

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SPECTRUM BRANDS, INC.,
Petitioner,

v.

ASSA ABLOY AB,
Patent Owner.

Case IPR2015-01563
Patent 7,706,778

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

BUNTING, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

Spectrum Brands, Inc. (“Petitioner”) filed a Petition requesting *inter partes* review of claims 1, 4, 6, 8, 10–14, 16–18, 22–25, 28–31, 33, and 34 (the “challenged claims”) of U.S. Patent No. 7,706,778 (Exhibit 1001, “the ’778 patent”) pursuant to 35 U.S.C. §§ 311–319. Paper 1 (“Pet.”). Patent Owner, Assa Abloy AB. (“Patent Owner”) waived filing of a Preliminary Response to the Petition. Paper 6. We have jurisdiction under 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted “unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.”

Upon consideration of the information presented in the Petition, and for the reasons explained below, we determine that Petitioner has not established a reasonable likelihood that the challenged claims are unpatentable. Accordingly, we decline to institute an *inter partes* review of the challenged claims of the ’778 patent.

II. BACKGROUND

A. *Related Matters*

The parties indicate that the ’778 patent is the subject of the following district court action: *HID Global Corporation et al. v. Kwikset Corporation et al.*, No. 14-cv-00947-CJC-DFM (C.D. Cal.). Pet. 5, Paper 5, 2. Petitioner filed an additional petition requesting *inter partes* review of the following related patent: U.S. Patent No. 8,150,374 (IPR2015-01562).¹ *Id.*

¹ IPR2015-01440 and IPR2015-01441 involving the ’778 patent and U.S. Patent No. 8,150,374, respectively, were both terminated pursuant to a settlement agreement.

B. The '778 Patent (Ex. 1001)

The '778 patent is directed to the use of mobile devices in an access control system to control “access to assets, places, or things by having access credentials remotely assigned and revoked.” Ex. 1001, 1:20–21. As shown in Figure 1, reproduced below, the system 100 automatically and remotely updates credential information associated with the mobile device.

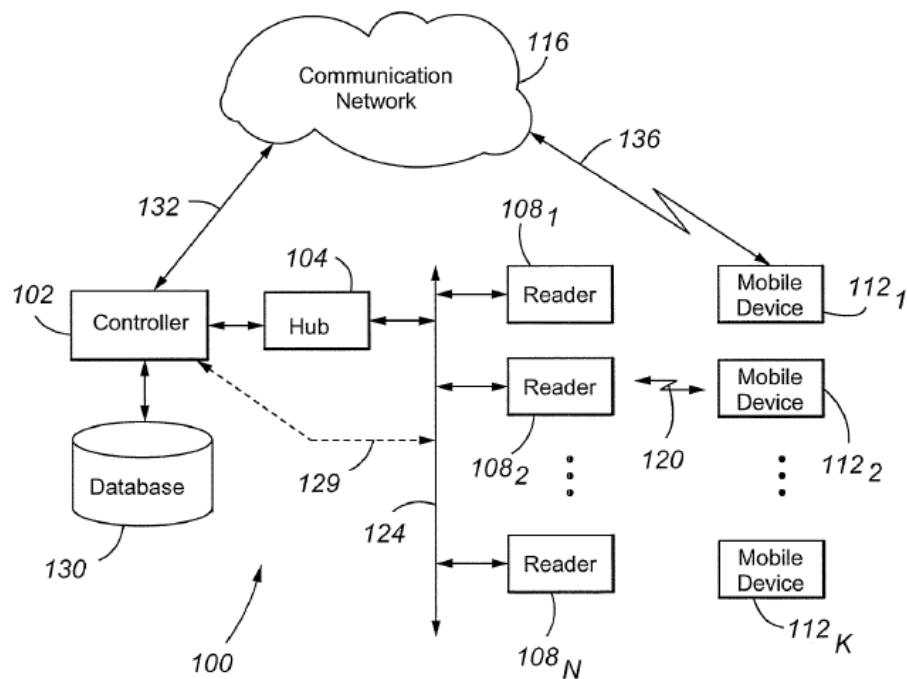


Fig. 1

Figure 1 is a diagrammatic view of a system for authenticating mobile devices and remotely updating associated credentials. *Id.* at 4:40–42.

System 100 includes controller 102 coupled to a plurality of readers 108 via interconnecting hub 104. *Id.* at 4:66–5:1. The controller also communicates with at least one of the plurality of mobile devices 112 via communication network 116. *Id.* at 6:61–63. The reader is associated with a particular asset, and “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 6:9–13.

The mobile device contains a memory 200 that “may be selectively modified and/or erased by the controller 102 and/or the reader 108.” *Id.* at 8:1–3. Identification information, including “credential information of the user of the mobile device 112, for instance, unique IDs, manufacture IDs, passwords, keys, encryption schemes, transmission protocols, and the like” is loaded into the mobile device memory. *Id.* at 8:9–12. The mobile device memory also includes self-authenticating data, e.g., “assets the mobile device **112** has access to, times of allowed access to each asset, and other data that can assist the mobile device in determining if it is eligible to gain access to a particular asset” (*Id.* at 8:22–25) and self-authenticating functions, e.g., “us[ing] the self-authenticating data to enable the mobile device **112** to make a determination of its own access rights with respect to an asset” (*Id.* at 8:25–28).

Upon presentation of the mobile device to the reader, the reader provides asset information and time of day information to the mobile device. *Id.* at 8:35–38. The mobile device analyzes the asset information and time of day information using its self-authenticating data to determine whether it is allowed to access the asset. *Id.* at 8:38–41. If the mobile device determines that it is allowed access to the asset (*Id.* at 8:44–45), it sends a signal to the reader “indicating that validation of the mobile device 112 has been confirmed and access should be granted” so that the reader allows access to the asset. *Id.* at 8:46–47.

The ’778 patent further describes in Figure 3 a method for automatically and remotely updating credential information on the mobile

device. *Id.* at 9:36–39; Fig. 3. For example, if credential information used by a mobile device to verify its authenticity is changed at the controller, the memory of the mobile device is likewise updated. *Id.* at 9:40–10:6. In another embodiment of a method for automatically and remotely updating credential information on the mobile device, described in Figure 4, a time interval between credential updates is determined. *Id.* at 10:7–23. New credential information is sent to the readers and the mobile devices periodically to keep self-authenticating data and/or functions active and up to date. *Id.* at 10:51–54.

C. Illustrative Claim

Of the challenged claims, claims 1, 16 and 33 of the '778 patent are independent. Claim 1 is illustrative of the challenged claims and is reproduced below:

1. A method of remotely maintaining a secure access system, comprising:
receiving, at a secure access system controller, a credential update for at least one user of the secure access system;
in response to receiving the credential update, said controller automatically initiating a system update process, the system update process comprising:
generating a message comprising information representing the credential update;
determining at least one target for said message, wherein said at least one target comprises at least one mobile device associated with the at least one user; and

transmitting said message to said at least one target;
and

wherein said at least one mobile device has a first set of credential data stored thereon, wherein upon receiving said message from said controller, said first set of credential data is changed to a second different set of credential data, wherein said message is transmitted to said at least one mobile device without receiving a request for said message from said at least one user, wherein said at least one mobile device is a smart mobile device, wherein said first set of credential data comprises self-authenticating data, wherein said second set of credential data comprises different self-authenticating data, and wherein said self-authenticating data enables said at least one mobile device to make a determination of its own access rights with respect to an asset.

Ex. 1001, 12:34–12:60.

D. Evidence Relied Upon

Petitioner relies on the following prior art references (Pet. 9–10):

Reference	Patent/Printed Publication	Date	Exhibit
Nielsen	U.S. Patent Application Publication No. 2002/0180582	Dec. 5, 2002	1002
Karkas et al. ("Karkas")	U.S. Patent Application Publication No. 2002/0031228	March 14, 2002	1003

E. Asserted Grounds of Unpatentability

Petitioner challenges claims 1, 4, 6, 8, 10–14, 16–18, 22–25, 28–31, 33, and 34 of the '778 patent based on the asserted grounds of

unpatentability set forth in the table below. Pet. 10. In support of the grounds of unpatentability referenced below, Petitioner relies on the Declaration of Dr. Mathew Green. Ex. 1004.

Reference	Basis	Claims Challenged
Nielsen and Karkas	§ 103	1, 4, 6, 8, 10–14, 16–18, 22–25, 28–31, 33, and 34
Nielsen, knowledge of a person of ordinary skill in the art	§ 103	1, 4, 6, 8, 10–14, 16–18, 22–25, 28–31, 33, and 34

III. ANALYSIS

A. Claim Interpretation

As a step in our analysis for determining whether to institute a review, we determine the meaning of the claims for purposes of this decision. In an *inter partes* review, claim terms in an unexpired patent are given their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *see also In re Cuozzo Speed Tech., LLC*, 793 F.3d 1268, 1278–79 (Fed. Cir. 2015) (“Congress implicitly approved the broadest reasonable interpretation standard in enacting the [America Invents Act],” and “the standard was properly adopted by PTO regulation”). Under the broadest reasonable interpretation standard, and absent any special definitions, claims terms are given 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). Any special definitions for claim terms or

phrases must be set forth with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). In the absence of such a definition, limitations are not to be read from the specification into the claims. *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993).

Petitioner proposes that we adopt claim constructions espoused by Patent Owner in other proceedings. Pet. 16–21. For purposes of this decision, we address below the construction of the claim term “self-authenticating data.” This term appears in each independent challenged claim, claims 1, 16, and 33.

According to Petitioner, “self-authenticating data” should be construed as “data that can assist the mobile device in determining if it is eligible to gain access to a particular asset.” *Id.* at 17 (citing Ex. 1006, A16). To support this construction, Petitioner directs our attention to the following portion of the specification describing examples of self-authenticating data as:

assets the mobile device 112 has access to, times of allowed access to each asset, and other data that can *assist the mobile device in determining if it is eligible to gain access to a particular asset.*

Id. (citing Ex. 1001, 8:21–28; Ex. 1006, A17) (emphasis added). Thus, Petitioner argues that the self-authenticating data “allows the mobile device to make some determination of eligibility on its own” Pet. 18.

We must first consider the term “self-authenticating data” in the context of the entire claim. For example, claim 1 recites:

wherein said first set of credential data comprises self-authenticating data, wherein said second set of credential data comprises different self-authenticating data, and *wherein said*

self-authenticating data enables said at least one mobile device to make a determination of its own access rights with respect to an asset.

Ex. 1001, 12:55–60 (emphasis added). As Petitioner recognizes, the “self-authenticating data” assists the mobile device in determining if it is eligible to gain access to a particular asset. *Id.* at 8:24–25. The Specification further describes how “[t]he self-authenticating functions use the self-authenticating data to *enable []mobile device 112 to make a determination of its own access right* with respect to an asset.” *Id.* at 8:25–28 (emphasis added). The Specification clarifies, for example, that the mobile device analyzes the asset information and time of day information provided by reader 108 using its self-authenticating data, and then the mobile device determines whether it is allowed access to the asset. *Id.* at 8:35–44. If the mobile device determines that it is allowed access, “it sends a signal back to the reader indicating that validation of the mobile device 112 has been confirmed and access should be granted.” *Id.* at 8:44–48. Our understanding that the mobile device uses the self-authenticating data in determining its own access rights with respect to an asset, is further confirmed by Patent Owner’s statement from the file history. During prosecution, the Patent Owner stated that the self-authenticating data “enables the mobile device to make a determination of its own access rights with respect to an asset” Ex. 1006, A18 (citing Ex. 1005, 36).

Upon considering the claim language and Specification, we determine that the broadest reasonable construction of “self-authenticating data” is “data that can assist the mobile device in determining if it is eligible to gain access to a particular asset.”

Having considered Petitioner's contentions in view of the Specification, and for purposes of this decision, we determine that no other claim terms require express construction. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) ("only those terms that are in controversy need be construed, and only to the extent necessary to resolve the controversy").

B. Obviousness based on Nielsen and Karkas

We now turn to Petitioner's asserted grounds of unpatentability. Petitioner contends claims 1, 4, 6, 8, 10–14, 16–18, 22–25, 28–31, 33, and 34 are unpatentable under 35 U.S.C. § 103 as having been obvious based on Nielsen and Karkas. Pet. 26–55.

Having considered the explanations and supporting evidence presented, we are not persuaded that, based on the record before us, Petitioner presents sufficient evidence to demonstrate a reasonable likelihood that it would prevail with respect to its contention that challenged claims 1, 4, 6, 8, 10–14, 16–18, 22–25, 28–31, 33, and 34 would have been obvious over Nielsen and Karkas. A detailed analysis of our determination follows after a brief overview of Nielsen and Karkas.

1. Overview of Nielsen (Ex. 1002)

Nielsen discloses an access control system for controlling access to a location and a method of managing a predetermined access right to the location. Ex. 1002 ¶ 1. Figure 2b, reproduced below, illustrates one embodiment of a lock control system.

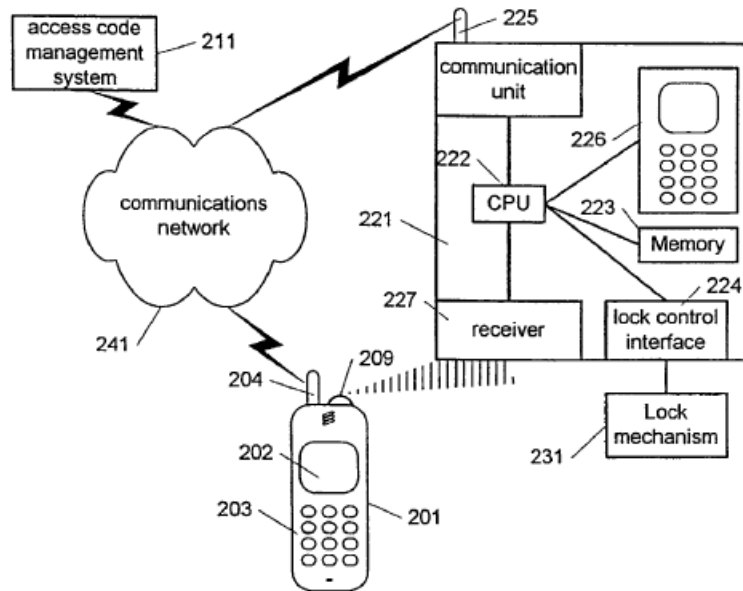


Fig. 2b

Figure 2b illustrates a block diagram of a system for controlling access to a location. *Id.* ¶ 105.

The lock control system includes an electronic key device 201, e.g., a mobile phone, equipped to communicate with both lock control unit 221 and access code management system 211. *Id.* ¶¶ 125, 127. The access code management system also is in communication with the lock control unit. *Id.* ¶ 128. Nielsen further describes how the access code management system generates and administers access codes, and transmits these access codes to the electronic key device and/or lock control unit upon request from a user, automatically, or periodically. *Id.* Similarly, the access code management system may “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.* Nielsen further teaches that,

When 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.

As described with respect to Figure 3, the process of managing access rights includes the steps of generating access codes and storing the generated access codes in a database associated with the access code management system (*Id.* ¶ 132), and transferring the access codes from the access management system to the lock control unit and electronic key device (*Id.* ¶ 133). Nielsen further discloses that the electronic key device includes a memory 507, and that the received access codes are stored in the memory. *Id.* ¶¶ 151–152. As described in Figure 5a, upon request from the user, the access code is retrieved from the memory of the electronic key device and displayed on an associated display 520. *Id.* ¶ 153. The user issues a command for initiating use of the selected access code, and the selected access code is transmitted to the lock control unit or alternatively, the access code management system. *Id.* ¶ 154. Alternatively, the access code is transmitted via a data or telephone communications channel. *Id.* ¶ 163. As described further with respect to Figure 6a, the lock control unit verifies the access code received from the electronic key device with access codes stored in its memory, and “[i]f the received access code corresponds to one of the valid stored access codes, the lock mechanism is operated” to grant access to the location. *Id.* ¶162.

2. Overview of Karkas (Ex. 1003)

Karkas discloses an access device for receiving a key and validity information, establishing a connection with another party, and providing the

key and validity information to that party. Ex. 1003, Abstract. “If the key and validity information are determined by the other party to be valid[,] access is provided.” *Id.* As shown in Figure 3, mobile station 8 is in communication with Bluetooth device 24, which may be “a lock or an access device.” *Id.* ¶¶ 24, 25. The mobile station may also be in communication with base transceiver station 6. *Id.* ¶ 30. Karkas describes the mobile station as having a processor 14, memory 18, display 16, first antenna 10 and second antenna 20. *Id.* ¶¶ 17–21, Figure 2.

Karkas further discloses a method that includes the steps of establishing a connection between the mobile station and the network via the base receiver station, wherein server 40 provides the mobile station with key information and additional information (*Id.* ¶¶ 31, 32); the mobile station establishes a connection with the Bluetooth device and sends the key to the Bluetooth device (*Id.* ¶¶ 35–36); the Bluetooth device checks the validity of the key by decrypting and comparing the key to information stored on the Bluetooth device, and provides access if the key is valid (*Id.* ¶¶ 37–38). The key may have an identification tag which identifies the service provider (*Id.* ¶ 39), or a time limit (*Id.* ¶ 41). Karkas further discloses that “[t]he validity time for the key can be in the non-encrypted part of the key so that the mobile station can remove it automatically.” (*Id.* ¶ 49) Alternatively, Karkas discloses that the validity time for the key may be encrypted, so that “the mobile station can automatically delete those keys which are out of date.” *Id.* ¶ 53.

3. Discussion

A claim is unpatentable under § 103(a) if “the differences between the [claimed] subject matter . . . and the prior art are such that the subject

matter[,] as a whole[,] would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, so-called secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Against this backdrop, we analyze this asserted ground based on obviousness, with the principles identified above in mind.

It is Petitioner’s obligation to explain clearly the arguments and evidence upon which it relies for each limitation of a claim challenged in a petition. See 37 C.F.R. § 42.22(a)(2) (the petition must include “[a] full statement of the reasons for the relief requested, including a detailed explanation of the significance of the evidence” (emphasis added)). See also 37 C.F.R. § 42.104 (b)(4). Petitioner asserts broadly that Nielsen discloses “nearly all of the limitations of the Challenged Claims of the ’788 patent” and relies on Karkas for the missing limitations. Pet. 27 (citing Ex. 1004 ¶ 54). To demonstrate which teachings in Nielsen and Karkas satisfy the limitations of the claims, the Petitioner includes a claim chart identifying quotations in the reference that it alleges correspond with claim elements. *Id.* at 31–55.

a. “Self-authenticating Data”

Petitioner argues that the combination of Nielsen and Karkas teaches the “self-authenticating data” claim term recited in claims 1, 16 and 33. *Id.* at 28–29. “Self-authenticating data,” according to Petitioner, includes

expiration times associated with credentials “because these expiration times allow a mobile device to determine that it is no longer eligible to gain access to a particular asset.” *Id.* at 28.

Acknowledging that Nielsen discloses access codes that automatically expire, but does not disclose that the mobile device itself performs the expiration analysis, Petitioner argues that “Karkas discloses ‘self-authenticating data’ and expressly states that is used on a mobile device.” *Id.* (citing Ex. 1004 ¶¶ 37–39, 57). To support this argument, Petitioner first directs us to the disclosure in Karkas regarding the use of keys “that have a time limit beyond which it is not valid” (*Id.* (citing Ex. 1003 ¶ 41)) and that “if the key is no longer valid, the mobile device in Karkas automatically removes it” (*Id.* (citing Ex. 1003 ¶ 49, 53). Relying on the testimony of Dr. Green, Petitioner concludes that the expiration data for the key “assists the mobile device in determining whether it has access to an asset” (*Id.* (citing Ex. 1004 ¶ 58)) because “[i]f the key has expired, the mobile device in Karkas independently recognizes that the key no longer provides access to an asset, and removes it from the device” (*Id.* (citing Ex. 1004 ¶ 57).

As noted above, we adopt Petitioner’s construction of “self-authenticating data” as “data that can assist the mobile device in determining if it is eligible to gain access to a particular asset.” We are not persuaded Petitioner’s arguments and evidence demonstrate sufficiently that Karkas discloses that the “self-authenticating data” enables the mobile device in making a determination of its own access rights with respect to the asset. Dr. Green’s testifies that this limitation is met by the description in Karkas concerning the automatic removal of expired keys by “encrypting certain elements of the access code, but not encrypting other elements” (Ex. 1004 ¶

57 (citing Ex. 1003 ¶ 49)). Dr. Green opines that “[s]uch expiration data for a key assists the mobile device in determining whether it has access to an asset, and Karkas’ teachings on expiration data therefore disclose ‘self-authenticating data.’” Ex. 1004 ¶ 58.

To the extent Petitioner and Dr. Green argue that a time limit embedded in a key represents data, we agree. Nonetheless, neither Petitioner nor Dr. Green explain sufficiently how the automatic removal of the key from the memory of the mobile device is data that enables the mobile device “to make a determination of *its own access rights* with respect to an asset.” (emphasis added). Petitioner and Dr. Green do not direct us to sufficient disclosure in Karkas regarding the mobile phone itself using the expired key or erased key to determine its own access rights with respect to an asset. For example, Petitioner and Dr. Green have not identified any description in Karkas that, after automatically removing an expired key (Ex. 1003 ¶ 53), the mobile phone itself would somehow know that it no longer has access rights to a particular asset. To the contrary, our review of Karkas reveals that the Bluetooth device is used to determine such access rights. *See e.g.*, Ex. 1003 ¶¶ 36–38:

Once the Bluetooth connection has been established, in step S4 the mobile station sends the key information to the Bluetooth device...*In step S5, the Bluetooth device will check the validity of the key.* In particular, the Bluetooth device attempts to decrypt the keys and will compare it with key information which it has stored thereon. In step S6, if the key is valid, then the Bluetooth device 24 will provide access (emphasis added).

Based on the current record, we are not persuaded by Petitioner that Karkas’ automatic removal of the expired key from the mobile device is “self-authenticating data,” as we have construed this term, that “enables at

least one mobile device to make a determination of its own access rights with respect to an asset.”

b. “Smart Mobile Device”

Next, we consider Petitioner’s argument that the combination of Nielsen and Karkas teaches the limitation in claims 1 and 16 requiring a “smart mobile device.” Pet. 29. Petitioner asserts that a “smart mobile device may be construed to mean ‘a mobile device that determines its own access rights and permissions.’” *Id.* at 21 (citing Ex. 1004 ¶¶ 24–25). Petitioner further acknowledges that “it is not explicit [in Nielsen] that the mobile phone may determine its own access rights and permissions.” *Id.* at 29 (citing Ex. 1004 ¶ 62). According to Petitioner, Karkas teaches mobile phones that use keys and act as “smart mobile devices” because the mobile phone “deletes keys when it determines the associated access rights and permissions are no longer valid.” *Id.* (citing Ex. 1004 ¶ 58). As discussed *supra*, however, neither Petitioner nor Dr. Green provide persuasive analysis that supports Petitioner’s conclusion that Karkas describes a mobile phone using the expired key or erased key to determine its own access rights and permissions with respect to an asset.

c. Remaining Dependent Claims

Petitioner’s analysis of the dependent claims do not cure the deficiency discussed above. Therefore, for the same reasons as discussed *supra* with respect to claims 1, 16, and 33, our determination concerning the insufficiency of Petitioner’s evidence applies equally to dependent claims 4, 6, 8, 10–14, 17–18, 22–25, 28–31, and 34.

d. Combination of Nielsen and Karkas

We also deny institution of the asserted grounds for the additional, independent reason that Petitioner has failed to articulate a sufficient rationale to combine the teachings of Nielsen and Karkas to arrive at the claimed invention. As to each of the challenged claims, Petitioner asserts that “it would have been obvious for skilled artisans to combine Nielsen with Karkas.” Pet. 26. Relying on the testimony of Dr. Green, Petitioner reasons that “both references were published in the same year, and both disclose analogous access control systems” (*Id.* (citing Ex. 1004 ¶ 48), and that “[b]oth references describe using mobile devices as keys, electronic locks, and a central management system” (*Id.* citing Ex. 1004 ¶¶ 34–37). For example, Petitioner notes that Nielsen discloses electronic key devices, lock control units and a central access code management system; Karkas discloses mobile stations, Bluetooth devices and a central control element; and both Nielsen and Karkas disclose mobile phones with embedded electronic access codes and similar wireless communication protocols. *Id.* at 27 (citing Ex. 1002 ¶¶ 1, 128; Ex. 1003 ¶¶ 24, 45, 49; Ex. 1004 ¶¶ 28, 35, 37, and 48). Thus, Petitioner concludes “[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.* (citing Ex. 1004 ¶ 50).

Petitioner does not provide sufficient articulated reasoning with rational underpinning explaining why one with ordinary skill in the art would modify the teachings of the applied references to address the noted differences. *See KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)) (“[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.”)). Petitioner’s observation that both references were published in the same year and are from the same field of endeavor falls short of an adequate rationale. The same field of endeavor analysis is merely the jumping-off point in the determination of whether a claimed invention is obvious. *See K-TEC, Inc. v. Vita-Mix Corp.*, 696 F.3d 1364, 1375 (Fed. Cir. 2012) (to qualify as prior art in an obviousness analysis, references must be analogous art—either from the same field of endeavor, or reasonably pertinent to the problem with which the inventor is involved). 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.

Here, Petitioner’s arguments do not provide the required articulated reasoning with rational underpinning, based on the evidence, to support the legal conclusion of obviousness. Petitioner’s conclusory argument regarding the general feasibility of incorporating the features of Karkas into Nielsen do not explain adequately how or why a person of ordinary skill in the art would attempt to improve Nielsen by looking to Karkas. Thus, having considered Petitioner’s arguments, we are not persuaded Petitioner has provided an articulated reasoning with rational underpinning sufficient to support the legal conclusion of obviousness.

4. Summary

Having considered fully the parties’ arguments and evidence, on the current record, Petitioner does not demonstrate a reasonable likelihood that it would prevail as to its contention that claims 1, 4, 6, 8, 10–14, 16–18, 22–

25, 28–31, 33, and 34 would have been obvious over the combination of Nielsen and Karkas. Accordingly, we do not institute an inter partes review of claims 1, 4, 6, 8, 10–14, 16–18, 22–25, 28–31, 33, and 34 as obvious over Nielsen and Karkas.

C. Obviousness Ground Based on Nielsen and the Knowledge of a Person of Ordinary Skill in the Art

Petitioner also challenged claims 1, 4, 6, 8, 10–14, 16–18, 22–25, 28–31, 33, and 34 as rendered obvious under 35 U.S.C. § 103(a) over Nielsen and the knowledge of a person of ordinary skill in the art (“POSITA”). Pet. 55–59.

We are not persuaded that, based on the record before us, Petitioner presents sufficient evidence to demonstrate a reasonable likelihood that it would prevail with respect to its contention that challenged claims 1, 4, 6, 8, 10–14, 16–18, 22–25, 28–31, 33, and 34 are obvious over Nielsen and the knowledge of the POSITA.

1. Discussion

Petitioner argues that Nielsen “discloses a system that is substantially similar to the secure access system disclosed in the ’778 Patent” (Pet. 55) and that the claim charts demonstrate “where almost all of the limitations of the Challenged Claims are disclosed in Nielsen” (*Id.*). As to the missing limitations, Petitioner asserts that the challenged claims are “obvious to a person of ordinary skill in the art in view of the teachings in Nielsen” (*Id.* at 56).

a. Self-Authenticating Data

With respect to the claim term “self-authenticating data” recited in claims 1, 16, and 33, Petitioner argues that Nielsen discloses access codes or

keys that automatically expire, but does not “disclose expressly that the mobile device uses the expiration data about the access code to determine whether it can access a particular asset. *Id.* (citing Ex. 1004 ¶¶ 72–74). Relying on the testimony of Dr. Green, Petitioner explains that a skilled artisan would have modified Nielsen to allow the mobile phone to remove expired access codes so that the “mobile phone would self-authenticate itself by determining those expired access codes could no longer be used to access a secure location.” *Id.* at 57 (citing Ex. 1004 ¶ 75).

Petitioner’s arguments in this regard are not persuasive. As discussed *supra*, we construe “self-authenticating data” as “data that can assist the mobile device in determining if it is eligible to gain access to a particular asset,” and the recited self-authenticating data “enables said at least one mobile device to make a determination of its own access rights with respect to an asset.” Neither Petitioner nor Dr. Green provide any persuasive analysis to support Petitioner’s contention that a skilled artisan would have modified Nielsen in the manner it suggests. Instead, Petitioner’s assertion that such modification would be advantageous “because removing expired access codes would conserve limited memory on the mobile phone and limit the number of access codes that a user would have to sift through when selecting codes to use” (*Id.* (citing Ex. 1004 ¶¶ 77–79)) seemingly supports saving memory and not authentication by the mobile phone.

Having considered Petitioner’s argument in this regard, we are not persuaded that Petitioner’s articulated reasoning has a rational underpinning and is sufficient to justify the proposed combination of Nielsen and the knowledge of the POSITA. *See Plantronics, Inc. v. Aliph, Inc.*, 724 F.3d 1343, 1354 (Fed. Cir. 2013):

Where, as here, the necessary reasoning is absent, we cannot simply assume that ‘an ordinary artisan would be awakened to modify prior art in such a way as to lead to an obviousness rejection.’ It is in such circumstances, moreover, that it is especially important to guard against the dangers of hindsight bias.” (citation omitted)

See also KSR, 550 U.S. at 421 (“A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning.”).

b. Remaining Dependent Claims

Petitioner’s analysis of the dependent claims do not cure the deficiency discussed above. Therefore, for the same reasons as discussed *supra* with respect to claims independent 1, 16, and 33, our determination concerning the insufficiency of Petitioner’s evidence applies equally to dependent claims 4, 6, 8, 10–14, 17, 18, 22–25, 28–31, and 34.

2. Summary

Having considered fully the parties’ arguments and evidence, on the current record, Petitioner does not demonstrate a reasonable likelihood that it would prevail as to its contention that claims 1, 4, 6, 8, 10–14, 16–18, 22–25, 28–31, 33, and 34 would have been obvious over the combination of Nielsen and POSITA. Accordingly, we do not institute an *inter partes* review of claims 1, 4, 6, 8, 10–14, 16–18, 22–25, 28–31, 33, and 34 as obvious over Nielsen and POSITA.

IV. CONCLUSION

For the foregoing reasons, we determine that Petitioner has not demonstrated a reasonable likelihood that at least one challenged claim is

IPR2015-01563
Patent 7,706,778

unpatentable based on the asserted grounds. We, therefore, do not institute an *inter partes* review on any of the asserted grounds as to any of the challenged claims.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that an inter partes review as to claims 1, 4, 6, 8, 10–14, 16–18, 22–25, 28–31, 33, and 34 of the '778 patent is DENIED.

IPR2015-01563
Patent 7,706,778

PETITIONER:

Michelle E. Armond

BoxSPEBRL@knobbe.com

John B. Sganga, Jr.

2jbs@knobbe.com

Brenton R. Babcock

2brb@knobbe.com

PATENT OWNER:

Benjamin Deming

bdeming@rutan.com