a period of time for which the access code is valid, 14:57-15:22; EX-1003 ¶ 97),

wherein the processor receives the reservation certificate from the application (*See Nielsen*, The lock control unit 221 comprises a receiver 227 for receiving the signal with the access code transmitted by the communications port 209 of the electronic key device 201, the receiver 227 is connected to a processing unit that controls the retrieved access codes, software application enables transmission of access codes by electronic key device, 10:55-11:8, 17:18-28; EX-1003 ¶ 98) **via a second communication protocol that is different from the first communication protocol** (*See Nielsen*, the access code transmitted to the lock control unit from the key device is via “infrared signals or radio transmission,” 10:50-54, 16:19-27, versus the standard communications network 241 e.g., mobile telephone network, used to transmit the access code from the access code management system 211 to the electronic key device, 12:3-21; EX-1003 ¶ 98), **based on use by the application of the communication setting** (*See Nielsen*, Software application enables transmission of access codes by electronic key device, 10:55-11:8, 17:18-28; EX-1003 ¶ 98), **wherein the processor compares the interval of the reservation to a current time accessible to the processor to determine if the reservation certificate is current** (*See Nielsen*, “Block 689,” the lock control unit verifies the received access codes including determining the

applicability of the limited access rights, e.g., determining if the current time corresponds with the validity period 410, 14:57-15:22, 16:60-17:6, Fig. 6a; EX-1003 ¶ 98); **and wherein the processor activates the door lock when the processor determines that the reservation certificate is current.** (See *Nielsen*, “Block 690,” upon verification of the access codes including the validity period, “the lock mechanism is operated in step 690, thereby granting access to the location. The operation may comprise unlocking and/or locking the lock mechanism,... If the verification 689 of the access code fails, the lock mechanism is not operated,” 14:57-15:22, 16:60-17:6, Fig. 6a; EX-1003 ¶ 98).

Claim 27

Nielsen discloses **the access control system of claim 26, wherein the first communication protocol comprises a cellular protocol.** (See *Nielsen*, a standard communications network 241 e.g., mobile telephone network, 12:3-21; EX-1003 ¶ 99).

Claim 30

Nielsen discloses **the access control system of claim 26, wherein the second communication protocol comprises a short-range wireless protocol.** (See *Nielsen*, the access code transmitted to the lock control unit from the key device is via “infrared signals or radio transmission,” 10:50-54, 16:19-27; EX-1003 ¶ 100).

Claim 35

Nielsen discloses **the access control system of claim 26, wherein the reservation certificate is encrypted.** (See *Nielsen*, “To obtain the highest level of Security all electronic communication may be encrypted” 20:55-62; EX-1003 ¶ 101).

C. Proposed Rejection 2, Claims 8, 9, 14, 26, 27, 30 and 35 are unpatentable over *Nielsen* in view of knowledge of a POSA

Claim 8

Nielsen renders obvious **an access control system** (See *Nielsen* “[a]n efficient method and a system for controlling access to a location secured by a lock mechanism controlled by a lock control unit,” Abstract; EX-1003 ¶¶ 102-103.)
comprising:

an access device (See *Nielsen*, “lock control unit 221,” 10:55-11:27, 12:42-54, Figs. 2a and 2b; EX-1003 ¶ 104) **comprising a communication module connected to a processor having control of a door lock** (See *Nielsen*, the lock control unit 221 comprises a receiver 227 and a processing unit 222 connected to a lock control interface 224 which is adapted to control a lock mechanism 231, 10:55-11:27, 12:42-54, Figs. 2a and 2b; EX-1003 ¶ 104);

an application on a portable terminal; (See *Nielsen*, “software application on electronic key device 201,” 10:34-41, 13:1-13, 17:18-28, Figs. 2a and 2b) and

a server to provide a communication setting and a reservation certificate to the application, the communication setting corresponding to the access device (*See Nielsen*, Access code management system 211 includes a server that provides access codes include communications software components to the software application, e.g., “lock control unit ID 402,” 12:21-31, 14:57-15:22, 17:18-28, Figs 2a and 2b, Fig. 4; EX-1003 ¶ 106), **and the reservation certificate comprising an interval of a reservation,** (*See Nielsen*, “The access code illustrated in FIG. 4 further comprises additional optional fields, comprising information about the type of access rights” and these access rights include “additional parameters, e.g., validity period 410,” indicating a period of time for which the access code is valid, 14:57-15:22; EX-1003 ¶ 106).

wherein the processor receives the reservation certificate from the application based on use by the application of the communications setting, (*See Nielsen*, “The lock control unit 221 comprises a receiver 227 for receiving the signal with the access code transmitted by the communications port 209 of the electronic key device 201,” and “[t]he receiver 227 is connected to a processing unit 222” (10:55-66); software applications/components and/or the identification of the lock control unit received from the access code management system enables transmission of access codes by the electronic key device, 17:18-28; EX-1003 ¶ 107) **and**

wherein the processor compares the interval of the reservation to a current time accessible to the processor to determine if the reservation certificate is current (*See Nielsen*, “Block 689,” the lock control unit verifies the received access codes which include determining the applicability of the limited access rights, e.g., determining if the current time corresponds with the validity period 410, 14:57-15:22, 16:60-17:6, Fig. 6a; EX-1003 ¶ 108.) **and**

wherein the processor activates the door lock when the processor determines that the reservation certificate is current. (*See Nielsen*, “Block 690,” upon verification of the access codes including the validity period, “the lock mechanism is operated in step 690, thereby granting access to the location. The operation may comprise unlocking and/or locking the lock mechanism,... If the verification 689 of the access code fails, the lock mechanism is not operated,” 14:57-15:22, 16:60-17:6, Fig. 6a; EX-1003 ¶ 109).

To the extent that *Nielsen* is not sufficiently explicit about the lock control unit ID being a communication setting, a POSA would have understood that at least the lock control unit ID falls within the description of a communication setting provided in the '474 Patent, namely that the communication setting “allow[s] the application to identify and communicate with a specific one of many” access devices. EX-1001 4:67-5:3; EX-1003 ¶ 110.

Alternatively, it would have been obvious to modify *Nielsen* such that the server provides a communication setting with or as part of the access code in the form of a communication protocol to be used by the smartphone to communicate with the lock control unit, e.g., Bluetooth ®, infrared, acoustic, etc., as described in *Nielsen* (16:19-37). EX-1003 ¶ 111. It was within the general knowledge of a POSA for servers to transmit communication settings to a portable terminal for setting up the communication with an intended device. EX-1003 ¶ 111. It would have been obvious to a POSA to do so in order to exploit the various communication capabilities of the smartphone and to extend the wireless access application to lock control units having other communication protocols, e.g., RF, IR, 802.11, optical, aural, etc., which would provide increased convenience to the user of the portable terminals in gaining access and for access control managers in employing access devices in different environments. EX-1003 ¶ 111.

Furthermore, it would have been obvious to a POSA to use generally known techniques for selectively permitting wireless communication to enhance security. EX-1003 ¶ 111. For example, a POSA readily understood that limiting the number of devices that have the settings necessary to communicate with a security device like a door lock adds a further layer of protection. EX-1003 ¶ 111. A POSA would have expected that the inclusion of a communication protocol with or as part of the access code would have had a reasonable expectation of success, because the

modification would have been developed in known ways to achieve entirely predictable results. EX-1003 ¶ 111.

Claim 9

Nielsen discloses **the access control system of claim 8, wherein the communication setting is specific to the access device.** (See *Nielsen*, the communication setting includes “A lock control unit ID 402, which identifies the lock control unit.” enabling the electronic key to communicate with the identified lock control unit, 14:57-15:22; EX-1003 ¶ 112).

Claim 14

Nielsen discloses **the access control system of claim 8, wherein the reservation certificate comprises the communication setting** (See *Nielsen*, “lock control unit ID 402” included in the access code provided to the electronic key devices and enables the transmission of access codes from the electronic key device to the respective lock control unit, 14:57-15:22, Fig. 4; EX-1003 ¶ 113).

Claim 26

Nielsen renders obvious **an access control system** (See *Nielsen* “[a]n efficient method and a system for controlling access to a location secured by a lock mechanism controlled by a lock control unit,” Abstract; EX-1003 ¶¶ 114-115.)
comprising:

an access device (*See Nielsen*, “lock control unit 221,” 10:55-11:27, 12:42-54, Figs. 2a and 2b; EX-1003 ¶ 116.) **comprising a communication module connected to a processor having control of a door lock** (*See Nielsen*, the lock control unit 221 comprises a receiver 227 and a processing unit 222 connected to a lock control interface 224 which is adapted to control a lock mechanism 231, 10:55-11:27, 12:42-54, Figs. 2a and 2b; EX-1003 ¶ 116.);

an application on a portable terminal (*See Nielsen*, “software application on electronic key device 201,” 10:34-41, 13:1-13, 16:19-27 and 17:18-28, Figs. 2a, 2b, 5a and 5b; EX-1003 ¶ 117.); **and**

a server to provide a communication setting to the application, the communication setting corresponding to the access device (*See Nielsen*, Access code management system 211 includes a server that provides access codes including communications software components and device IDs to the software application to enable communication, e.g., “lock control unit ID 402,” 12:21-31, 14:57-15:22, 17:18-28, Figs 2a and 2b, Fig. 4; EX-1003 ¶ 118), **and further to provide, via a first communication protocol** (*See Nielsen*, a standard communications network 241 e.g., mobile telephone network, 12:3-21; EX-1003 ¶ 118), **a reservation certificate to the application**, (*See Nielsen*, Access code management system 211 provides access codes to the software application, 12:21-31, 17:18-28, Figs 2a and 2b, Fig. 4; EX-1003 ¶ 118) **the reservation certificate**

comprising an interval of a reservation (*See Nielsen*, “The access code illustrated in FIG. 4 further comprises additional optional fields, comprising information about the type of access rights” include “additional parameters, e.g., validity period 410,” indicating a period of time for which the access code is valid 14:57-15:22; EX-1003 ¶ 118),

wherein the processor receives the reservation certificate from the application (*See Nielsen*, The lock control unit 221 comprises a receiver 227 for receiving the signal with the access code transmitted by the communications port 209 of the electronic key device 201, the receiver 227 is connected to a processing unit that controls the retrieved access codes, software application enables transmission of access codes by electronic key device, 10:55-11:8, 17:18-28; EX-1003 ¶ 119) **via a second communication protocol that is different from the first communication protocol** (*See Nielsen*, the access code transmitted to the lock control unit from the key device is via “infrared signals or radio transmission,” 10:50-54, 16:19-27, versus the standard communications network 241 e.g., mobile telephone network, used to transmit the access code from the access code management system 211 to the electronic key device, 12:3-21; EX-1003 ¶ 119), **based on use by the application of the communication setting** (*See Nielsen*, Software application enables transmission of access codes by electronic key device, 10:55-11:8, 17:18-28; EX-1003 ¶ 119), **wherein the processor**

compares the interval of the reservation to a current time accessible to the processor to determine if the reservation certificate is current (*See Nielsen*, “Block 689,” the lock control unit verifies the received access codes including determining the applicability of the limited access rights, e.g., determining if the current time corresponds with the validity period 410, 14:57-15:22, 16:60-17:6, Fig. 6a; EX-1003 ¶ 119); **and wherein the processor activates the door lock when the processor determines that the reservation certificate is current.** (*See Nielsen*, “Block 690,” upon verification of the access codes including the validity period, “the lock mechanism is operated in step 690, thereby granting access to the location. The operation may comprise unlocking and/or locking the lock mechanism,... If the verification 689 of the access code fails, the lock mechanism is not operated,” 14:57-15:22, 16:60-17:6, Fig. 6a; EX-1003 ¶ 119).

To the extent that *Nielsen* is not sufficiently explicit about the lock control unit ID being a communication setting, a POSA would have understood, at least the lock control unit ID falls within the description of a communication setting provided in the ’474 Patent, namely that the communication setting “allow[s] the application to identify and communicate with a specific one of many” access devices. EX-1001 4:67-5:3; EX-1003 ¶ 120.

Alternatively, it would have been obvious to modify *Nielsen* such that the server provides provide a communication setting in the form of a communication

protocol, e.g., Bluetooth®, infrared, acoustic, etc., as described in *Nielsen* (16:19-37) to be used by the smartphone to communicate with the lock control unit. EX-1003 ¶ 121. It was within the general knowledge of a POSA for servers to transmit communication settings to a portable terminal for setting up the communication with an intended device. EX-1003 ¶ 121. It would have been obvious to a POSA to do so in order to exploit the various communication capabilities of the smartphone and to extend the wireless access application to lock control units having other communication protocols, e.g., RF, IR, 802.11, optical, aural, etc., which would provide increased convenience to the user of the portable terminals in gaining access to a variety of lock units and would benefit access control managers enabling employing access devices with protocols to operate in different environments. EX-1003 ¶ 121. Furthermore, it would have been obvious to a POSA to use generally known techniques for selectively permitting wireless communication to enhance security. EX-1003 ¶ 121. For example, a POSA readily understood that limiting the number of devices that have the settings necessary to communicate with a security device like a door lock adds a further layer of protection. EX-1003 ¶ 121. A POSA would have expected that the inclusion of a communication protocol with or as part of the access code would have had a reasonable expectation of success, because the modification would have

been developed in known ways to achieve entirely predictable results. EX-1003 ¶ 121.

Claim 27

Nielsen discloses **the access control system of claim 26, wherein the first communication protocol comprises a cellular protocol.** (See *Nielsen*, a standard communications network 241 e.g., mobile telephone network, 12:3-21; EX-1003 ¶ 122).

Claim 30

Nielsen discloses **the access control system of claim 26, wherein the second communication protocol comprises a short-range wireless protocol.** (See *Nielsen*, the access code transmitted to the lock control unit from the key device is via “infrared signals or radio transmission,” 10:50-54, 16:19-27; EX-1003 ¶ 123).

Claim 35

Nielsen discloses **the access control system of claim 26, wherein the reservation certificate is encrypted.** (See *Nielsen*, “To obtain the highest level of Security all electronic communication may be encrypted,” 20:55-62; EX-1003 ¶ 124).

To the extent that other limitations are not explicitly disclosed, the limitations would have been obvious given the knowledge of a POSA, since as

described in the State of the Art section, each of the limitations were well known and their use would achieve predictable results. EX-1003 ¶ 125.

D. Proposed Rejection 3, Claims 1, 2, 5-7, 15-16, 19-20 and 24 are unpatentable over *Nielsen* in view of *Kung* and *Buckingham*

Claims 1, 2, 5-7, 15-16, 19-20 and 24 are unpatentable under § 103 as obvious over U.S. Patent 7,012,503 (“*Nielsen*,”) in view of U.S. Patent Publication 2005/0021954 (“*Kung*”) and International Published Application WO 2006/101614 (“*Buckingham*”). EX-1003 ¶ 126.

Claim 1

Nielsen in view of *Kung* and *Buckingham* render obvious **an access control system** (*See Nielsen* “[a]n efficient method and a system for controlling access to a location secured by a lock mechanism controlled by a lock control unit.” Abstract; EX-1003 ¶¶ 127-128.) **comprising:**

an access device (*See Nielsen*, “lock control unit 221,” 10:55-11:27, 12:42-54, Figs. 2a and 2b; EX-1003 ¶ 129) **comprising a communication module connected to a processor having control of a door lock;** (*See Nielsen*, the lock control unit 221 comprises a receiver 227 and a processing unit 222 connected to a lock control interface 224 which is adapted to control a lock mechanism 231, 10:55-11:27, 12:42-54, Figs. 2a and 2b; EX-1003 ¶ 129);

an application on a portable terminal; (*See Nielsen*, “software application on electronic key device 201,” 10:34-41, 13:1-13, 16:19-27, 17:18-28, Figs. 2a, 2b, 5a and 5b; EX-1003 ¶ 130) **and**

a server to provide a communication setting to the application, the communication setting corresponding to the access device, (*See Nielsen*, Access code management system 211 includes a server that provides access codes including communications software components and device identification “lock control unit ID 402,” to the software application enabling transmission of access codes from the electronic key device, 12:21-31, 14:57-15:22, 17:18-28, Figs 2a and 2b, Fig. 4; EX-1003 ¶ 131), **and to further provide a reservation certificate to the application** (*See Nielsen*, the server provides access codes to the software application, including a “lock control unit ID 402,” 12:21-31, 14:57-15:22, 17:18-28, Figs 2a and 2b, Fig. 4; EX-1003 ¶ 131), **the reservation certificate comprising an interval of a reservation,** (*See Nielsen*, “The access code illustrated in FIG. 4 further comprises additional optional fields, comprising information about the type of access rights” and these access rights include “additional parameters, e.g., validity period 410,” indicating a period of time for which the access code is valid, 14:57-15:22; EX-1003 ¶ 131).

wherein the application compares the interval of the reservation to a current time accessible to the application to determine if the reservation

certificate is current (*See Nielsen*, “Block 689,” the received access codes are verified including the validity period 410, 14:57-15:22, 16:60-17:6, Fig. 6a; EX-1003 ¶ 132) **and wherein, the application activates the door lock by communicating with the access device via the communication setting** (*See Nielsen*, the lock control unit 221 comprises a receiver 227 for receiving the signal with the access code transmitted by the communications port 209 of the electronic key device 201, the receiver 227 is connected to a processing unit that controls the retrieved access codes, software application enables transmission of access codes by electronic key device, 10:55-11:8, 17:18-28; EX-1003 ¶ 132) **when the application determines that the reservation certificate is current.** (*See Nielsen*, “Block 689,” verifies the received access codes including the validity period 410, “Block 690,” upon verification of the access codes including the validity period, “the lock mechanism is operated in step 690, thereby granting access to the location. The operation may comprise unlocking and/or locking the lock mechanism,... If the verification 689 of the access code fails, the lock mechanism is not operated,” 14:57-15:22, 16:60-17:6, Fig. 6a; EX-1003 ¶ 132).

Nielsen discloses that the comparison may be performed at the lock control unit. *Nielsen* does not include a specific example of the application on the electronic key device performing the comparison corresponding to the limitation of “wherein the application compares the interval of the reservation to a current time

accessible to the application to determine if the reservation certificate is current.”

EX-1003 ¶ 133.

Kung discloses the limitation of **wherein the application compares the interval of the reservation to a current time accessible to the application to determine if the reservation certificate is current.** (See *Kung*, “all authentication operations may be performed at PAD 100,” “the process of authentication may involve checking the current date and time (which may be obtained, for example, from clock 132) against the validity period of the digital certificate,” [0015], [0039], [0040], Figs. 1 and 2; EX-1003 ¶ 134).

Buckingham teaches transferring functions and components from the locking device on the hotel door (**access device**) to the primary access control electronics (**portable terminal**) to reduce power consumption and costs. (See *Buckingham*, [0003], [0004], [0005], [0006], [0008], [0012]; EX-1003 ¶ 135).

Therefore, it would have been obvious to a POSA to modify the system of *Nielsen* to perform the authentication/verification of the validity period at the PAD (**portable terminal**) as taught by *Kung*. EX-1003 ¶ 136. A POSA would have been motivated to make the modification to reduce power consumption of the electronic lock (**access device**) and subsequent installment and maintenance costs as taught by *Buckingham*. EX-1003 ¶ 136. A POSA would have expected that the

combination would have had a reasonable expectation of success given the well known use and compatibility of the claimed components. EX-1003 ¶ 136.

To the extent that *Nielsen* is not sufficiently explicit about the lock control unit ID being a communication setting, a POSA would have understood, at least the lock control unit ID falls within the description of a communication setting provided in the '474 Patent, namely that the communication setting “allow[s] the application to identify and communicate with a specific one of many” access devices. EX-1001 4:67-5:3; EX-1003 ¶ 137.

Alternatively, it would have been obvious to modify *Nielsen* such that the server provides a communication setting with or as part of the access code in the form of a communication protocol to be used by the smartphone to communicate with the lock control unit, e.g. Bluetooth ®, infrared, acoustic, etc., as described in *Nielsen* (16:19-37). EX-1003 ¶ 138. It was within the general knowledge of a POSA for servers to transmit communication settings to a portable terminal for setting up the communication with an intended device. EX-1003 ¶ 138. It would have been obvious to a POSA to do so in order to exploit the various communication capabilities of the smartphone, and extend the wireless access application to lock control units having other communication protocols, e.g., RF, IR, 802.11, optical, aural, etc., which would provide increased convenience to the user of the portable terminals in gaining access and for access control managers in

employing access devices in different environments. EX-1003 ¶ 138.

Furthermore, it would have been obvious to a POSA to use generally known techniques for selectively permitting wireless communication to enhance security. EX-1003 ¶ 138. For example, a POSA readily understood that limiting the number of devices that have the settings necessary to communicate with a security device like a door lock adds a further layer of protection. EX-1003 ¶ 138. A POSA would have expected that the inclusion of a communication protocol with or as part of the access code would have had a reasonable expectation of success, because the modification would have been developed in known ways to achieve entirely predictable results. EX-1003 ¶ 138.

Claim 2

Nielsen discloses **the access control system of claim 1, wherein the communication setting is specific to the access device.** (See *Nielsen*, “lock control unit ID 402,” 14:57-15:22 Fig. 4; EX-1003 ¶ 139)

Claim 5

Nielsen in view of *Kung* and *Buckingham* disclose **wherein the application uses Bluetooth to communicate with the access device and the communication setting comprises a Bluetooth ID.** (See *Buckingham*, “Wireless communication between the control assembly 14 and the network and/or between the control assembly 14 and the door lock unit 12 is preferably conducted via radio frequency

(RF) communication, but may alternatively and/or additionally utilize infrared (IR) or other types of communication (e.g., ultrasound (U/S), etc.). Such wireless RF communication may utilize, for example, 802.11b radio frequency protocol, WI-FI, Bluetooth®, 802.15.4, or any other suitable wireless protocol,” [0024]; EX-1003 ¶ 140).

A POSA understood a Bluetooth ID (or BD_ADDR) uniquely identifies a Bluetooth device and is required to enable communication with a Bluetooth device. It would have been obvious to a POSA to provide the Bluetooth ID in the access code of *Nielsen*, *Kung*, and *Buckingham*. A POSA would be motivated to include the Bluetooth ID in order to positively identify the selected lock control unit and enable wireless communication between the mobile device and the lock control unit. EX-1003 ¶ 141. A POSA would have expected that the combination would have had a reasonable expectation of success given the well known and ubiquitous use of Bluetooth communications. EX-1003 ¶ 141.

Claim 6

Nielsen in view of *Kung* and *Buckingham* disclose **wherein the application uses Wi-Fi to communicate with the access device and the communication setting comprises a network SSID.** (See *Buckingham*, “Wireless communication between the control assembly 14 and the network and/or between the control assembly 14 and the door lock unit 12 is preferably conducted via radio frequency

(RF) communication, but may alternatively and/or additionally utilize infrared (IR) or other types of communication (e.g., ultrasound (U/S), etc.). Such wireless RF communication may utilize, for example, 802.11 b radio frequency protocol, **WI-FI**, Bluetooth®, 802.15.4, or any other suitable wireless protocol.” [0024] (emphasis added); EX-1003 ¶ 142)

A POSA understood that a SSID uniquely identifies a Wi-Fi network and is required to enable communication over the network. It would have been obvious to a POSA to provide the SSID in the access code of *Nielsen*, *Kung* and *Buckingham*. A POSA would be motivated to include the SSID in order to positively identify the Wi-Fi network associated with selected lock control unit and enable wireless communication between the mobile device and the lock control unit via the Wi-Fi network. EX-1003 ¶ 143. A POSA would have expected that the combination would have had a reasonable expectation of success given the well known and ubiquitous use of Wi-Fi communications. EX-1003 ¶ 143.

Claim 7

Nielsen in view of *Kung* and *Buckingham* disclose **wherein the reservation certificate comprises the communication setting**. (See *Nielsen*, “lock control unit ID 402” included in the access code provided to the electronic key devices and enables the transmission of access codes from the electronic key device to the respective lock control unit, 14:57-15:22, Fig. 4; EX-1003 ¶ 144)

Claim 15

Nielsen in view of *Kung* and *Buckingham* render obvious **an access control system** (*See Nielsen* “[a]n efficient method and a system for controlling access to a location secured by a lock mechanism controlled by a lock control unit,” Abstract; EX-1003 ¶ 145.) **comprising:**

an access device (*See Nielsen*, “lock control unit 221,” 10:55-11:27, 12:42-54, Figs. 2a and 2b; EX-1003 ¶ 146) **comprising a communication module connected to a processor having control of a door lock** (*See Nielsen*, the lock control unit 221 comprises a receiver 227 and a processing unit 222 connected to a lock control interface 224 which is adapted to control a lock mechanism 231, 10:55-11:27, 12:42-54, Figs. 2a and 2b; EX-1003 ¶ 146);

an application on a portable terminal (*See Nielsen*, “software application on electronic key device 201,” 10:34-41, 13:1-13, 16:19-27, 17:18-28, Figs. 2a, 2b, 5a and 5b; EX-1003 ¶ 147); **and**

a server (*See Nielsen*, “Access code management system 211,” 12:21-31, 17:18-28, Figs 2a and 2b; EX-1003 ¶ 148) **to provide a communication setting to the application, the communication setting corresponding to the access device** (*See Nielsen*, Access code management system 211 includes a server that provides access codes including communications software components and device identification “lock control unit ID 402,” to the software application enabling

transmission of access codes from the electronic key device, 12:21-31, 14:57-15:22, 17:18-28, Figs 2a and 2b, Fig. 4; EX-1003 ¶ 148), **and to further provide, via a first communication protocol** (*See Nielsen*, a standard communications network 241, e.g., mobile telephone network, 12:3-21; EX-1003 ¶ 148), **a reservation certificate to the application** (*See Nielsen*, “[v]ia the communications link between the electronic key device 201 and the access code management System 211, access codes may be transmitted from the access code management system 211 to the electronic key device 201” the access codes provide to the software application, including a “lock control unit ID 402,” 12:10-15,21-31, 14:57-15:22, 17:18-28, Figs 2a and 2b, Fig. 4; EX-1003 ¶ 148), **the reservation certificate comprising an interval of a reservation,** (*See Nielsen*, “The access code illustrated in FIG. 4 further comprises additional optional fields, comprising information about the type of access rights” and these access rights include “additional parameters, e.g., validity period 410,” indicating a period of time for which the access code is valid, 14:57-15:22; EX-1003 ¶ 148).

wherein the application compares the interval of the reservation to a current time accessible to the application to determine if the reservation certificate is current (*See Nielsen*, “Block 689,” the received access codes are verified including determining the applicability of the limited access rights, e.g. determining if the current time corresponds with the validity period 410, 14:57-

15:22, 16:60-17:6, Fig. 6a; EX-1003 ¶ 149) **and wherein the application activates the door lock by communicating with the access device** (*See Nielsen*, the lock control unit 221 comprises a receiver 227 for receiving the signal with the access code transmitted by the communications port 209 of the electronic key device 201, the receiver 227 is connected to a processing unit that controls the retrieved access codes, Software application enables transmission of access codes by electronic key device, 10:55-11:8, 17:18-28; EX-1003 ¶ 149) **via a second communication protocol that is different from the first communication protocol** (*See Nielsen*, “infrared signals or radio transmission,” 10:50-54, 16:19-27; EX-1003 ¶ 149), **based on use by the application of the communication setting** (*See Nielsen*, Software applications and “lock control unit ID 402,” enable transmission of access codes by electronic key device to the lock control unit, 10:55-11:8, 17:18-28; EX-1003 ¶ 149), **when the application determines that the reservation certificate is current.** (*See Nielsen*, “Block 689,” verifies the received access codes including the validity period 410, “Block 690,” upon verification of the access codes including the validity period, “the lock mechanism is operated in step 690, thereby granting access to the location. The operation may comprise unlocking and/or locking the lock mechanism,... If the verification 689 of the access code fails, the lock mechanism is not operated,” 14:57-15:22, 16:60-17:6, Fig. 6a; EX-1003 ¶ 149).

Nielsen discloses the comparison of the validity period reservation to verify the access codes generally and as an example discloses the comparison may be performed at the lock control unit. *Nielsen* does not include a specific example of the application on the electronic key device performing the comparison corresponding to the limitation of “wherein the application compares the interval of the reservation to a current time accessible to the application to determine if the reservation certificate is current.” EX-1003 ¶ 150.

Kung discloses the limitation of **wherein the application compares the interval of the reservation to a current time accessible to the application to determine if the reservation certificate is current.** (See *Kung*, “all authentication operations may be performed at PAD 100,” “the process of authentication may involve checking the current date and time (which may be obtained, for example, from clock 132) against the validity period of the digital certificate” [0015], [0039], [0040], Figs. 1 and 2; EX-1003 ¶ 151).

Buckingham teaches transferring functions and components from the locking device (**access device**) to the primary access control electronics (**portable terminal**) to reduce power consumption and costs. (See *Buckingham*, [0003], [0004], [0005], [0006], [0008], [0012]; EX-1003 ¶ 152).

Therefore, it would have been obvious to a POSA to modify the system of *Nielsen* to perform the authentication/verification of the validity period at the PAD

(**portable terminal**) as taught by *Kung*. EX-1003 ¶ 153. A POSA would have been motivated to make the modification to reduce power consumption of the electronic lock (access unit) and subsequent instalment and maintenance costs as taught by *Buckingham*. EX-1003 ¶ 153. A POSA would have expected that the combination would have had a reasonable expectation of success given the well known use and compatibility of the claimed components. EX-1003 ¶ 153.

To the extent that *Nielsen* is not sufficiently explicit about the lock control unit ID being a communication setting, a POSA would have understood, at least the lock control unit ID falls within the description of a communication setting provided in the '474 Patent, namely that the communication setting “allow[s] the application to identify and communicate with a specific one of many” access devices. EX-1001 4:67-5:3; EX-1003 ¶ 154.

Alternatively, it would have been obvious to modify *Nielsen* such that the server provides a communication setting with or as part of the access code in the form of a communication protocol to be used by the smartphone to communicate with the lock control unit, e.g., Bluetooth ®, infrared, acoustic, etc., as described in *Nielsen* (16:19-37). EX-1003 ¶ 155. It was within the general knowledge of a POSA for servers to transmit communication settings to a portable terminal for setting up the communication with an intended device. EX-1003 ¶ 155. It would have been obvious to a POSA to do so in order to exploit the various

communication capabilities of the smartphone and to extend the wireless access application to lock control units having other communication protocols, e.g., RF, IR, 802.11, optical, aural, etc., which would provide increased convenience to the user of the portable terminals in gaining access and for access control managers in employing access devices in different environments. EX-1003 ¶ 155.

Furthermore, it would have been obvious to a POSA to use generally known techniques for selectively permitting wireless communication to enhance security. EX-1003 ¶ 155. For example, a POSA readily understood that limiting the number of devices that have the settings necessary to communicate with a security device like a door lock adds a further layer of protection. EX-1003 ¶ 155. A POSA would have expected that the inclusion of a communication protocol with or as part of the access code would have had a reasonable expectation of success, because the modification would have been developed in known ways to achieve entirely predictable results. EX-1003 ¶ 155.

Claim 16

Nielsen discloses **the access control system of claim 15, wherein the first communication protocol comprises a cellular protocol.** (*See Nielsen*, a standard communications network 241 e.g., mobile telephone network, 12:3-21; EX-1003 ¶ 156).

Claim 19

Nielsen discloses **the access control system of claim 15, wherein the second communication protocol comprises a short-range wireless protocol.** (See *Nielsen*, the access code transmitted to the lock control unit from the key device is via “infrared signals or radio transmission,” 10:50-54, 16:19-27; EX-1003 ¶ 157).

Claim 20

Nielsen in view of *Kung* and *Buckingham* disclose **the access control system of claim 19, wherein the short-range wireless protocol comprises Bluetooth.** (See *Buckingham*, “Wireless communication between the control assembly 14 and the network and/or between the control assembly 14 and the door lock unit 12 is preferably conducted via radio frequency (RF) communication, but may alternatively and/or additionally utilize infrared (IR) or other types of communication (e.g., ultrasound (U/S), etc.). Such wireless RF communication may utilize, for example, 802.11 b radio frequency protocol, WI-FI, **Bluetooth®**, 802.15.4, or any other suitable wireless protocol,” [0024] (emphasis added); EX-1003 ¶ 158).

Claim 24

Nielsen in view of *Kung* and *Buckingham* disclose **the access control system of claim 15, wherein the reservation certificate is encrypted.** (See

Nielsen, “To obtain the highest level of Security all electronic communication may be encrypted,” 20:55-62; EX-1003 ¶ 159)

To the extent that other limitations recited in the above claims are not explicitly disclosed, the limitations would have been obvious given the knowledge of a POSA, since as described in the State of the Art section, each of the limitations were well known and their use would achieve predictable results. EX-1003 ¶ 160.

E. Proposed Rejection 4, Claims 1, 8, 15, 16, 19, 26, 27 and 30 are unpatentable over *Ullmann* in view of *Barnes*

Claims 1, 8, 15, 16, 19, 26, 27 and 30 are unpatentable under § 103 as obvious over U.S. Patent 8,635,462 (“*Ullmann*”) in view of U.S. Pub. No. 2007/0173266 (“*Barnes*”). EX-1003 ¶ 161.

Claim 1

Ullmann in view of *Barnes* renders obvious **an access control system** (*See Ullmann*, “a device for managing access control,” 1:14-15; EX-1003 ¶ 162)

comprising:

an access device (*See Ullmann*, “locking unit,” 1:12-34, Fig. 1; EX-1003 ¶ 163) **comprising a communication module connected to a processor having control of a door lock** (*See Ullmann*, “RFID-based locking unit,” includes a

RFID module connected to an “evaluation circuit,” that controls a locking unit, 1:16-18, 1:26-28, 8:13-17, Fig. 2; EX-1003 ¶ 163);

an application on a portable terminal (*See Ullmann*, “mobile telecommunication devices 5,” “each comprise an RFID module,” and are programmed with authorization information to function as keys, 2:23-32, 8:23-27, 9:10-15, Figs 1 and 2; EX-1003 ¶ 164); and

a server (*See Ullmann*, “central processor,” 6:35-38, Figs. 1 and 2; EX-1003 ¶ 165) **to provide a communication setting to the application, the communication setting corresponding to the access device,** (*See Ullmann*, “authorization information” includes a lock identification, the authorization information is utilized by the NFC module of the mobile telecommunication device to enable communications with the locking unit via NFC connection, “in the simplest case, the authorization information is sent to the mobile telecommunication device 5 as a lock identification. If, in a strongly simplified example, the locking units of the objects illustrated in FIG. 1 have the identifications 100, 101 and 102, the transmission of the authorization information to a telecommunication device 5 in the form of the identification 101 will mean that this will correspond to an access authorization for the locking unit having the identification 101,” 8:13-44, 9:10-15; EX-1003 ¶ 165) **and to further provide a reservation certificate to the application** (*See Ullmann*, the authorization

information includes a lock identification “the central processor 1 is connected to a mobile wireless tele-communication network 4, such as a GSM mobile network, and can send authorization information to mobile telecommunication devices 5 via the GSM network 4,” 6:35-38, 8:13-22; EX-1003 ¶ 165), **[the reservation certificate comprising an interval of a reservation,**

wherein the application compares the interval of the reservation to a current time accessible to the application to determine if the reservation certificate is current and]⁴

wherein, the application activates the door lock by communicating with the access device via the communication setting when the application determines that the reservation certificate is current. (See *Ullman*, the locking unit, based on a comparison of the lock identification transmitted by the key with its own lock identification, will recognize the presence of an access authorization in the event of a match, whereupon the lock will be enabled, 8:35-44; EX-1003 ¶ 166).

Ullmann does not explicitly disclose the authorization information (*reservation certificate*) **comprising an interval of a reservation**, nor does it explicitly disclose that **the application compares the interval of the reservation**

⁴ These limitations are provided by *Barnes*, as explained below.

to a current time accessible to the application to determine if the reservation certificate is current.

Barnes discloses **the reservation certificate comprising an interval of a reservation** and that **the application compares the interval of the reservation to a current time accessible to the application to determine if the reservation certificate is current.** (See *Barnes*, the transmission of a guest entry code is controlled by software on a portable communications device and predicated on satisfying temporal criteria provided by the server as check in information, a POSA would recognize that by transmitting the guest's entry codes by the portable communications device based on temporal criteria implicitly teaches a comparison of the temporal data of the check in information against the current time by the software on the portable communications device, EX-1008 [0365], [0366]; EX-1003 ¶ 168).

It would have been obvious to modify the system of *Ullmann* as described above to include temporal data and determine if the temporal criteria (*interval of reservation*) supplied by the server is satisfied via the programing/software on the portable terminal (*application*) as taught by *Barnes*. EX-1003 ¶ 169. A POSA would have been motivated to include the temporal data/criteria taught by *Barnes* in the Authorization information of *Ullmann* in order to more precisely manage access and add another layer of security in preventing unauthorized access. EX-

1003 ¶ 169. A POSA would also have been motivated to determine whether the criteria is satisfied via the application as taught by *Barnes* in order to leverage the processing assets of the users portable terminal rather than expending the cost (in expense and energy usage) to incorporate the technology in the lock unit. EX-1003 ¶ 169. A POSA would have also been confident of success given the well known use of time windows to control access and lack of technical difficulty in implementation. EX-1003 ¶ 169.

Claim 8

Ullmann in view of *Barnes* renders obvious **an access control system** (See *Ullmann*, “a device for managing access control,” 1:14-15; EX-1003 ¶¶180-181) **comprising:**

an access device (See *Ullmann*, “locking unit,” 1:12-34, Fig. 1; EX-1003 ¶ 182) **comprising a communication module connected to a processor having control of a door lock;** (See *Ullmann*, “RFID-based locking unit,” includes a RFID module connected to an “evaluation circuit,” that controls a locking unit, 1:16-18, 1:26-28, 8:13-17, Fig. 2; EX-1003 ¶ 182).

an application on a portable terminal; (See *Ullmann*, “mobile telecommunication devices 5,” “each comprise an RFID module,” and are programmed with authorization information to function as keys, 2:23-32, 8:23-27, 9:10-15, Figs 1 and 2; EX-1003 ¶ 183) **and**

a server (*See Ullmann*, “central processor,” 6:35-38, Figs. 1 and 2; EX-1003 ¶ 184) **to provide a communication setting** (*See Ullmann*, “authorization information” includes lock identification, the authorization information is utilized by the NFC module of the mobile telecommunication device to enable communications with the locking unit via NFC connection, “In the simplest case, the authorization information is sent to the mobile telecommunication device 5 as a lock identification. If, in a strongly simplified example, the locking units of the objects illustrated in FIG. 1 have the identifications 100, 101 and 102, the transmission of the authorization information to a telecommunication device 5 in the form of the identification 101 will mean that this will correspond to an access authorization for the locking unit having the identification 101,” 8:13-44, 9:10-15; EX-1003 ¶ 184) **and a reservation certificate to the application**, (*See Ullmann*, the authorization information includes a lock identification “the central processor 1 is connected to a mobile wireless tele-communication network 4, such as a GSM mobile network, and can send authorization information to mobile telecommunication devices 5 via the GSM network 4,” 6:35-38, 8:13-22; EX-1003 ¶ 184) **the communication setting corresponding to the access device**, (*See Ullmann*, “In the simplest case, the authorization information is sent to the mobile telecommunication device 5 as a lock identification. If, in a strongly simplified example, the locking units of the objects illustrated in FIG. 1 have the

identifications 100, 101 and 102, the transmission of the authorization information to a telecommunication device 5 in the form of the identification 101 will mean that this will correspond to an access authorization for the locking unit having the identification 101,” 8:13-44, 9:10-15; EX-1003 ¶ 184) **and [the reservation certificate comprising an interval of a reservation,]**

wherein the processor receives the reservation certificate from the application based on use by the application of the communications setting, (See *Ullmann*, “when the telecommunication device 5, which is used as a key, is taken near a locking unit having the identification 101, and the authorization information, i.e. the lock identification “101’, is transmitted to the locking unit,” 8:35-44; EX-1003 ¶ 185) **and**

wherein the processor compares the interval of the reservation to a current time accessible to the processor to determine if the reservation certificate is current (See *Ullmann*, “a comparator circuit for comparing the received authorization information with the own lock identification,” 4:10-23; EX-1003 ¶ 186) **and**

wherein the processor activates the door lock when the processor determines that the reservation certificate is current. (See *Ullman*, the locking unit, based on a comparison of the lock identification transmitted by the key with its own lock identification, will recognize the presence of an access authorization

in the event of a match, whereupon the lock will be enabled, 8:35-44; EX-1003 ¶ 187).

Ullmann does not explicitly disclose that the authorization information (*communication setting and reservation certificate*) includes an interval of reservation nor that the activation of the door lock is predicated upon a comparison of the current time accessible by the processor to the interval of reservation.

Barnes discloses **the reservation certificate comprising an interval of a reservation** (i.e., temporal criteria) and **compares the interval of the reservation to a current time accessible to the processor to determine if the reservation certificate is current**. (See *Barnes*, gaining access to a hotel room via transmission of an entry code is predicated on satisfying temporal criteria provided by the server as check in information, a POSA would recognize authorizing access based on temporal criteria implicitly teaches a comparison of the temporal data of the check in information against the current time, [0365], [0366]; EX-1003 ¶ 189).

It would have been obvious to modify the system of *Ullmann* as described above to include temporal data and determine if the temporal criteria (*interval of reservation*) supplied by the server is satisfied as taught by *Barnes*. EX-1003 ¶ 190. A POSA would have been motivated to include the temporal data/criteria taught by *Barnes* in the Authorization information of *Ullmann* in order to more precisely manage access and add another layer of security in preventing

unauthorized access. EX-1003 ¶ 190. A POSA would have expected that the combination would have had a reasonable expectation of success given the well known use of time windows to control access and the lack of technical difficulty of implementation. EX-1003 ¶ 190.

Claim 15

Ullmann in view of *Barnes* renders obvious **an access control system** (*See Ullmann*, “a device for managing access control,” 1:14-15; EX-1003 ¶ 170)

comprising:

an access device (*See Ullmann*, “locking unit,” 1:12-34, Fig. 1; EX-1003 ¶ 171) **comprising a communication module connected to a processor having control of a door lock** (*See Ullmann*, “RFID-based locking unit,” includes a RFID module connected to an “evaluation circuit,” that controls a locking unit, 1:16-18, 1:26-28, 8:13-17, Fig. 2; EX-1003 ¶ 171);

an application on a portable terminal (*See Ullmann*, “mobile telecommunication devices 5,” “each comprise an RFID module,” and are programmed with authorization information to function as keys, 2:23-32, 8:23-27, 9:10-15, Figs 1 and 2; EX-1003 ¶ 172); **and**

a server (*See Ullmann*, “central processor,” 6:35-38, Figs. 1 and 2) **to provide a communication setting to the application, the communication setting corresponding to the access device,** (*See Ullmann*, “authorization

information” includes a lock identification, the authorization information is utilized by the NFC module of the mobile telecommunication device to enable communications with the locking unit via NFC connection, “In the simplest case, the authorization information is sent to the mobile telecommunication device 5 as a lock identification. If, in a strongly simplified example, the locking units of the objects illustrated in FIG. 1 have the identifications 100, 101 and 102, the transmission of the authorization information to a telecommunication device 5 in the form of the identification 101 will mean that this will correspond to an access authorization for the locking unit having the identification 101,” 8:13-44, 9:10-15; EX-1003 ¶ 173) **and to further provide, via a first communication protocol, a reservation certificate to the application** (See *Ullmann*, the authorization information includes a lock identification, “the central processor 1 is connected to a mobile wireless tele-communication network 4, such as a GSM mobile network, and can send authorization information to mobile telecommunication devices 5 via the GSM network 4,” 6:35-38, 8:13-22; EX-1003 ¶ 173), **[the reservation certificate comprising an interval of a reservation,**

wherein the application compares the interval of the reservation to a current time accessible to the application to determine if the reservation certificate is current]

and wherein the application activates the door lock by communicating with the access device (*See Ullman*, the locking unit, based on a comparison of the lock identification transmitted by the key with its own lock identification, will recognize the presence of an access authorization in the event of a match, whereupon the lock will be enabled, 8:35-44; EX-1003 ¶ 174) **via a second communication protocol that is different from the first communication protocol** (*See Ullmann*, “NFC connection” 9:10-15, “[T]he authorization information in this case is stored in such a manner as to be available to a telecommunication interface of the mobile telecommunication device in order to enable the wireless transmission of the authorization information to the locking unit via this communication interface. In a preferred manner, this is a separate communication interface of the telecommunication device, which is different from the communication interface via which the authorization information is received from the central processor,” 3:23-33; EX-1003 ¶ 174), **based on use by the application of the communication setting, when the application determines that the reservation certificate is current.** (*See Ullman*, the locking unit, based on a comparison of the lock identification transmitted by the key with its own lock identification, will recognize the presence of an access authorization in the event of a match, whereupon the lock will be enabled, 8:35-44; EX-1003 ¶ 174).

Ullmann does not explicitly disclose the authorization information (*reservation certificate*) **comprising an interval of a reservation**, nor does it explicitly disclose that **application compares the interval of the reservation to a current time accessible to the application to determine if the reservation certificate is current**.

Barnes discloses **the reservation certificate comprising an interval of a reservation** and that **the application compares the interval of the reservation to a current time accessible to the application to determine if the reservation certificate is current**. (See *Barnes*, the transmission of a guest entry code is controlled by a portable communications device and predicated on satisfying temporal criteria provided by the server as check in information, a POSA would recognize that by transmitting the guest's entry codes by the portable communications device based on temporal criteria implicitly teaches a comparison of the temporal data of the check in information against the current time by the software on the portable communications device, [0365], [0366]; EX-1003 ¶ 176).

It would have been obvious to modify the system of *Ullmann* as described above to include temporal data and determine if the temporal criteria (*interval of reservation*) supplied by the server is satisfied via the programing/software on the portable terminal (*application*) as taught by *Barnes*. EX-1003 ¶ 177. A POSA would have been motivated to include the temporal data/criteria taught by *Barnes*

in the Authorization information of *Ullmann* in order to more precisely manage access and add another layer of security in preventing unauthorized access. EX-1003 ¶ 177. A POSA would also have been motivated to determine whether the criteria is satisfied via the application as taught by *Barnes* in order to leverage the processing assets of the users portable terminal rather than expending the cost to incorporate the technology in the lock unit. EX-1003 ¶ 177. A POSA would have also been confident of success given the well known use of time windows to control access and lack of technical difficulty in implementation. EX-1003 ¶ 177.

Claim 16

Ullmann discloses **the access control system of claim 15, wherein the first communication protocol comprises a cellular protocol.** (See *Ullmann*, the authorization information includes a lock identification, “the central processor 1 is connected to a mobile wireless tele-communication network 4, such as a GSM mobile network, and can send authorization information to mobile telecommunication devices 5 via the GSM network 4,” 6:35-38, 8:13-22; EX-1003 ¶ 178)

Claim 19

Ullmann discloses **the access control system of claim 15, wherein the second communication protocol comprises a short-range wireless protocol.** (See *Ullmann*, “NFC connection,” 9:10-15, EX-1003 ¶ 179).

Claim 26

Ullmann in view of *Barnes* renders obvious **an access control system** (*See Ullmann*, “a device for managing access control,” 1:14-15; EX-1003 ¶¶ 191-192) **comprising:**

an access device (*See Ullmann*, “locking unit,” 1:12-34, Fig. 1; EX-1003 ¶ 193) **comprising a communication module connected to a processor having control of a door lock;** (*See Ullmann*, “RFID-based locking unit,” includes a RFID module connected to an “evaluation circuit,” that controls a locking unit, 1:16-18, 1:26-28, 8:13-17, Fig. 2; EX-1003 ¶ 193).

an application on a portable terminal (*See Ullmann*, “mobile telecommunication devices 5,” “each comprise an RFID module,” and are programmed with authorization information to function as keys, 2:23-32, 8:23-27, 9:10-15, Figs 1 and 2; EX-1003 ¶ 194); **and**

a server (*See Ullmann*, “central processor,” 6:35-38, Figs. 1 and 2; EX-1003 ¶ 195) **to provide a communication setting to the application, the communication setting corresponding to the access device** (*See Ullmann*, “authorization information” includes lock identification, the authorization information is utilized by the NFC module of the mobile telecommunication device to enable communications with the locking unit via NFC connection, “In the simplest case, the authorization information is sent to the mobile

telecommunication device 5 as a lock identification. If, in a strongly simplified example, the locking units of the objects illustrated in FIG. 1 have the identifications 100, 101 and 102, the transmission of the authorization information to a telecommunication device 5 in the form of the identification 101 will mean that this will correspond to an access authorization for the locking unit having the identification 101,” 8:13-44, 9:10-15; EX-1003 ¶ 195), **and further to provide, via a first communication protocol, a reservation certificate to the application** (See *Ullmann*, the authorization information includes a lock identification, “the central processor 1 is connected to a mobile wireless tele-communication network 4, such as a GSM mobile network, and can send authorization information to mobile telecommunication devices 5 via the GSM network 4,” 6:35-38, 8:13-22; EX-1003 ¶ 195), **[the reservation certificate comprising an interval of a reservation,]**

wherein the processor receives the reservation certificate from the application (See *Ullmann*, “when the telecommunication device 5, which is used as a key, is taken near a locking unit having the identification 101, and the authorization information, i.e. the lock identification “101’, is transmitted to the locking unit,” 8:35-44; EX-1003 ¶ 196) **via a second communication protocol that is different from the first communication protocol** (See *Ullmann*, “NFC connection” 9:10-15, “[T]he authorization information in this case is stored in such

a manner as to be available to a telecommunication interface of the mobile telecommunication device in order to enable the wireless transmission of the authorization information to the locking unit via this communication interface. In a preferred manner, this is a separate communication interface of the telecommunication device, which is different from the communication interface via which the authorization information is received from the central processor,” 3:23-33; EX-1003 ¶ 196), **based on use by the application of the communication setting**, (See *Ullmann*, “when the telecommunication device 5, which is used as a key, is taken near a locking unit having the identification 101, and the authorization information, i.e. the lock identification “101’, is transmitted to the locking unit,” 8:35-44; EX-1003 ¶ 196) **wherein the processor compares the interval of the reservation to a current time accessible to the processor to determine if the reservation certificate is current**; (See *Ullmann*, “a comparator circuit for comparing the received authorization information with the own lock identification,” 4:10-23; EX-1003 ¶ 196) **and wherein the processor activates the door lock when the processor determines that the reservation certificate is current**. (See *Ullman*, the locking unit, based on a comparison of the lock identification transmitted by the key with its own lock identification, will recognize the presence of an access authorization

in the event of a match, whereupon the lock will be enabled, 8:35-44; EX-1003 ¶ 197).

Ullmann does not explicitly disclose that the authorization information (*communication setting and reservation certificate*) includes an interval of reservation nor that the activation of the door lock is predicated upon a comparison of the current time accessible by the processor to the interval of reservation.

Barnes discloses **the reservation certificate comprising an interval of a reservation** (i.e., temporal criteria) and **compares the interval of the reservation to a current time accessible to the processor to determine if the reservation certificate is current**. (See *Barnes*, gaining access to a hotel room via transmission of an entry code is predicated on satisfying temporal criteria provided by the server as check in information, a POSA would recognize authorizing access based on temporal criteria implicitly teaches a comparison of the temporal data of the check in information against the current time, [0365], [0366]; EX-1003 ¶ 199).

It would have been obvious to modify the system of *Ullmann* as described above to include temporal data and determine if the temporal criteria (*interval of reservation*) supplied by the server is satisfied as taught by *Barnes*. EX-1003 ¶ 200. A POSA would have been motivated to include the temporal data/criteria taught by *Barnes* in the Authorization information of *Ullmann* in order to more precisely manage access and add another layer of security in preventing

unauthorized access. EX-1003 ¶ 200. A POSA would have also been confident of success given the well known use of time windows to control access and lack of technical difficulty in implementation. EX-1003 ¶ 200.

Claim 27

Ullmann discloses **wherein the first communication protocol comprises a cellular protocol.** (See *Ullmann*, the authorization information includes a lock identification, “the central processor 1 is connected to a mobile wireless telecommunication network 4, such as a GSM mobile network, and can send authorization information to mobile telecommunication devices 5 via the GSM network 4,” 6:35-38, 8:13-22; EX-1003 ¶ 201)

Claim 30

Ullmann discloses **wherein the second communication protocol comprises a short-range wireless protocol.** (See *Ullmann*, “NFC connection,” 9:10-15, EX-1003 ¶ 202)

F. Secondary Considerations

This Request demonstrates that Claims 1, 2, 5-9, 14-16, 19-20, 24, 26-27, 30, and 35 of the '474 Patent are unpatentable as obvious in view of the prior art references. The Applicant did not identify any evidence of secondary considerations during prosecution, and the clear teachings in the prior art cannot be overcome by any supposed “secondary considerations.”

V. DISCLOSURE OF CONCURRENT LITIGATION AND ADMINISTRATIVE PROCEEDINGS

Based on publicly available information, the '474 Patent has been the subject of the following litigations, each of which remain pending at the time of this filing:

ASSA ABLOY Global Solutions, Inc. v. Liberty Access Technologies Licensing LLC, N.D. Ill. Case 1-23-cv-00756 (filed Feb. 7, 2023).

Liberty Access Technologies Licensing LLC v. ASSA ABLOY AB et al, E.D. Tex. Case 2-22-cv-00507 (filed Dec. 30, 2022).

Liberty Access Technologies Licensing LLC v. Marriott International, Inc., E.D. Tex. Case 2-22-cv-00318 (filed Aug. 18, 2022).

Requester is not a party to or otherwise involved in any of the above proceedings.

Based on publicly available information, the '474 Patent has not been the subject of any prior or current reexaminations or post-grant proceedings. Requester is unaware of any other proceedings involving the '474 Patent.

VI. CONCLUSION

The Commissioner is hereby authorized to charge Deposit Account 50-6990 the *Ex Parte* Reexamination fee of \$13,080 under 37 C.F.R. § 1.20(c)(2) and § 1.20(c)(3). Requester believes no other fee is due with this submission, however

the Commissioner is hereby authorized to charge any fee deficiency or credit any over-payment to Deposit Account 50-6990.

Please direct all correspondence in this matter to the undersigned.

Dated: May 11, 2023

Respectfully submitted,

By: /John M Baird/
John M. Baird
USPTO Reg. No. 57,585
Duane Morris LLP
901 New York Ave. NW,
Suite 700 East
Washington, D.C. 20001-4795
JMBaird@duanemorris.com

Patrick Craig Muldoon*
USPTO Reg. No. 47,343
Duane Morris LLP
901 New York Ave. NW,
Suite 700 East
Washington, D.C. 20001-4795
pcmuldoon@duanemorris.com

Nicole Candelori*
USPTO Reg. 77,218
Duane Morris LLP
901 New York Ave. NW,
Suite 700 East
Washington, D.C. 20001-4795
NCandelori@duanemorris.com

ATTORNEYS FOR REQUESTER

**Not admitted in D.C. Practice in
D.C. limited to matters and*

*proceedings before the U.S. Patent
and Trademark Office and federal
courts.*