Trials@uspto.gov
571.272.7822

Paper No. 35
Filed: January 12, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SPECTRUM BRANDS, INC., and
UNIKEY TECHNOLOGIES, INC.,
Petitioners,

v.

ASSA ABLOY AB,
Patent Owner.

Case IPR2015-01562[1]
Patent 8,150,374 B2

Before RAMA G. ELLURU, BEVERLY M. BUNTING, and CHRISTOPHER G. PAULRAJ, *Administrative Patent Judges*.

PAULRAJ, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

[1] Petitioner UniKey Technologies, Inc. from IPR2016-00686 has been joined as a Petitioner to this proceeding.

I. INTRODUCTION

A. Background

Petitioner Spectrum Brands, Inc. ("Spectrum") filed a Petition requesting *inter partes* review of claims 1, 3, 5, 7, 9–16, 21–23, 26, 29, and 30 of U.S. Patent No. 8,150,374 B2 (Ex. 1001, "the '374 patent"). Paper 1 ("Pet."). Assa Abloy AB ("Patent Owner") filed a Waiver of its Preliminary Response pursuant to 37 C.F.R. § 42.107(b). Paper 7. We determined that the information presented in the Petition demonstrated that there was a reasonable likelihood that Petitioner Spectrum would prevail in challenging these claims as unpatentable under 35 U.S.C. § 103(a). Pursuant to 35 U.S.C. § 314, the Board instituted trial on January 15, 2016, as to these claims of the '374 patent. Paper 7 ("Institution Decision"; "Inst. Dec.").

Patent Owner filed a Response to the Petition. Paper 16 ("PO Resp."). Petitioner Spectrum filed a Reply to Patent Owner's Response. Paper 19 ("Reply").

Thereafter, Petitioner UniKey Technologies, Inc. ("UniKey") filed a separate Petition for *inter partes* review, challenging claims 1, 3, 5, 7, 9–16, 21–23, 26, 29, and 30 of the '374 patent based on similar grounds to those presented by Spectrum. *See* IPR2016-00686, Paper 2. We instituted *inter partes* review based on UniKey's Petition to the extent that the grounds set forth therein are consistent with the basis for our institution of this proceeding, and joined UniKey as a Petitioner to this proceeding. *See* Paper 29 (instituting *inter partes* review based on UniKey's Petition and joining UniKey as a Petitioner to IPR2015-01562). As a condition of UniKey's joinder, the parties submitted a joint stipulation setting forth the parameters of UniKey's participation in this proceeding, including the requirement that

"UniKey will not have any right to separate or additional briefing, discovery, or speaking time for the duration of the contest involving [the '374 patent], through termination of the joined proceedings and through any related appeal." Paper 27, 1. UniKey also filed a statement "withdraw[ing] all grounds and arguments presented in IPR2016-00686 to the extent that they differ from the Panel's ground for institution in IPR2015-01562." Paper 32.[2]

An oral hearing was held on September 27, 2016. The transcript of the hearing has been entered into the record. Paper 34 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. Based on the record before us, we conclude that Petitioners have demonstrated by a preponderance of the evidence that claims 1, 3, 5, 9–16, 22, 23, 26, 29, and 30 of the '374 patent are unpatentable. We conclude that Petitioners have *not* demonstrated the unpatentability of claims 7 and 21 by a preponderance of the evidence.

B. Related Proceedings

The parties identify a related district court litigation matter involving the '374 patent: *HID Global Corporation et al. v. Kwikset Corporation et al.*, No. 14-cv-00947-CJC-DFM (C.D. Cal.). Pet. 5; Paper 5, 2.

C. The '374 Patent (Ex. 1001)

The '374 patent relates generally to the use of mobile devices in a secure access system to control access to assets, places, or things by having access credentials remotely assigned and revoked. Ex. 1001, Abstract. As

[2] We, therefore, collectively refer to Spectrum and UniKey as "Petitioners" in this Final Written Decision. However, we only consider the arguments and evidence presented along with Spectrum's Petition and Reply.

explained in the ’374 patent, “[i]n a conventional access control system, the door reader/interrogators positioned at ingress/egress points are connected to a control panel,” but “[t]here are . . . circumstances in which control panels associated with remote locations . . . are not regularly updated.” *Id.* at 2:55–3:2. Accordingly, “[i]f a person’s status changes from authorized to unauthorized, it might take a relatively long time for the control panel associated with a remote door to get the message and bar the credential associated with this person from access.” *Id.* at 3:2–5.

The ’374 patent seeks to address this situation by providing “a system and method that automatically updates credentials on a mobile device immediately after authorization changes have been made.” *Id.* at 3:18–21. Figure 1 of the ’374 patent is reproduced below:

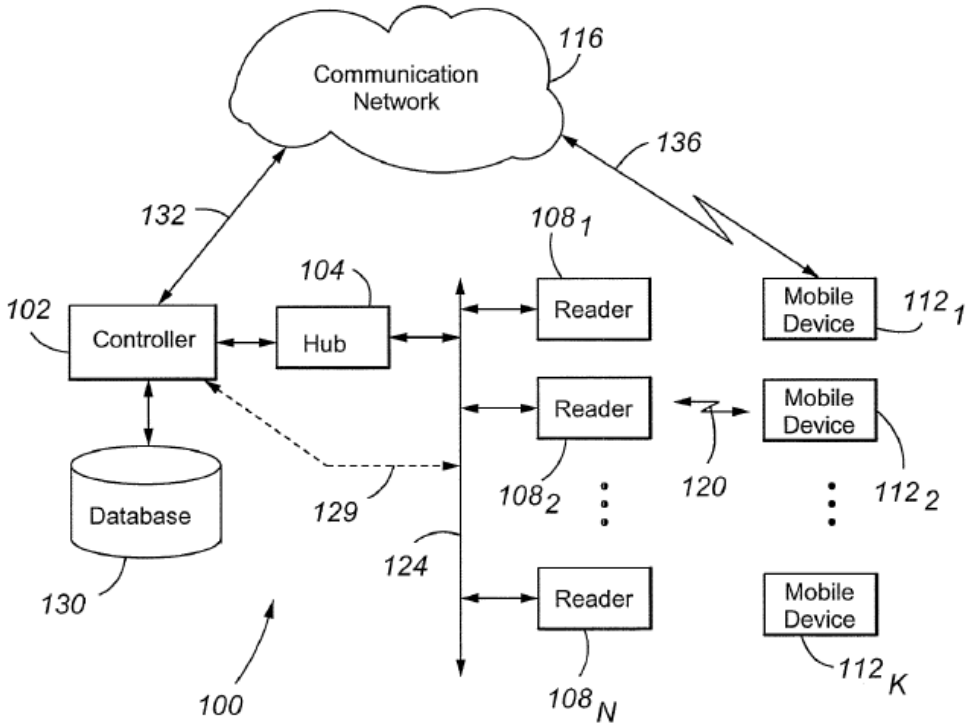

Fig. 1

Figure 1 shows an embodiment of a network access system 100 that comprises a controller 102, a hub 104, a plurality of readers 108_{1-n}, and a plurality of mobile devices 112_{1-k}. Ex. 1001, 4:65–5:2. "Each reader 108 is adapted for exchanging information with the controller 102 and for requesting data from the mobile device 112 to verify the authenticity of the mobile device." *Id.* at 6:10–13. Each reader 108 is associated typically with a particular asset, such as a door protecting access to a secure room or a computer lock protecting sensitive information. *Id.* at 6:13–16. Upon verification of credential information stored on the mobile device 112, the reader 108 or the controller 102 may generate signals that "facilitate[e] execution of the results of interrogating the mobile device (e.g., engages/disengages a locking mechanism, allows/disallows movement of a monitored article, temporarily disables itself, activates an alarm system, provides access to a computer system, provides access to a particular document, and the like)." Ex. 1001, 6:16–25. The system further includes a database 130, which can be either integral to or separate from controller 102, in order to maintain records associated with the readers 108, mobile devices 112, as well as algorithms used for testing the authenticity of the mobile devices. *Id.* at 5:63–6:3.

The system described in the '374 patent also utilizes a communication network 116, which provides a way for the controller 102 to automatically notify and/or update information to the mobile devices 112 related to the access system 100. *Id.* at 7:5–8. The '374 patent describes methods for automatically and remotely updating credential information on the mobile device either when the credential information is changed at the controller or

when a determined time interval between credential updates has passed. *Id.* at 9:36–10:50; Figs. 3, 4.

D. Illustrative Claims

Petitioners challenge claims 1, 3, 5, 7, 9–16, 21–23, 26, 29, and 30 of the ’374 patent. Claims 1, 14, and 30 are the only independent claims, and the remainder of the challenged claims depend from them respectively. Claims 1 and 14 are illustrative of the claimed subject matter, and reproduced below:

1. A method of remotely maintaining a secure access system, comprising:

storing, at a secure access system controller, a first set of credential data for at least one user of the secure access system, the secure access system controller in communication with a plurality of readers;

receiving, at the secure access system controller, a credential update for the at least one user of the secure access system; and

in response to receiving the credential update, the controller replacing the first set of credential data with a second set of credential data that is different from the first set of credential data and the controller further automatically initiating a system update process, the system update process comprising:

generating a message comprising information representing the controller's replacement of the first set of credential data with the second set of credential data;

determining at least one target for the message, wherein the at least one target comprises at least one mobile device associated with the at least one user;

transmitting the message to the at least one target;

receiving the message at the at least one mobile device; and

modifying at least a portion of memory of the at least one

mobile device according to the updated credential information,

wherein the modifying comprises at least one of disabling, revoking, and re-writing at least a portion of the memory.

14. A secure access system, comprising:

at least one mobile device comprising memory, wherein the memory comprises credential information;

> a controller in communication with a plurality of readers that secure one or more assets, the controller being configured to receive a credential update for at least one user of the secure access system, the credential update impacting the at least one user's permissions for accessing the one or more assets secured by the plurality of readers and, in response to receiving the credential update, automatically initiate a system update process, wherein during the system update process the controller automatically causes a message to be generated that comprises the updated credential, and causes the message to be transmitted to the at least one mobile device associated with the at least one user, wherein the plurality of readers are configured to determine an authenticity of the at least one mobile device, and wherein credential information on the memory is at least one of disabled, revoked, and re-written in response to receiving the message; and
>
> a database which maintains information related to the system, wherein the controller is further operable to cause a second message to be generated that comprises the updated credential and causes the second message to be transmitted to at least one of the database and the plurality of readers.

E. Patentability Challenges

In the Petition, Petitioner Spectrum challenged claims 1, 3, 5, 7, 9–16, 21–23, 26, 29 and 30 based on a) Nielsen[3] and Karkas,[4] and b) Nielsen and the Knowledge of a Person of Ordinary Skill in the Art. Pet. 22–51. We instituted *inter partes* review of all the challenged claims under 35 U.S.C. § 103(a) as obvious over Nielsen in view of Karkas. Inst. Dec. 16. During oral argument, Patent Owner challenged whether it received sufficient notice about which prior art teachings (i.e., Nielsen individually, or Nielsen in combination with Karkas) were relied upon by Petitioners to allege

[3] Nielsen, US 2002/0180582 A1, pub. Dec. 5, 2002 (Ex. 1002)
[4] Karkas, US 2002/0031228 A1, pub. Mar. 14, 2002 (Ex 1003).

obviousness for each of the claims challenged in this *inter partes* review. Tr. 29–33.

Although we grouped all the challenged claims together as part of a single ground of unpatentability in the final order of our Institution Decision, we nonetheless recognized that "Petitioner relies primarily on the teachings of Nielsen to allege the obviousness of claims 1, 3, 5, 8–16, 22, 23, 26, 29, and 30." Inst. Dec. 11. Indeed, we discussed the teachings of Karkas only with respect to the obviousness challenge of dependent claims 7 and 21. *Id.* at 13–15; *see also* Pet. 23 (stating that "Nielsen discloses nearly all the limitations of the Challenged Claims of the '374 patent," and discussing the "missing limitations [that] are supplied by Karkas" only for claims 7 and 21); Tr. 5:13–6:11 (Petitioner Spectrum's counsel clarifying that Petitioners are alleging single-reference obviousness based on Nielsen alone for all claims except claims 7 and 21). We further stated that "[b]ecause we have already taken the knowledge of a person of ordinary skill in the art into account in our consideration of the validity challenge based on Nielsen and Karkas, Petitioner has not presented a sufficient basis to institute on the second ground," noting that "the rationale that Petitioner has presented with respect to the challenge based on Nielsen in view of the knowledge of a person of ordinary skill in the art is equally applicable to the challenge based on the combination of Nielsen and Karkas." Inst. Dec. 15.

Therefore, contrary to Patent Owner's argument during the oral hearing (Tr. 29–33), we determine that Patent Owner received sufficient notice of which prior art teachings (i.e., Nielsen individually, or Nielsen in combination with Karkas) were relied upon by Petitioners to allege

obviousness in this *inter partes* review.[5] We further exercise our discretion to recast the challenges presented in the Petition in view of the specific prior art actually relied upon for the challenged claims. *See In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1273 (Fed. Cir. 2015) ("Nor does the IPR statute expressly limit the Board's authority at the final decision stage to the grounds alleged in the IPR petition."), *aff'd, Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131 (2016); *see also SightSound Techs., LLC v. Apple Inc.*, 809 F.3d 1307, 1312–13 (Fed. Cir. 2015) (noting that governing statutory provisions do not limit the Board's authority to proceed with AIA trial proceedings only on the specific statutory grounds alleged in the petition).

Accordingly, the following patentability challenges are at issue in this *inter partes* review:

Claims	**Basis**	**References**
1, 3, 5, 9–16, 22, 23, 26, 29, and 30	§ 103(a)	Nielsen
7 and 21	§ 103(a)	Nielsen and Karkas

II. ANALYSIS

A. Claim Construction

In an *inter partes* review, claim terms in an unexpired patent are interpreted according to their broadest reasonable constructions in light of

[5] Accordingly, we address Patent Owner's arguments regarding a lack of motivation to combine Nielsen and Karkas as applicable only to claims 7 and 21. *See* PO Resp. 10–19. With respect to the other challenged claims, we consider Karkas as relevant only to the extent it serves as evidence of the "background" knowledge of skilled artisans. *See Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1365 (Fed. Cir. 2015) ("Art can legitimately serve to document the knowledge that skilled artisans would bring to bear in reading the prior art identified as producing obviousness.").

the Specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2146 (2016). Under the broadest reasonable construction standard, claim terms are presumed to have their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). "Absent claim language carrying a narrow meaning, the PTO should only limit the claim based on the specification . . . when [it] expressly disclaim[s] the broader definition." *In re Bigio*, 381 F.3d 1320, 1325 (Fed Cir. 2004). "Although an inventor is indeed free to define the specific terms used to describe his or her invention, this must be done with reasonable clarity, deliberateness, and precision." *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

We determine, for purpose of this Final Written Decision, that no terms in the challenged claims require express construction. *See, e.g., Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011) ("[C]laim terms need only be construed 'to the extent necessary to resolve the controversy.'" (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

B. Content of the Prior Art

1. Nielsen (Ex. 1002)

Nielsen discloses an access control system for allowing access to a location that includes "an electronic key device, a lock control unit, and a computer system for use in such a system, a storage module for use in such an electronic key device, and a method of managing a predetermined access right to a location." Ex. 1002 ¶ 1. The computer system is referred to as an

"access code management system." *Id.* ¶ 128. Nielsen teaches that the electronic key device may be a mobile phone. *Id.* ¶¶ 38, 125. Figure 2b, reproduced below, illustrates one embodiment of Nielsen's system:

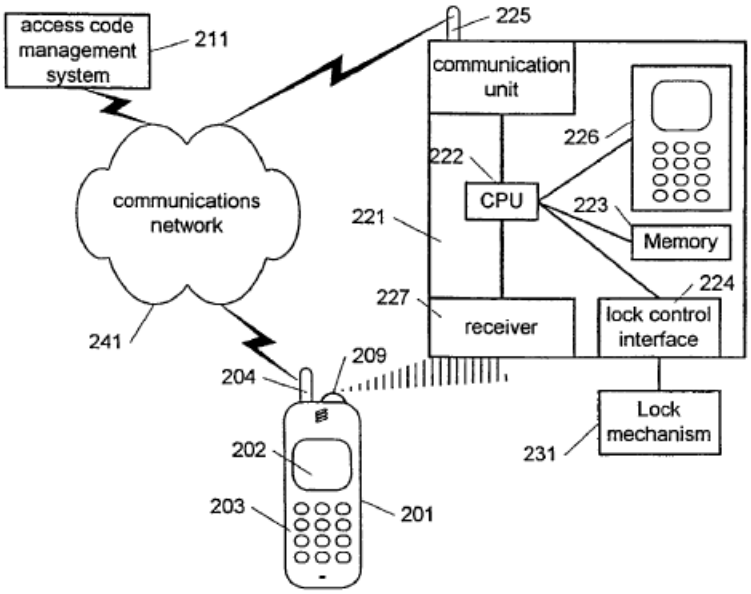

Fig. 2b

The embodiment of Figure 2b includes an electronic key device 201, such as a mobile phone, that is equipped with a communication port 209 for transmitting control signals to the lock control unit 221 and a keypad "for selecting one of the access codes which may be stored in the device." Ex. 1002 ¶ 125. Additionally, "[t]he lock control unit 221 comprises a communications unit 225 to receive the data transmitted from the access code management system 211." *Id.* ¶ 129; *see also id.* ¶ 44 ("transmitting, via a communications network, at least one access code from an access code management system to a . . . plurality of electronic key devices and lock control units substantially simultaneously").

Figure 3 of Nielsen is reproduced below:

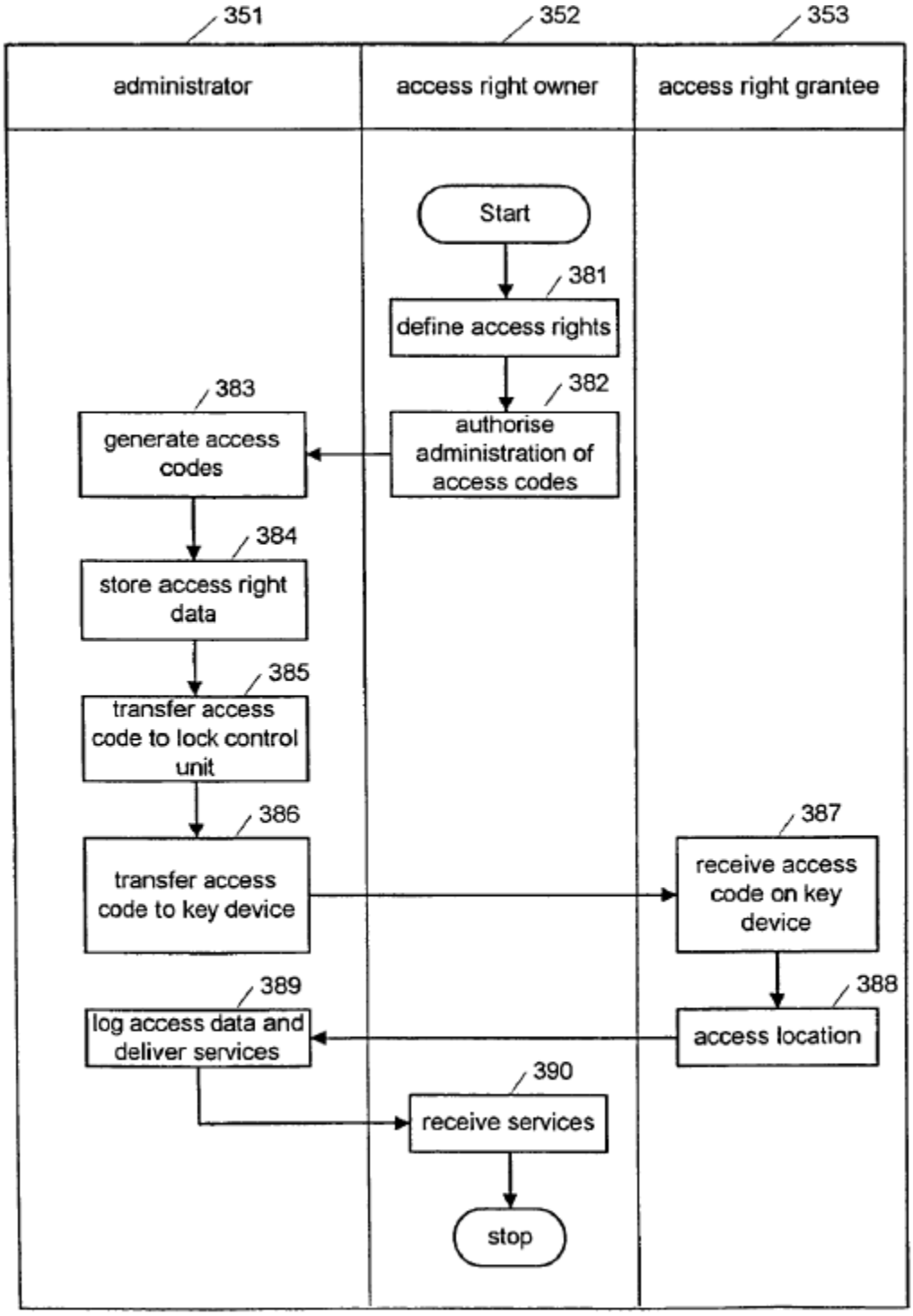

Fig. 3

Figure 3 of Nielsen "shows a flow diagram of the access code management

process according to an embodiment of the invention" described in Nielsen. Ex. 1002 ¶ 106. Nielsen states that "[t]he access code management system 211 generates and administers the access codes as described in connection with FIGS. 3 and 9*a-b*." *Id.* ¶ 128. According to Nielsen:

> The access code management system 211 transmits access codes to the electronic key device 201 and/or the lock control unit 221. The access codes may be transmitted upon request from a user or automatically. Additionally, the access code may be transmitted periodically, in order to replace the access codes on a lock control unit and the corresponding electronic key devices, thereby improving the security of the system. The access code management system 211 may also automatically, or upon request, invalidate access codes by sending a corresponding control signal to the lock control unit 221 and/or the electronic key device 201.

Id. Access codes may be transmitted using short messaging service (SMS) or other higher speed data channels. *Id.* ¶ 127. Nielsen further teaches that "[w]hen data items comprising access codes are received by the aerial 504 [of the electronic key device] from the access code management system or a service provider, they are routed via the circuit 505 to the SIM card 506, where the control unit 508 stores the data in the memory 507b." *Id.* ¶ 152.

2. Karkas (Ex. 1003)

Karkas teaches a system for providing secure "access to an entity" using mobile stations, i.e., mobile phones, operating on wireless cellular networks. Ex. 1003 ¶¶ 1, 2. Karkas discloses transmitting key information over a network from a server to a mobile station. *Id.* ¶ 32 ("the server 40 provides the mobile station with key information"). The system of Karkas also includes a Bluetooth device that acts as a lock. *Id.* ¶ 25 ("the Bluetooth device [may] be a lock or an access device"). The mobile station sends key information to the Bluetooth device, which may provide access to a room if

the key is valid. *Id.* ¶ 36 ("the mobile station sends the key information to the Bluetooth device"); ¶ 38 ("if the key is valid, then the Bluetooth device 24 will provide access for example to the room"). Karkas further discloses that keys may expire after a certain time period, and "that the mobile station can automatically delete those keys which are out of date." *Id.* ¶ 53.

C. Level of Ordinary Skill in the Art

According to Petitioners, "[a] person having ordinary skill in the field at the time of the purported invention of the '374 Patent would have at least a bachelor's degree in computer science, computer engineering, or electrical engineering combined with at least one year of industry experience in security systems." Pet. 14 (citing Ex. 1004 ¶¶ 40–42). Patent Owner does not address the level of ordinary skill in its Response. However, Patent Owner's expert, Dr. John Villasenor, "conclude[s] that a person of ordinary skill in the art would have at least an undergraduate degree in computer science or electrical engineering and one year of experience in mobile devices and the associated communications networks and systems applied in the context of secure access control systems." Ex. 2002 ¶ 39.

We agree with Dr. Villasenor insofar as the relevant field for the '374 patent is more accurately defined as "electronic control access systems" rather than merely "security systems" (*id.* ¶ 41), but otherwise find no meaningful difference between the level of ordinary skill in the art proposed by the parties' experts. We also recognize that the level of skill in the art is reflected in the prior art references themselves, which focus on mobile-phone based electronic access systems, and take that into consideration in our analysis. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). As such, we determine that a person of ordinary skill in the art would

have least an undergraduate degree in computer science or electrical engineering and one year of experience in electronic control access systems.

D. Obviousness Analysis

In the Petition, Petitioners included a claim chart mapping the teachings of Nielsen and/or Karkas to each of the challenged claims. Pet. 25–50. In addition to the teachings of the references, Petitioners also rely upon the Declaration of Professor Matthew Green, Ph.D. Ex. 1004. Based on the record developed during this proceeding, we determine that Petitioners have shown by a preponderance of the evidence that Nielsen renders obvious claims 1, 3, 5, 8–16, 22, 23, 26, 29, and 30. We adopt the arguments and evidence set forth in the Petition as applied to these claims. We determine, however, that Petitioners have *not* shown by a preponderance of the evidence that Nielsen in combination with Karkas renders obvious claims 7 and 21. We have considered the parties' arguments and evidence, which we address below.[6]

[6] Patent Owner also argues that "[b]y merely citing to various portions of each of Nielsen and Karkas in parallel, without providing any explanation of the significance of the quoted passages with respect to the recited claim language, Petitioner has failed to satisfy its obligation under 35 U.S.C. § 322(a)(3) and 37 C.F.R. § 42.22(a)(1)." PO Resp. 57. We determined that the Petition satisfied these requirements when instituting *inter partes* review in this proceeding. In particular, the Petition provided an explanation as to the significance of the quoted passages from the prior art by identifying the claim elements to which they correspond, explaining any differences between the prior art and the claim elements, and identifying reason to combine the references. Pet. 16–24. The Petition also included detailed claim charts, identifying supporting evidence, for the patentability challenges presented. *Id.* at 25–50. We, therefore, conclude that the Petition satisfies the requirements of 35 U.S.C. § 322(a)(3) and 37 C.F.R. § 42.22(a)(1).

1. Obviousness Based on Nielsen Alone

a. Claim 1

Independent claim 1 recites, in relevant part, the steps of a) "storing, at a . . . controller, a first set of credential data for at least one user of the secure access system, the secure access system controller in communication with a plurality of readers"; and b) "receiving, at the . . . controller, a credential update for the at least one user." Ex. 1001, 12:35–41 (steps "1a" and "1b"). In the claim chart included with the Petition, Petitioners cite to paragraphs 44, 128, and 132 of Nielsen to allege that step 1a is taught, and to paragraph 132 and Figure 3 of Nielsen to allege that step 1b is taught. Pet. 26–28.

Patent Owner argues that the Petition improperly inverts steps 1a and 1b when mapping those limitations to Nielsen. PO Resp. 20–27. In particular, Patent Owner contends that Nielsen's Figure 3 illustrates that the alleged "receiving" step—which includes step 381 ("define access rights"), step 382 ("authorize administration of access codes"), and step 383 ("generate access codes")—is performed before the alleged "storing" step—i.e., step 384 ("store access data"). *Id.* at 23–24. Patent Owner points out that Nielsen ¶ 132 teaches that step 381 is the "initial step" of the process depicted in Figure 3. *Id.* at 22. Patent Owner further argues that the Petition fails to justify the mapping of steps 1a and 1b, both performed by the "controller," onto two different entities taught by Nielsen—the "administrator" and "owner." *Id.* at 27–28.

Petitioners, in the Reply, argue that steps 1a and 1b do not require a particular order. Reply 10–12. Regardless, Petitioners contend that Nielsen discloses the performance of steps 1a and 1b in either order because

"Nielsen teaches repeatedly performing [the process of Figure 3] when a user's access code is ***replaced*** with a new access code." *Id.* at 12–13 (citing Ex. 1002 ¶ 128). Petitioners also argue that Nielsen discloses a single entity, i.e., the "administrator," which receives and stores credential data as claim 1 recites. *Id.* at 14–15.

We agree with Patent Owner that claim 1 requires that step 1b follow step 1a. As recognized by Petitioners, the Federal Circuit has observed that "[u]nless the steps of a method actually recite an order, the steps are not ordinarily construed to require one." Reply 10–11 (quoting *Altiris, Inc. v. Symantec Corp.*, 318 F.3d 1363, 1369 (Fed. Cir. 2003)). In this case, however, the plain language of claim 1 requires "storing . . . a first set of credential data," "receiving . . . a credential update," and "in response to receiving the credential update, . . . replacing the first set of credential data with a second set of credential data that is different from the first set of credential data." Ex. 1001, 12:35–45. Thus, we agree that "[l]ogic compels the conclusion that step 1b follows step 1a, because the controller's receipt of a 'credential update' associated with 'different' data would follow the first set of credential data previously stored at the controller." PO Resp. 21. *See Mformation Techs., Inc. v. Research In Motion Ltd.*, 764 F.3d 1392, 1398–99 (Fed. Cir. 2014) ("[A] claim requires an ordering of steps when the claim language, as a matter of logic or grammar, requires that the steps be performed in the order written, or the specification directly or implicitly requires an order of steps." (internal quotation marks omitted)).

With reference to Figure 3, Nielsen teaches that "[i]n the initial step 381, the access right owner 352 defines the access rights to be granted, possibly including a list of possible access right grantees," that "[i]n step

382, the access right owner 352 authorizes the administrator 351 to generate and assign access keys," that "[b]y means of an access code management system, the administrator in step 383 transforms the access right definition into a set of electronic access codes," and that "[i]n step 384, the access codes and other related data are stored." Ex. 1002 ¶ 132. Thus, we agree with Patent Owner that "the relied upon steps of Nielsen teach a process that differs from the steps recited in claim 1" insofar as Figure 3 shows the "receiving" step(s) performed before the "storing" step 384. PO Resp. 25. Specifically, that Figure 3 of Nielsen does not show that the process is iterative.

Nonetheless, we find that Nielsen suggests a process wherein access codes (i.e., "credential data") that are stored in the access code management system are periodically replaced with new and different access codes (i.e., a "credential update"). *See* Ex. 1002 ¶ 128 ("[T]he access code may be transmitted periodically, in order to replace the access codes on a lock control unit and the corresponding electronic key . . . ."). The same paragraph of Nielsen also indicates that "[t]he access code management system 211 generates and administers the access codes as described in connection with FIGS. 3 and 9a-b." *Id.* Thus, we determine that the skilled artisan would have found it obvious to initially store access codes, and thereafter repeat the process described in the flow chart of Figure 3 in order to replace previously stored access codes. As explained by Dr. Green, the purpose of Nielsen periodically replacing previous access codes "is to improve the security of the system," such as in the situation when codes are invalidated if misused or lost. *See* Ex. 1004 ¶ 29. Nielsen explicitly references Figure 3 when referencing how the access code management

system administers access codes (Ex. 1002 ¶ 128), thereby providing a suggestion and motivation to modify Nielsen's teachings so as to repeat the process of Figure 3 when replacing previously stored access codes in order to improve security.

We further find that Nielsen teaches a single entity that both receives and stores access codes. We are unpersuaded by Patent Owner's argument that the Petition improperly maps steps 1a and 1b, both performed by the controller, onto two different entities. PO Resp. 27–28. Although Figure 3 shows that the access right owner (352) "define[s] access rights" (step 381) and "authorize[s] administration of access codes" (step 382), it is administrator (351) that "generate[s] the access codes" (step 384) and "store[s] access right data" (step 384). Ex. 1002, Fig. 3. Thus, when the administrator 351 generates and stores access codes based on access rights defined by the access right owner, we find that it is a single entity that plays a role with respect to both steps 1a and 1b.

Claim 1 further requires a step of "replacing the first set of credential data with a second set of credential data that is different from the first set of credential data." Ex. 1001, 12:43–45 (step "1c"). Petitioners contend that Nielsen teaches this limitation when it periodically replaces access codes used by locks and/or keys, as discussed above. Pet. 28 (citing Ex. 1002 ¶ 128). Petitioners also contend that "Nielsen teaches that the access code management system performs this periodic 'replacing' step 'in response to receiving' the access right definition," which "specifies how often the replacing occurs." *Id.* at 28–29 (citing Ex. 1002 ¶¶ 33, 37).

With respect to step 1c, Patent Owner argues that the cited teachings of Nielsen ¶ 128 "describe how '***the*** access code' (singular) may be

transmitted periodically to replace 'the access code***s***' on a lock control unit and the corresponding electronic key devices," and "[t]his refers to sending the ***same*** access code, preventing change to an access code in the controller rather than yielding an ***update*** to that access code." PO Resp. 29 (citing Ex. 2002 ¶¶ 142–148, 164, 212). Moreover, Patent Owner contends, "this passage from Nielsen fails to describe a process that occurs ***within the controller itself***, to update credential data stored on the controller including replacing a first set with a different, second set of credential data." *Id.* (citing Ex. 2002 ¶¶ 143, 148). Additionally, Patent Owner argues that ¶¶ 33 and 37 from Nielsen fall short of instructing a skilled artisan about how the requirements of claim 1 can be performed "from within the controller itself." *Id.* at 30 (citing Ex. 2002 ¶¶ 145–146). We are unpersuaded by these arguments.

We find no basis in the record to conclude that Nielsen teaches the transmission of only the *same* access code when it discusses periodically "replacing" access codes. Ex. 1002 ¶ 128. To the contrary, Nielsen expressly teaches that "an access code may be replaced by a *new* access code, for example in cases of misuse or loss of an electronic key device." *Id.* ¶ 51 (emphasis added). Moreover, to the extent Nielsen does not explicitly teach that the replacement access codes are different from prior access codes, we determine that such a feature would have been an obvious implementation of Nielsen's system because it would be consistent with the goal of "improving the security of the system" set forth in Nielsen. *Id.* ¶ 128; *see also id.* ¶ 33 (stating that the "access right profile . . . may be *changed* on short notice or in regular or random time intervals in order to increase the security of the access control"). As explained by Petitioners,

"[s]ending the same access codes over and over would hardly increase security as Nielsen instructs, . . . and would be as insecure as a locksmith providing an identical house key after someone's wallet and keys were lost." Reply 16–17. We also agree with Petitioners' position that Nielsen discloses that the replacement of access codes occurs within the controller. *Id.* at 17. In particular, Nielsen explains that the "access code management system 211 [(i.e., the claimed controller)] transmits access codes to the electronic key device 201 and/or the lock control unit 221," and therefore performs the function of periodically replacing the access codes. Ex. 1002 ¶ 128.

Claim 1 also requires, in relevant part, a system update process that includes generating a message concerning the replacement of credential data, and "determining at least one target for the message, wherein the at least one target comprises at least one mobile device associated with the at least one user." Ex. 1001, 12:51–53 (step "1c(ii)"). The Petition alleges that Nielsen satisfies this requirement based on its teaching that "[t]he access code management system 211 transmits access codes to the electronic key device 201," and that "the access right grantee 353 has electronic key devices." Pet. 30 (citing Ex. 1002 ¶¶ 128, 133–134). The Petition also relies upon Nielsen's disclosure that the electronic key device 201 may be a "mobile phone" or a "mobile communication device." *Id.* (citing Ex. 1002 ¶¶ 38, 113, 125).

Patent Owner argues that step 1c(ii) "is an active step that requires the controller to determine which mobile device (or devices) from a group should receive the credential update message." PO Resp. 33. Patent Owner argues that the cited passages of Nielsen do not disclose the determination of a target prior to transmission. *Id.* at 33–34. We disagree.

Nielsen teaches that access codes are transferred only to the key device(s) that belong to the specific access right grantee. Ex. 1002 ¶¶ 128, 133–134. Nielsen further teaches "*customizing* an access right profile for each electronic key device" and states that "the access right profile of *individual* electronic key devices… may be changed." *Id.* ¶¶ 19, 21 (emphases added). Thus, we find that Nielsen teaches that the system determines which of the individual electronic key devices (i.e., mobile phone) should be targeted to receive the replacement access codes, thereby satisfying the requirement of step 1c(ii).

Patent Owner has not made any additional arguments regarding claim 1.[7] We adopt Petitioners' arguments and evidence as to why Nielsen teaches the other undisputed limitations of claim 1. *See* Pet. 25–32. We therefore determine that Petitioners have shown, by a preponderance of the evidence, that Nielsen suggests the requirements of claim 1.

b. Claims 14 and 30

Independent claim 14 is directed to a "secure access system" that includes a "controller . . . configured to receive a credential update" and "automatically initiate a system update process" in a manner similar to the method recited in claim 1. Ex. 1001, 13:44–64. Independent claim 30 is directed to a "mobile device for use by a user in a secure access system" that includes "an interface . . . operable to receive messages relating to updated-credential information," and that "upon receipt of a first message, the credential information for the user is automatically changed from a first state to a second state," and that "in the event that the first message is not

[7] *See* Paper 8, 3 ("The patent owner is cautioned that any arguments for patentability not raised in the response will be deemed waived.").

received, the credential information is maintained in the first state and as a result becomes obsolete." *Id.* at 14:61–15:13. Petitioners rely upon the same teachings of Nielsen discussed above to allege that claims 14 and 30 are also obvious. *See* Pet. 37–43, 47–50.

Patent Owner makes similar arguments to those presented for claim 1. In particular, with respect to claim 14, Patent Owner argues that Nielsen does not disclose a controller configured to receive a credential update for at least one secure access system." PO Resp. 37–41. With respect to claim 30, Patent Owner also argues that "Nielsen does not disclose 'credential information' that is 'changed from a first state to a second state' and 'becomes obsolete,' all based on 'receipt' or non-receipt of 'a first message.'" PO Resp. 45–48. Patent Owner contends that "[t]he Petition fails to demonstrate that Nielsen is capable of sending updated credential information, let alone sending a credential update that changes the state of a credential." *Id.* at 45.

For the reasons discussed above, we find that Nielsen renders obvious the claim requirements related to a "credential update" when it discusses the access code management system 211 being used to automatically and periodically transmit replacement access codes to the electronic key device 201 and/or the lock control unit 221. *See* Ex. 1002 ¶ 128. Because Nielsen teaches replacement by a "new access code" and the need to increase security (Ex. 1002 ¶¶ 33, 51, 128), we disagree with Patent Owner's contention that Nielsen only describes transmitting the same access code over and over again. PO Resp. 46. As such, we find the replacement of the access codes in an electronic key device would also satisfy the requirement

that "the credential information for the user is automatically changed from a first state to a second state" set forth in claim 30.

Furthermore, in view of Nielsen's teaching that access rights may be granted only for "one or more validity periods" or a limited "number of times the access right is valid" (Ex. 1002 ¶ 37), we find that Nielsen's system satisfies the requirement that "in the event that the first message is not received, the credential information is maintained in the first state and as a result becomes obsolete" also set forth in claim 30. Contrary to Patent Owner's argument, we disagree that Petitioners' expert Dr. Green admitted that Nielsen alone fails to suggest this feature. PO Resp. 48. Rather, Dr. Green testified that "Nielsen teaches a structure of credentials that have properties, such as validity periods and other structures, such as the number of times the access right is valid," and "it would be obvious to a person of ordinary skill in the art that these [structures] ultimately would result in credentials becoming obsolete if you implemented this." Ex. 2004, 195:11–18. Although Dr. Green further testified that "Karkas really provides expressed disclosure of how you would go about implementing the mechanism that's described in Nielsen" (*id.* at 195:18–20) he did not indicate that that reliance on Karkas's teachings is necessary to render claim 30 obvious. *See id.* at 195:25–196:8 ("Nielsen describes a mechanism, and and Karkas provides expressed disclosure of how to implement a mechanism. . . . It's as though Nielsen says, 'Make a can of tomato soup,' and Karkas says, 'Here are instructions for making a can of tomato soup.'").

We adopt Petitioners' arguments and evidence as to why Nielsen teaches or suggests the other undisputed limitations of claims 14 and 30.

Accordingly, based on the preponderance of the evidence before us, we conclude that Nielsen satisfies claims 14 and 30.

c. Claim 3

Claim 3 depends from claim 1 and recites:

> wherein the at least one mobile device has the first set of credential data stored thereon prior to the at least one mobile device receiving the message, and wherein upon receiving the message from the controller, the first set of credential data on the at least one mobile device is changed to the second different set of credential data and wherein the message is transmitted to the at least one mobile device without the controller receiving a request for the message from the at least one user.

Ex. 1001, 12:64–13:5.

For this limitation, the Petition cites to Nielsen's teaching that access codes may be stored in the electronic key device 201, and the access code may be transmitted periodically in order to replace the access codes on the corresponding electronic key device. Pet. 32 (citing Ex. 1002 ¶¶ 125, 128, 152). Patent Owner argues that "the message" recited in claim 3 refers to the credential update message generated by the controller, and that Nielsen ¶ 128 "refers to periodic transmission of the ***same*** access code, not a credential ***update***." PO Resp. 34.

For the reasons set forth above, we disagree with Patent Owner's contention that Nielsen only describes transmitting the same access code over and over again. We adopt Petitioners' arguments and evidence as to why Nielsen teaches the limitation of claim 3. Based on the preponderance of the evidence before us, we conclude that the teachings of Nielsen identified by Petitioners describe the limitations of challenged claim 3.

d. Claims 5 and 16

Claim 5 depends from claim 1, and recites "in the event that the at least one mobile device does not receive the message and is subsequently presented to a first reader in the plurality of readers, determining, by the first reader, that the at least one mobile device is invalid." Ex. 1001, 13:10–04. Similarly, claim 16 ultimately depends from claim 14, and recites "in the event that the at least one mobile device does not receive the message, credentials of the at least one mobile device become obsolete." *Id.* at 14:13–15.

For claim 5, the Petition relies upon Nielsen's teaching that the lock control unit verifies the access codes, and "[i]f the verification 689 of the access code fails, the lock mechanism is not operated." Pet. 33 (citing Ex. 1002 ¶ 162). For claim 16, the Petition alleges that Nielsen teaches that access rights become obsolete after one or more validity periods or a number of times the access right is valid are exceeded. *Id.* at 45 (citing Ex. 1002 ¶ 37).

With respect to both these claims, Patent Owner argues that the cited passages of Nielsen do not disclose that invalidity or obsolescence of the mobile device is tied to not receiving the credential update message. PO Resp. 35–36, 41–42. We disagree, as we find that Nielsen fairly suggests that verification will fail, thereby rendering the electronic key device invalid or obsolete, if an "old" access code expires (as a result of exceeding a validity period or number of uses), and a new access code is not received to replace it. Ex. 1002 ¶¶ 37, 162. Patent Owner argues that Petitioner Spectrum's expert, Dr. Green, admitted that "there are many reasons that verification could fail that go beyond not having the key." PO Resp. 35

(citing Ex. 2004, 159:22–23). Dr. Green also testified that Nielsen suggests that the mobile device's failure to receive an updated credential is certainly one of those reasons. *See* Ex. 2004, 149:6–16 (stating that Nielsen ¶ 162 describes "the situation where your old credential is not valid, and you did not receive a message giving you a new credential, then you won't be able to open the door").

We adopt Petitioners' arguments and evidence as to why Nielsen teaches the limitations of claims 5 and 16. Based on the preponderance of the evidence before us, we conclude that the teachings of Nielsen identified by Petitioners describes the limitations of challenged claims 5 and 16.

e. Claim 12

Claim 11 depends from claim 1 and recites, *inter alia*, "generating a second message comprising information related to the at least one mobile device being presented to the reader," and "sending the second message to at least one of a database, controller, and another mobile device." Ex. 1001, 13:33–37. Claim 12 depends from claim 11, and further recites that "wherein the second message is sent via a short message service (SMS) message." *Id.* at 13:38–39.

Petitioners contend that the "second message" recited in claims 11 and 12 is satisfied by Nielsen's disclosure that "log data" may be stored on the electronic key device and sent to be stored in a database. Pet. 36 (citing Ex. 1002 ¶¶ 62, 66). With respect to the requirement in claim 12 that the second message is sent via SMS, Petitioners further rely upon Nielsen's teaching that "[t]his data transmission may utilize the so-called Short Messaging Service (SMS)." *Id.* at 36–37 (citing Ex. 1002 ¶ 127).

Patent Owner argues that Nielsen ¶ 127 only teaches that the SMS message carries access codes and not log data. PO Resp. 37. We recognize that the "data transmission" mentioned in that paragraph refers to the prior sentence, which states that "[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." Ex. 1002 ¶ 127. Nonetheless, Patent Owner fails to direct us to anything in Nielsen to suggest that the use of SMS messages is limited to sending only access codes and that log data could not be transmitted via SMS. Rather, Nielsen expressly teaches that, instead of storing log data locally in the lock control unit or electronic key device, "a message identifying the above session may be sent to the access code management system, where it is stored . . . preferably in a database." *Id.* ¶ 166. Patent Owner contends that Petitioners' expert Dr. Green "conceded that the omitted language [from Nielsen ¶ 127] in reality discloses using SMS to carry access codes and not log data." PO Resp. 37 (citing Ex. 2002 ¶¶ 177; Ex. 2004, 171:11–172:11 and 172:24–173:22). However, as further explained by Dr. Green, Nielsen provides an example of SMS communication for the transmission of access codes from the access management system to the electronic key device, but "the existence of those channels as the means to communicate sheds light in the context" of Nielsen ¶ 166. Ex. 2004, 173:23–174:12. We are, therefore, persuaded by Petitioner's arguments and evidence that a skilled artisan would have had reason to utilize the existing SMS communication channel to transmit log data in Nielsen's system because it would have taken advantage of infrastructure already present in the mobile phone.

We adopt Petitioners' arguments and evidence as to why Nielsen teaches the limitation of claim 12. Accordingly, based on the preponderance of the evidence before us, we conclude that the teachings of Nielsen identified by Petitioners suggests the requirements of claim 12.

f. Claim 26

Claim 26 depends from claim 14, and recites "wherein the at least one mobile device comprises a plurality of mobile devices, and wherein credential information in less than all of the plurality of mobile devices is altered." Ex. 1001, 14:48–51. For this claim, Petitioners rely upon Nielsen's teaching of "customizing an access right profile for each electronic key device," wherein "the access right profile of individual electronic key devices and lock control units may be changed on short notice or in regular or random time intervals in order to increase the security of the access control." Pet. 46–47 (citing Ex. 1002 ¶¶ 19, 21).

Patent Owner argues that "[b]ecause the system of Nielsen clearly fails to describe the 'credential update' of claim 14 . . . , the system necessarily also lacks the functionality to transmit the credential update to all of the mobile device, let alone a subset as required by claim 26." PO Resp. 43. As discussed above, we determine that the requirements of a "credential update" in claim 14 are suggested by Nielsen. Patent Owner further argues that the cited teachings of Nielsen (customized access rights profiles, and variable change schedules to the access rights profiles) are unrelated to selective data transmission, and the Petition fails to demonstrate "how these two features can be combined to describe a selective data transmission of an updated credential to a subset of devices" or "how such a combination would have been obvious for one of ordinary skill in the art in order to do

so." *Id.* at 43–44. We are not persuaded by this argument, as we find that Nielsen's teaching that the access right profile of individual electronic key devices may be customized or changed, is a teaching that credential information in less than all of the plurality of mobile devices is altered. Ex. 1002 ¶¶ 19, 21.

We adopt Petitioners' arguments and evidence as to why Nielsen teaches the limitation of claim 26. Accordingly, based on the preponderance of the evidence before us, we conclude that the teachings of Nielsen identified by Petitioners suggests the requirements of claim 26.

g. Remaining Claims

Patent Owner has not presented any separate arguments for challenged claims 9–11, 13, 15, 22, 23, and 29. *See* PO Resp. 19–50. Based on the arguments and evidence presented, we find Petitioners' evidence that Nielsen teaches or suggests the limitations recited in these claims to be persuasive, and adopt Petitioners' reasoning. *See* Pet. 34–37 and 43–47.

2. Obviousness Based on Nielsen and Karkas (Claims 7 and 21)

Claim 7 depends from claim 1, and recites: "disabling at least a portion of the memory unless an enabling message is received." Ex. 1001, 13:17–19. Claim 21 depends from claim 14, and recites: "wherein the mobile device comprises a timing-out mechanism, wherein the timing-out mechanism is operable to disable the memory unless an enabling message is received from the controller." *Id.* at 14. As discussed above, the teachings of both Karkas and Nielsen are relied upon to allege that these dependent claims are obvious. *See* Pet. 23; Inst. Dec. 13–15.

Petitioners acknowledge that Nielsen does not expressly disclose disabling the stored access codes unless an enabling message is received.

Pet. 24 (citing Ex. 1004 ¶ 52). According to Petitioners, the requirement of "disabling" memory is satisfied by "changing the contents of memory to prevent those contents from being used." *Id.* at 23 (citing Ex. 1001, 9:44–47; Ex. 1004 ¶ 51). Petitioners contend that "Karkas, however, teaches this limitation in at least two ways: (1) keys that require a PIN, and (2) keys that expire unless their validity time is extended." *Id.* Petitioners, therefore, assert that Karkas teaches that the memory is disabled unless a PIN or new validity time (i.e., the enabling message) is provided. *Id.* Petitioners further assert that Karkas' disclosure of providing a new validity period for an access code also teaches a "timing-out mechanism" to disable memory, as required by claim 21.

Patent Owner argues that it would not have been obvious to combine Nielsen and Karkas for any of the challenged claims. PO Resp. 10–19. With respect to claims 7 and 21 in particular, Patent Owner argues that the skilled artisan "would not combine Nielsen and Karkas, as the latter teaches away from Nielsen in that Karkas discourages connecting the locks (or readers) to," whereas Nielsen "promotes such connectivity." *Id.* at 36, 42.

We agree with Patent Owner that Petitioners have not articulated a sufficient reason with rational underpinning to combine the teachings of Nielsen and Karkas to arrive specifically at the method and system recited, respectively, in claims 7 and 21. Rather, Petitioners only identify general reasons in the Petition, such as the fact that a) "both references were published in the same year, and both disclose analogous access control systems"; b) "[b]oth references describe using mobile devices as keys, electronic locks, and a central management system (the server or controller)"; and c) "[b]oth Nielsen and Karkas describe mobile phones with

embedded electronic access codes and similar wireless communication protocols." Pet. 22. According to Petitioners, "[b]ecause the access control systems in Nielsen and Karkas are so similar, many features disclosed in Karkas are readily compatible and easily incorporated into Nielsen." *Id.*

Petitioners, however, do not explain sufficiently why the skilled artisan would turn to Karkas's teaching in order to remedy the acknowledged deficiency in Nielsen with respect to the requirements of claims 7 and 21. "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).[8] For example, Petitioners contend that "skilled artisans would have recognized that the requirement that a user enter a PIN number to access an electronic key could be implemented as a 'password' in Nielsen," but do not identify any specific benefit to be gained from using Karkas's PIN number as Nielsen's password. *Id.* at 22–23. Nor have Petitioners identified any benefit from using the time limits taught by Karkas, especially when Nielsen itself teaches the use of "validity periods." Ex. 1002 ¶ 37; Ex. 1003 ¶¶ 48–49. The mere fact that Nielsen and Karkas are "similar" in many respects, and that Karkas independently teaches a "timing-out mechanism" and disabling

[8] Petitioners contend that "[a]s discussed in the accompanying Declaration of Dr. Green, there are many other reasons to combine these Nielsen and Karkas." Pet. 23 (citing Ex. 1004 ¶¶ 44–49). However, we decline to consider any "other reasons" that are not discussed specifically in the Petition, as it would otherwise amount to an improper incorporation by reference. *See* 37 C.F.R. § 42.6(a)(3) ("Arguments must not be incorporated by reference from one document into another document.").

memory unless an enabling message is received, is not in itself a reason to combine their teachings in the manner claimed. *Cf. Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1369 (Fed. Cir. 2012) (noting that "both of these references independently accomplish similar functions," and "[b]ecause each device independently operates effectively, a person having ordinary skill in the art . . . would have no reason to combine the features of both devices into a single device"). Moreover, as explained in *KSR*, "a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." *KSR*, 550 U.S. at 418.

Accordingly, we determine that a preponderance of the evidence does not support a reason to combine Nielsen's and Karkas's teachings in order to include the features of disabling memory or a timing-out mechanism in the manner proposed by Petitioners for claims 7 and 21.

3. Objective Indicia of Non-Obviousness

In an obviousness analysis, we must also consider any objective evidence of nonobviousness ("secondary considerations") that is presented. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). The totality of the evidence submitted may show that the challenged claims would not have been obvious to one of ordinary skill in the art. *In re Piasecki*, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984). To be relevant, evidence of nonobviousness must be reasonably commensurate in scope with the claimed invention. *In re Kao*, 639 F.3d 1057, 1068 (Fed. Cir. 2011). Furthermore, there must be a nexus between the merits of the claimed invention and the evidence of secondary considerations. *In re GPAC Inc.*, 57 F.3d 1573, 1580 (Fed. Cir. 1995).

As objective indicia of non-obviousness for all the challenged claims, Patent Owner relies upon industry praise and commercial success for its physical access control systems (PACS) products. PO Resp. 50–57. We have considered the secondary considerations evidence presented by Patent Owner, but do not find it sufficient, individually or in combination, to "overcome the strong prima facie case of obviousness" made of record. *See Wyers v. Master Lock Co.*, 616 F.3d 1231, 1246 (Fed. Cir. 2010).

a. Whether Patent Owner's Products Practice the Claims of the '374 Patent

To demonstrate nexus, Patent Owner first contends that its mobile device-based PACS products practice the claims of the '374 patent, as shown in the expert declaration of Dr. John Villasenor, Ph.D. PO Resp. 52. In particular, Patent Owner asserts that "Dr. Villasenor confirmed that the ASSA ABLOY mobile device-based PACS perform each and every limitation recited in the claims as set forth in his affidavit," and cites to the Villasenor declaration as "reflecting the results of an investigation to confirm that HID Global and ASSA ABLOY Hospitality products practice the claims." *Id.* (citing Ex. 2002 ¶ 90, App. C, 83-85). We find that Patent Owner's evidence that its products embody the invention disclosed and claimed in the '374 Patent is relatively weak because the proffered evidence does not link explicitly any alleged success or praise to the claimed features of the mobile device.

Appendix C to the Villasenor declaration is an article from "Hospitality Upgrade" indicating that "ASSA ABLOY Hospitality . . . has announced the deployment of its ASSA ABLOY Hospitality Mobile Access, a highly advances mobile phone-based keyless entry solution developed specifically for the global market." Ex. 2002, App. C. The article does not

mention the ’374 patent specifically, nor is there any other indication that the mobile-based solution discussed therein includes the particular features claimed in the ’374 patent. Paragraphs 90 and 91 of the Villasenor declaration discuss the May 2015 Hospitality Upgrade publication, but fail to provide any further clarification about how Patent Owner’s product practices the ‘374 patent claims. Ex. 2002 ¶¶ 90–91.

We also recognize that Dr. Villasenor indicates in his declaration that he spoke with Mr. Julian Lovelock, VP Strategic Innovation for HID Global regarding the “Seos” platform used in Patent Owner’s products. *Id.* ¶ 83. Dr. Villasenor states that “[w]e discussed each of the elements of each of claims 1, 14, and 30, and Mr. Lovelock confirmed for me that the Seos solutions provided by both HID Global and by ASSA ABLOY Hospitality practice each of these claims.” *Id.* Patent Owner asserts that

> Mr. Lovelock explained that in the Seos platform, credential data is stored at a controller, and that the controller has the capability to communicate with both mobile devices and readers. Mr. Lovelock further explained that the credential data is transmitted to a mobile device, enabling that device to be used for secure access to a space such as a hotel room or a hotel gym. In addition, Mr. Lovelock explained that . . . the controller can receive a credential update (e.g., if a hotel guests extends a stay) which replaces the original credential in the controller, and that an update process is performed. The update process may occur automatically without action taken by the user of the mobile device, and includes determining a mobile device for the updated credential, transmitting to the mobile device a message containing the information about the credential replacement, and rewriting a portion of the memory in the mobile device in accordance with the updated credential. Mr. Lovelock also explained, for example, that a hotel guest who might originally have planned to check out on Wednesday might be considering extending his or her stay to Thursday. If the hotel guest makes a

> request to the hotel to extend the stay (and if it is granted), then a message reflecting an updated credential will be sent to the guest's mobile phone. If, however, that message is not received, then the credential in the mobile phone will become obsolete.

Id. ¶ 84. Dr. Villasenor, however, does not cite to any underlying technical documents that may have corroborated Mr. Lovelock's explanation about how the Seos platform operates; nor has Dr. Villasenor mapped Mr. Lovelock's explanation to specific claim elements. Also, Mr. Lovelock himself has not submitted a declaration in this proceeding.

We, thus, give Dr. Villasenor's opinion that Patent Owner's Seos platform practices the claims little weight. *See In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1368 (Fed. Cir. 2004) ("[T]he Board is entitled to weigh the declarations and conclude that the lack of factual corroboration warrants discounting the opinions expressed in the declarations."); *see also* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight."). Further, we recognize that Dr. Villasenor's testimony is the only evidence of record on this issue, as Petitioners have not submitted a rebuttal declaration attesting that Patent Owner's products do not practice the claims.

b. Industry Praise

Patent Owner contends that "ASSA ABLOY PACS—and in particular, those that practice the independent claims—have received an exceptional amount of industry praise." PO Resp. 53. As support, Patent Owner points to its own press releases as well as other industry reviews or articles allegedly "demonstrate[ing] that those in the industry focused their

praise on ASSA ABLOY's mobile device-based PACS, the subject of independent claims 1, 14, and 30." *Id.*

Industry praise for an invention may provide evidence of non-obviousness where the industry praise is linked to the claimed invention. *See Geo. M. Martin Co. v. Alliance Mach. Sys. Int'l LLC*, 618 F.3d 1294, 1305 (Fed. Cir. 2010); *Asyst Techs., Inc. v. Emtrak, Inc.*, 544 F.3d 1310, 1316 (Fed. Cir. 2008); *see also Vulcan Eng'g Co., Inc. v. Fata Aluminum, Inc.*, 278 F.3d 1366, 1373 (Fed. Cir. 2002) ("Appreciation by contemporaries skilled in the field of the invention is a useful indicator of whether the invention would have been obvious to such persons at the time it was made.").

As noted above, however, we find that Patent Owner's evidence that its PACS products practice the claims of the '374 patent is relatively weak. Moreover, we do not find that any industry praise relied upon by Patent Owner focused specifically on the claimed features of the '374 patent, such as those related to a "credential update," which Patent Owner relies upon to distinguish its claimed method and system from the prior art. For example, Patent Owner and Dr. Villasenor point to one article stating that "[t]he convenient mobile-phone-based solution allows them to use their own smart device as a room key and go directly to their assigned room, eliminating the need to wait in line at the front desk for check-in or check-out." PO Resp. 53 (citing Ex. 2002 ¶¶ 92–93, App. D). Patent Owner also points to a Hospitality Upgrade publication from November 2015 indicating that a German hotel chain selected ASSA ABLOY Hospitality's Mobile Access product, and which states that "[c]onvenience aside, Mobile Access also provides some of the latest security safeguards that are available to hotels

today . . . The smartphone places the key in a secure key vault within the hotel's mobile app." *Id.* (citing Ex. 2002 ¶¶ 94–95, App. E). Patent Owner further points to another hospitality industry publication indicating that the Starwood Preferred Guest (SPG) Keyless system, which utilizes Patent Owner's platform, won the 2015 Hospitality Award. *Id.* (citing Ex. 2002 ¶¶ 109–110).

In general, these articles, as well as Patent Owner's press releases (*e.g.*, Ex. 2002 ¶¶ 104–105), highlight the security and convenience associated with using a mobile phone to unlock hotel rooms. Patent Owner, however, fails to explain how or why the additional security or convenience is related specifically to the invention claimed in the '374 patent as opposed to what was previously known in the prior art. *Cf. Bayer Healthcare Pharm., Inc. v. Watson Pharm., Inc.*, 713 F.3d 1369, 1377 (Fed. Cir. 2013) ("Such bare journal citations and self-referential commendation fall well short of demonstrating true industry praise. Furthermore, industry praise of what was clearly rendered obvious by published references is not a persuasive secondary consideration."). As such, Patent Owner has not established a sufficient nexus between the merits of the challenged claims and the alleged industry praise.

Accordingly, we determine that Patent Owner's evidence of industry praise does not support a conclusion of non-obviousness.

c. Commercial Success

Patent Owner further contends that the commercial success of its mobile-based PACS products supports the non-obviousness of the challenged claims. PO Resp. 54–57.

"Commercial success is relevant because the law presumes an idea would successfully have been brought to market sooner, in response to market forces, had the idea been obvious to persons skilled in the art." *Merck & Co. v. Teva Pharm. USA, Inc.*, 395 F.3d 1364, 1376 (Fed. Cir. 2005). "Thus, the law deems evidence of (1) commercial success, and (2) some causal relation or 'nexus' between an invention and commercial success of a product embodying that invention, probative of whether an invention was non-obvious." *Id.*

As the basis for its alleged commercial success, Patent Owner asserts that "from the introduction of their mobile device-based PACS into a nonexistent market over two years ago, ASSA ABLOY has sold over 100,000 units," and relies upon an "interim report showing 30,000 readers shipped in just over a year." PO Resp. 55 (citing Ex. 2002 ¶¶ 83–89, App. C). Patent Owner further asserts that [t]his considerable sales volume in a nascent industry initially pioneered by ASSA ABLOY itself shows undeniable commercial success." *Id.* (citing Ex. 2002 ¶¶ 106–108, App. K). Patent Owner, however, has not offered any evidence indicating that the reported sales volume would be considered commercially successful in the context of the industry as a whole. Patent Owner also has not identified any evidence indicating how the alleged sales volume would translate into a dollar amount. As such, we find the number of units sold by Patent Owner to have little probative weight in assessing commercial success. *See J.T. Eaton & Co. v. Atl. Paste & Glue Co.*, 106 F.3d 1563, 1571 (Fed. Cir. 1997) ("When a patentee can demonstrate commercial success, usually shown by *significant sales in a relevant market*, and that the successful product is the invention disclosed and claimed in the patent, it is presumed that the

commercial success is due to the patented invention.") (emphasis added); *In re Baxter Travenol Labs.*, 952 F.2d 388, 392 (Fed. Cir. 1991) (holding that "information solely on numbers of units sold is insufficient to establish commercial success" where "[n]o market share information was provided beyond saying that [the products] were 'significantly favored' by users").

Moreover, even if the alleged sales volume were deemed significant, we determine that a sufficient nexus has not been established between any commercial success for Patent Owner's PACS products and the claimed invention. As recognized by Patent Owner, the Federal Circuit has stated, "[a] prima facie case of nexus is generally made out when the patentee shows both that there is commercial success, and that the thing (product or method) that is commercially successful is the invention disclosed and claimed in the patent." *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988); PO Resp. 54. As discussed above, however, we find that the conclusory testimony of Dr. Villasenor does not sufficiently show that the allegedly commercially successful products practice the claims.

We are not persuaded by Patent Owner's argument that the sales of Patent Owner's products were necessarily driven by the claimed features as opposed to other factors. Patent Owner asserts that a nexus exists based on the fact that a) "numerous industry participants have published reviews touting and praising the claimed features;" and b) "ASSA ABLOY's public engagements have focused on highlighting the claimed features to potential customers." PO Resp. 56. As noted above, the industry praise relied upon by Patent Owner only highlighted the security and convenience associated generally with the use of mobile phones to unlock hotel rooms as opposed to

the specific credential updating mechanism claimed in the '374 patent. The proffered advertisements do not specifically highlight or extoll the claimed credential updating mechanism within the mobile-based PACS products. *See* Ex. 2002 ¶¶ 86–88, 102–104, Apps. A, H, and I. For example, Patent Owner points out that it highlighted the fact that its product offers a "seamless self-service check-in/check-out experience," and "today's travelers are able to bypass front desk queues entirely and instead go directly to their rooms to begin enjoying their hotel experience immediately. PO Resp. 56 (citing Ex. 2002, App. A). However, that feature would be a benefit associated with *any* mobile-based keyless entry system, including those described by the Nielsen and Karkas references.

Thus, any presumption concerning the commercial success of Patent Owner's products is, at best, weak. To the extent that a presumption exists, we find that it has been rebutted. Petitioners point out that Patent Owner was the "the world's leading manufacturer and supplier of locking solutions" before the '374 Patent was filed, and thus "could simply leverage its existing market power to sell more locks." Reply 24 (citing Ex. 1008 (Patent Owner's 2004 Annual Report), ii). *Cf. Geo. M. Martin Co.*, 618 F.3d at 1304 (holding that patent challenger "conclusively established that much of [patent owner's] commercial success was due to [patent owner's] pre-existing market share."); *Ruiz v. A.B. Chance Co.*, 357 F.3d 1270, 1277 (Fed. Cir. 2004) (affirming a finding that commercial success was attributable not to the asserted patent but to the patentee's "experience with screw anchors combined with being the first large screw anchor manufacturer to enter the [relevant] market"). We, therefore, are persuaded

by Petitioners' argument that Patent Owner's sales were likely due to other factors.

Accordingly, we determine that Patent Owner's evidence of commercial success does not support a conclusion of non-obviousness.

4. Summary

For the foregoing reasons, we are persuaded that Petitioners have shown, by a preponderance of the evidence, that claims 1, 3, 5, 9–16, 22, 23, 26, 29, and 30 of the '374 patent are obvious based on Nielsen. We are not persuaded, however, that Petitioners have shown, by a preponderance of the evidence, that claims 7 and 21 are obvious based on Nielsen and Karkas.

III. PATENT OWNER'S MOTION TO EXCLUDE

Patent Owner filed a Motion to Exclude certain evidence. Paper 24 ("Mot. to Exclude"). Specifically, Patent Owner seeks to exclude portions of Dr. Villasenor's cross-examination testimony, Exhibit 1007, and Patent Owner's 2004 Annual Report, Exhibit 2008. Petitioners filed an Opposition to the Motion to Exclude (Paper 28), to which Patent Owner filed a Reply (Paper 31).

Because we do not rely upon any of the cited portions of Dr. Villasenor's testimony in reaching our decision, we dismiss Patent Owner's Motion to Exclude as moot with respect to Exhibit 1007.

We do rely upon Petitioners' arguments made with respect to Exhibit 1008 in reaching our conclusion regarding commercial success. Patent Owner seeks to exclude Exhibit 1008 under Federal Rules of Evidence 402 and 403 on the basis that "[t]he quoted passage from the 2004 ASSA ABLOY Annual Report and the Annual Report itself also confuses the issue of commercial success because such evidence does not address the nexus

between the commercial success of the Seos product and the claims of the '374 patent." Mot. to Exclude 8. Patent Owner argues that "the quoted passage is not relevant because it is removed by 10 years from the commercial success events Dr. Villasenor addressed," and "bears no relationship to, and does not serve to prove, disprove or rebut the nexus between the commercial success of the Seos product in the hospitality or enterprise industries and the claimed credential updating features embodied in the Seos system." *Id.* at 9. We disagree. As discussed above, we find that the quoted passage of the Annual Report statement is evidence of Patent Owner's pre-existing market share, and, thus, relevant to the issue of whether the alleged commercial success has a nexus to the claimed invention. We have taken into account the fact that the 2004 Annual Report is from over 10 years ago, and do not find that it will cause any confusion. To the contrary, the 2004 Annual Report is more probative to the issue of pre-existing market share than more recent reports insofar as the '374 patent claims an effective filing date based on a provisional application filed in April 2005. Ex. 1001, Title Page.

Accordingly, we determine that Exhibit 1008 is admissible evidence under Rules 402 and 403, and we deny Patent Owner's Motion to Exclude as to that exhibit.

IV. CONCLUSION

We conclude that Petitioners have demonstrated by a preponderance of the evidence that claims 1, 3, 5, 9–16, 22, 23, 26, 29, and 30 of the '374 patent are unpatentable based on Nielsen.

We conclude that Petitioners have not demonstrated the unpatentability of claims 7 and 21 by a preponderance of the evidence.

We deny Patent Owner's Motion to Exclude with respect to Exhibit 1008, and dismiss that Motion as moot with respect to Exhibit 1007.

V. ORDER

Accordingly, it is:

ORDERED that claims 1, 3, 5, 9–16, 22, 23, 26, 29, and 30 of U.S. Patent 8,150,374 B2 are held to be unpatentable;

FURTHER ORDERED that claims 7 and 21 of U.S. Patent 8,150,374 B2 have not been shown to be unpatentable;

FURTHER ORDERED that Patent Owner's Motion to Exclude is *dismissed-in part* and *denied-in-part*; and

FURTHER ORDERED that because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

FOR PETITIONER SPECTRUM:

Michelle Armond
John Sganga
Brenton Babcock
KNOBBE, MARTENS, OLSON & BEAR, LLP
2mea@knobbe.com
2jbs@knobbe.com
2brb@knobbe.com

FOR PETITIONER UNIKEY:

Steven Bauer
Joseph Capraro Jr.
Gerald Worth
Micah Miller
PROSKAUER ROSE LLP
PTABMattersBoston@proskauer.com
jcapraro@proskauer.com
gworth@proskauer.com
mmiller@proskauer.com

FOR PATENT OWNER:

W. Karl Renner
Thomas Rozylowicz
Christopher Marchese
Gregory Walters
FISH & RICHARDSON P.C.
IPR42746-0011IP1@fr.com
IPR42746-0002IP1@fr.com
PTABInbound@fr.com

Benjamin Deming
RUTAN & TUCKER, LLP
bdeming@rutan.com