

2022-00024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC,
Petitioner,

v.

LIBERTY PEAK VENTURES, LLC,
Patent Owner.

IPR2022-00024
Patent 8,066,181 B2

Before KARL D. EASTHOM, DAVID C. McKONE, and
SCOTT RAEVSKY, *Administrative Patent Judges*.

McKONE, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
Dismissing Patent Owner's Motion to Exclude
35 U.S.C. § 318(a)

I. INTRODUCTION

A. Background and Summary

On October 21, 2021, Unified Patents, LLC (“Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting *inter partes* review of claims 1, 2, 4, 6, and 7 of U.S. Patent No. 8,066,181 B2 (Ex. 1001, “the ’181 patent”). On January 21, 2022, Liberty Peak Ventures, LLC (“Patent Owner”) filed a disclaimer disclaiming claims 6 and 7. Ex. 2001.

Patent Owner filed a Preliminary Response (Paper 5, “Prelim. Resp.”). With our authorization (Ex. 3001), Petitioner filed a Preliminary Reply to Patent Owner’s Preliminary Response (Paper 6, “Prelim. Reply”) and Patent Owner filed a Preliminary Sur-Reply (Paper 7, “Prelim. Sur-reply”). Pursuant to 35 U.S.C. § 314, we instituted this proceeding as to claims 1, 2, and 4. Paper 8 (“Inst. Dec.”). We declined to institute a trial on claims 6 and 7. Inst. Dec. 2 (citing 37 C.F.R. § 42.107(e) (2021) (“[n]o *inter partes* review will be instituted based on disclaimed claims.”); *Intuitive Surgical, Inc. v. Ethicon LLC*, IPR2018-01248, Paper 7 at 2 n.1, 9–10 (PTAB Feb. 7, 2019) (discussing effect of disclaimer, the Board’s governing regulations, and Federal Circuit precedent)).

Patent Owner filed a Patent Owner’s Response (Paper 11, “PO Resp.”), Petitioner filed a Reply to the Patent Owner’s Response (Paper 12, “Reply”), and Patent Owner filed a Sur-reply to the Reply (Paper 15, “Sur-reply”).

Patent Owner filed a Motion to Exclude evidence (Paper 18, “Mot. Exclude”), Petitioner filed an opposition (Paper 19), and Patent Owner filed a reply to the opposition (Paper 20).

An oral argument was held in this proceeding on January 23, 2023. Paper 23 (“Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This Decision is a final written decision under 35 U.S.C. § 318(a) as to the patentability of claims 1, 2, and 4. Based on the record before us, Petitioner has proved, by a preponderance of the evidence, that claims 1, 2, and 4 are unpatentable. Patent Owner’s Motion to Exclude is dismissed as moot.

B. Related Matters

Patent Owner has not asserted the ’181 patent in district court litigation against Petitioner. Pet. 70, 75; Paper 4, 2. Patent Owner, however, has asserted the ’181 patent in *Liberty Peak Ventures, LLC v. Citigroup Inc.*, No. 6:21-cv-00710-ADA (W.D. Tex.). Pet 75; Paper 4, 2.

C. The ’181 Patent

1. Summary

The ’181 patent describes systems and methods for securing Radio Frequency Identification (“RFID”) transactions. Ex. 1001, 1:43–48. Figure 1 of the ’181 patent is reproduced below.

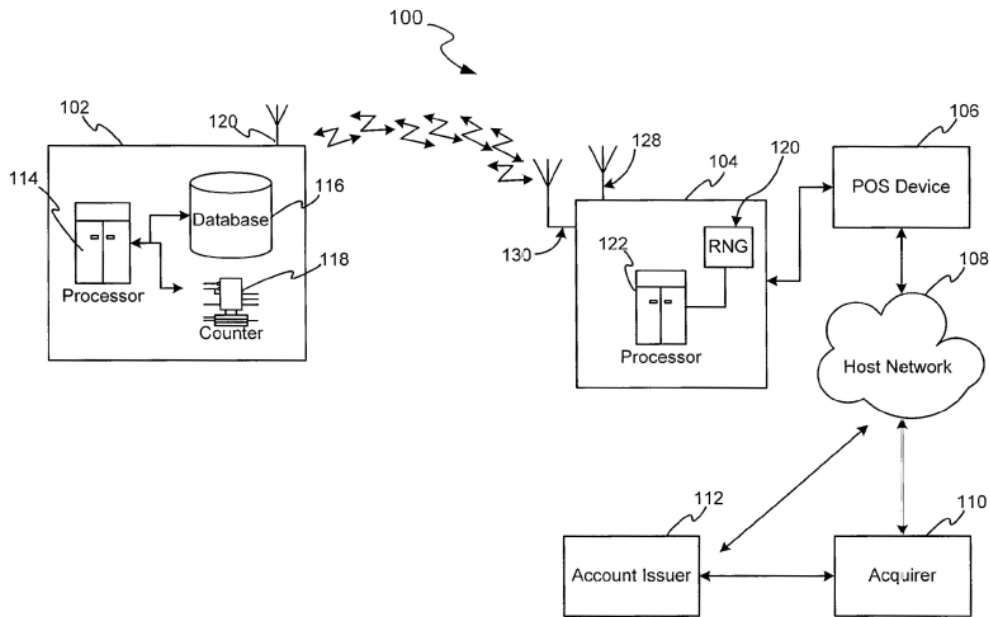


FIGURE 1

Figure 1 is a block diagram of the components of an RFID system used to complete RFID transactions. *Id.* at 3:56–58, 7:13–16. RFID system 100 includes RFID transaction device 102 and RFID reader 104. *Id.* at 7:16–18. RFID reader 104 may communicate with merchant point-of-sale device (“POS”) 106 for completing a transaction. *Id.* at 7:18–25.

Figure 4 of the '181 patent is reproduced below.

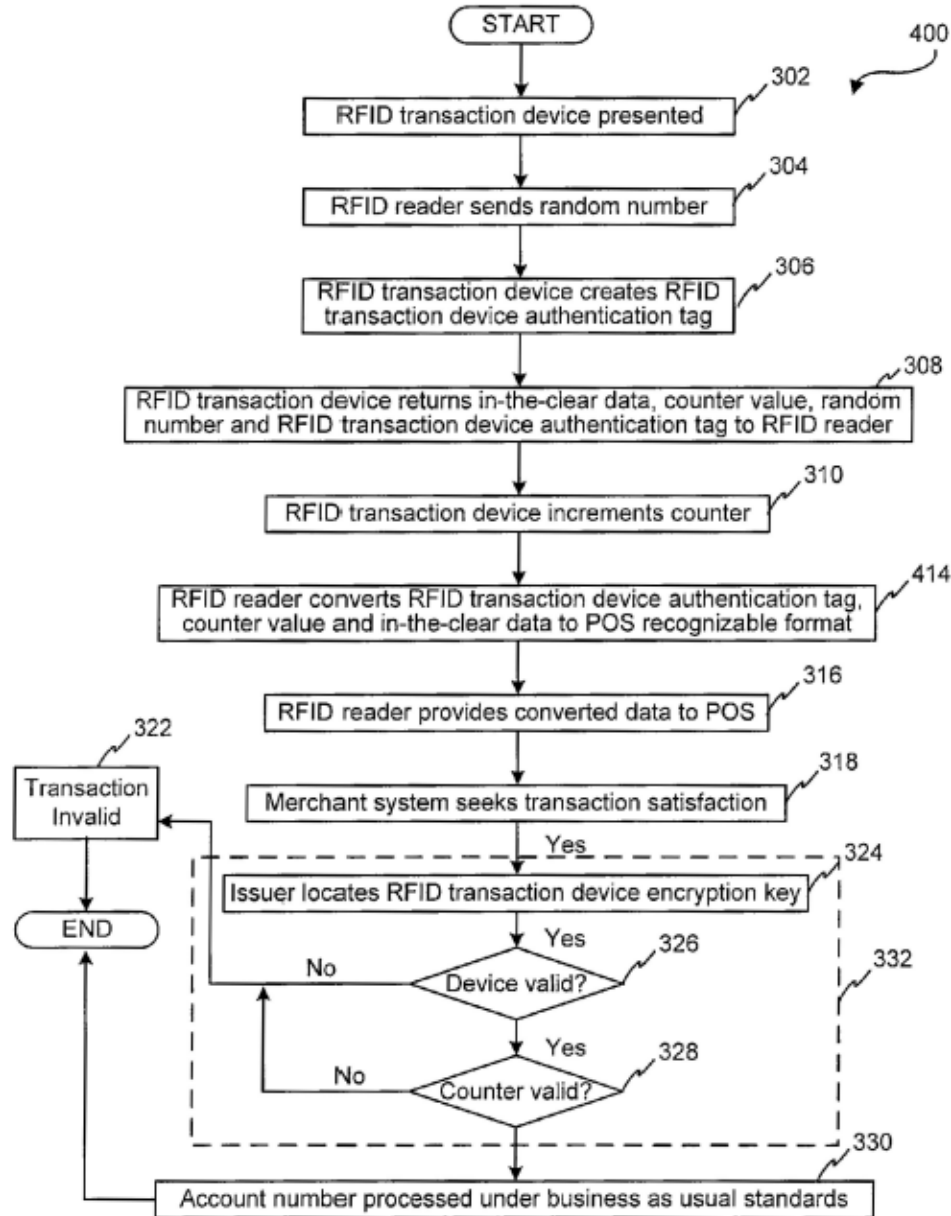


FIGURE 4

Figure 4 is “a flow diagram of an exemplary RFID transaction device authentication” where “RFID transaction device 102 is validated using the counter value.” *Id.* at 3:65–67, 12:43–45. At step 304, RFID reader 104 sends a random number to RFID transaction device 102. *Id.* at 12:45–48. At step 306, “RFID transaction device 102 receives the random number and

creates a RFID transaction device authentication tag using the random number, the in-the-clear data^[1], and a counter value.” *Id.* at 12:49–52. At step 308, RFID transaction device 102 provides the RFID transaction device authentication tag to RFID reader 104. *Id.* at 12:51–54. At step 310, RFID transaction device 102 increments the counter value. *Id.* at 12:54–56. RFID reader 104 and POS 106 then communicate to complete the transaction. *Id.* at 12:57–67.

Petitioner challenges claims 1, 2, and 4. Claims 2 and 4 depend from claim 1.

Claim 1 is illustrative and is reproduced below.

1. A method comprising:
generating, in a radio frequency identification (RFID) transaction device, an RFID transaction device authentication tag using a random number, a transaction device identifier, and a counter value, wherein the random number is received from an RFID reader;
transmitting the RFID transaction device authentication tag to the RFID reader; and
incrementing the counter value;
wherein an RFID transaction is authorized in response to verification of the RFID transaction device authentication tag.

¹ “Typically, the merchant receives the customer identifying information from the RFID reader which receives the information from the RFID device as unencrypted data (‘in-the-clear data’).” *Id.* at 3:4–8.

D. Evidence

Petitioner relies on the references listed below:

Reference		Date	Exhibit No.
Wankmueller	WO 03/050749 A1	Pub. June 19, 2003	1008
Johnson	US 6,078,888	June 20, 2000	1011
Walker	US 6,163,771	Dec. 19, 2000	1012
Davis	US 5,577,121	Nov. 19, 1996	1013
Nerlikar	US 5,629,981	May 13, 1997	1014

Petitioner also relies on the declaration of Bruce McNair (Ex. 1015) and the Supplemental Declaration of Mr. McNair (Ex. 1028).

Patent Owner does not rely on expert testimony.

E. Asserted Grounds of Unpatentability

We instituted on the following grounds of unpatentability:

No.	Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1	1	102(b) ²	Wankmueller
2	1, 4	103(a)	Wankmueller
3	1, 2, 4,	103(a)	Johnson, Walker
4	1, 2, 4	103(a)	Johnson, Walker, Davis
5	1, 2, 4	103(a)	Johnson, Walker, Nerlikar

² The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. §§ 102 and 103. Because the ’181 patent was filed before March 16, 2013, the effective date of the relevant amendments, the pre-AIA versions of §§ 102 and 103 apply.

No.	Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
6	1, 2, 4	103(a)	Johnson, Walker, Davis, Nerlikar

II. ANALYSIS

A. Claim Construction

We construe a claim

using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.

37 C.F.R. § 42.100(b); *see also Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

The parties dispute whether the method of claim 1 has a required order. Claim 1 recites, inter alia, “generating . . . an RFID transaction device authentication tag using . . . a counter value,” and “incrementing the counter value.” Patent Owner argues that “claim 1 must be read as reciting an authentication tag that is generated using a pre-incrementation instance of the counter value.” PO Resp. 9. Thus, Patent Owner argues that there is an order to the steps of claim 1, at least as to the generating and incrementing steps, with the generating step occurring before the incrementing step. *Id.* at 2–12.

“Unless the steps of a method actually recite an order, the steps are not ordinarily construed to require one. However, such a result can ensue when the method steps implicitly require that they be performed in the order written.” *Interactive Gift Express, Inc. v. Compuserve Inc.*, 256 F.3d 1323,

1342 (Fed. Cir. 2001) (internal citations omitted). The Federal Circuit has characterized this as a “general rule.” *Mformation Techs., Inc. v. Research in Motion Ltd.*, 764 F.3d 1392, 1398 (Fed. Cir. 2014). To determine whether the steps of a method nevertheless should be construed to have an order, “[f]irst, we look to the claim language to determine if, as a matter of logic or grammar, they must be performed in the order written.” *Altiris, Inc. v. Symantec Corp.*, 318 F.3d 1363, 1369 (Fed. Cir. 2003). “If not, we next look to the rest of the specification to determine whether it ‘directly or implicitly requires such a narrow construction.’” *Id.* at 1370 (quoting *Interactive Gift*, 256 F.3d at 1343). “If not, the sequence in which such steps are written is not a requirement.” *Id.*

As to the first step, the logic or grammar reflected in the claim language, we consider whether some steps of a method must take place as preconditions for other steps. *See Mantech Envtl. Corp. v. Hudson Envtl. Servs., Inc.*, 152 F.3d 1368 (Fed. Cir. 1998). The *Mantech* case provides an example. In that case, a claimed step of introducing acetic acid to a well could not take place until after the step in which the well was provided; a step of introducing an aqueous solution for mixing with the acidified groundwater could not take place until after the acetic acid was mixed with the groundwater in the well; and a step of introducing a treating flow into the ground water could not take place without the acidic condition and ferrous ions created by prior steps. *Id.* at 1375–76; *see also E-Pass Techs., Inc. v. 3Com Corp.*, 473 F.3d 1213, 1222 (Fed. Cir. 2007) (“Substantively, because the language of most of the steps of its method claim refer to the completed results of the prior step, E-Pass must show that all of those steps were performed in order.”).

Similarly, in *Loral Fairchild Corp. v. Sony Corp.*, 181 F.3d 1313, 1321 (Fed. Cir. 1999), a step of forming implanted barrier regions in a semiconductor substrate necessarily followed a step of forming a first insulation layer because the claim recited that the edges of the implanted barrier regions are aligned with the vertical edges of the insulation layer. According to the Federal Circuit, “[b]y the literal language of the claim, the edges of the implantation barrier regions are aligned with the edges of the insulation layer; hence, the insulation layer must already be in place in order to align the barrier regions with it during ion implantation.” *Id.*

In *Mformation*, in the claim phrase “delivering the command from the mailbox at the server to the wireless device by establishing a connection between the wireless device and the server, [and] transmitting the contents of the mailbox from the server to the wireless device,” the Federal Circuit determined that “claim 1 requires that a connection be established before transmission” because “the separate sub-step for establishing a connection would become ‘superfluous’ if we concluded that a connection did not have to be established (completed) before transmission,” and further reasoned “that is because, under such construction of the claim, establishing a connection is necessarily encompassed in transmitting a command.” 764 F.3d at 1399. As to other steps in the claimed method, “[a]s a matter of logic, a mailbox must be established before the contents of said mailbox can be transmitted.” *Id.* at 1400.

In contrast, in *Altiris*, a step of “setting said boot selection flag” did not necessarily follow “testing automatically for source of said means of booting; said testing including reading a boot selection flag and comparing said boot selection flag with a known flag setting” because the claim

language “neither grammatically nor logically indicates that the ‘setting’ step must occur in a particular order compared to other steps.” 318 F.3d at 1370. Petitioner points out that, in *Altiris*, the boot selection flag of the setting step derived its antecedent basis from the testing step, yet the Federal Circuit still found no grammatical or logical reason to order those steps. Reply 3. Similarly, in *Interactive Gift*, a first step of providing information did not necessarily have to take place before a fourth step of receiving the request reproduction code, as “[l]ogically, information could be sent after a request is made.” 256 F.3d at 1343.

Claim 1 in this proceeding recites a method including the steps of
generating, in a radio frequency identification (RFID)
transaction device, an RFID transaction device authentication
tag using a random number, a transaction device identifier, and
a counter value, wherein the random number is received from
an RFID reader;
. . . and,
incrementing the counter value.

Patent Owner argues that

Use of the term “the” when reciting “incrementing *the* counter value” indicates unequivocally that the counter value being incremented is the same counter value used as part of the generating step. In other words, claim 1 recites an authentication tag that is generated using a pre-incrementation instance of a counter value.

PO Resp. 6. According to Patent Owner,

[a]s a matter of logic and grammar, it is “a” counter value that is used in generating the RFID transaction device identifier, and “the” same counter value that is incremented. Logically and grammatically, it must be the earlier recited counter value from the generating step that is incremented. No other counter values are recited in the claim and the counter value from the

generating step is identified by an indefinite article, “a,” while the counter value from the incrementing step is identified by a definite article, “the.”

Id. at 8–9; *see also* Sur-reply 4 (“[A]s a matter of logic and grammar, claim 1 unequivocally recites that the counter value that is incremented is the counter value used as part of the generating step. In other words, claim 1 recites an authentication tag that is generated using a pre-incrementation instance of a counter value.”).

Petitioner argues that Patent Owner’s only basis in the language of claim 1 for imposing an order on the steps is the antecedent basis “the counter value” in the incrementing step derives from “a counter value” recited in the generating step. Reply 2. Petitioner argues that, in *Altiris*, the Federal Circuit declined to find an order in claimed steps, even though the later-recited step had a term that derived antecedent basis from an earlier-recited step. *Id.* at 3. Petitioner argues that use of definite articles is a requirement under 35 U.S.C. § 112(b), and does not signal a departure from the general rule that method steps are not construed to require an order. *Id.* at 2–3 (citing MPEP § 2173.05(e)).

Contrary to Patent Owner’s arguments, claim 1’s use of the article “a” before “counter value” in the generating step and “the” before “counter value” in the incrementing step simply provides proper antecedent basis for the counter value. Although *Altiris* did not expressly discuss antecedent basis, it is an example showing that antecedent basis alone does not signal that the logic or grammar of a method claim requires an order. 318 F.3d at 1369–70. The reference to “the counter,” referring back to “a counter,” is necessary to make clear that the claim is referring to the same counter in both instances, rather than separate counters. *See* MPEP § 2173.05(e) (“The

lack of clarity could arise where a claim refers to ‘said lever’ or ‘the lever,’ where the claim contains no earlier recitation or limitation of a lever and where it would be unclear as to what element the limitation was making reference. Similarly, if two different levers are recited earlier in the claim, the recitation of ‘said lever’ in the same or subsequent claim would be unclear where it is uncertain which of the two levers was intended.”).

Patent Owner points to nothing else in the language of claim 1, aside from antecedent basis, to show that the logic or grammar of the claim imposes an order to the steps. Patent Owner argues that, “as a matter of logic and grammar, claim 1 unequivocally recites that the counter value that is incremented is the counter value used as part of the generating step. In other words, claim 1 recites an authentication tag that is generated using a pre-incrementation instance of a counter value.” Sur-reply 4. This argument, however, recasts the argument that the use of the definite article “the” in “the counter value” of the incrementing step of claim 1 refers back to “a counter value” in the generating step, i.e., Patent Owner’s antecedent basis argument. Patent Owner further argues that

claim 1 needs to be understood as requiring a certain order because subsequent steps reference a previous step, logically mandating that the prior step must have been performed; to wit: generating an RFID transaction device authentication tag using a counter value, followed by transmitting the RFID transaction device authentication tag, followed by incrementing the counter value.

Id. at 5. However, the only reference in the incrementing step to the generating step is antecedent basis for “the counter value.” This argument, too, is just a recasting of Patent Owner’s antecedent basis argument, which we find unpersuasive.

Petitioner argues that claim 1 does not recite any pre-incremented counter value, or any other conditional or temporal language indicating when the counter must be incremented relative to other steps of claim 1, and concludes that “as a matter of logic, the timing of incrementing relative to other steps is immaterial as long as the value increments for each transaction.” Reply 3. We agree with Petitioner. Unlike the claims at issue in *Mantech*, *E-Pass*, *Loral*, and *Mformation*, nothing in claim 1 suggests that the incrementing step depends on the result of, or would be superfluous to, the generating step.

As explained above, if we do not find that the logic or grammar of claim 1 imposes an order on its steps, “we next look to the rest of the specification to determine whether it ‘directly or implicitly requires such a narrow construction.’” *Altiris*, 318 F.3d at 1370 (quoting *Interactive Gift*, 256 F.3d at 1343).

Patent Owner argues that the Specification’s embodiments corresponding to Figures 3, 4, 6, and 7 describe providing an RFID reader with a pre-incrementation instance of a counter value. PO Resp. 3–5. In Figure 4 (reproduced above) for example, RFID reader 104 sends RFID transaction device 102 a random number at step 304, RFID transaction device 102 creates a transaction device authentication tag at step 306, RFID transaction device 102 sends that tag to RFID reader 104 at step 308, and RFID transaction device 102 increments the counter in step 310. *Id.* at 3–4 (citing Ex. 1001, 3:65–67, 12:43–56, Fig. 4). In describing Figure 4, the Specification states

FIG. 4 illustrates another exemplary embodiment of the present invention wherein RFID transaction device 102 is validated using the counter value. In this exemplary embodiment, RFID

transaction device 102 is presented (step 302) and RFID reader 104 sends a random number to RFID transaction device 102 (step 304). RFID transaction device 102 receives the random number and creates a RFID transaction device authentication tag using the random number, the in the-clear data, and a counter value (step 306). RFID transaction device 102 may then provide the RFID transaction device authentication tag, random number, counter value, and in the-clear data to RFID reader 104 (step 308). RFID transaction device 102 may increment the counter value by a predetermined value (step 310).

Ex. 1001, 12:43–56. Here, the Specification characterizes Figure 4 as an “exemplary embodiment,” and, although it describes incrementing the counter after creating the authentication tag, it does not ascribe any importance to that timing. This portion of the Specification also includes no description that could be interpreted as a definition of the invention or disavowal of incrementing the counter at a different point in the process. Rather, it indicates that the counter “may” be incremented in step 310, not must.

As to Figures 3, 6, and 7, Patent Owner identifies steps 306, 310, steps 606, 610, and steps 606, 610, respectively as additional examples of creating the authentication tag before incrementing the counter. PO Resp. 4–5 (citing Ex. 1001, 11:45–59, 13:44–14:7, 14:63–15:30). The Specification similarly characterizes these as examples (“FIG. 6 depicts an exemplary method”; Figure 7 depicts “[a]n exemplary embodiment”), and describes generating an authentication tag before a counter is incremented in these examples, but includes no indication that these examples limit the invention or that the timing of incrementing the counter is important. Ex. 1001, 11:26–59, 13:44–14:7.

In other embodiments, the Specification describes the RFID device incrementing its counter before it generates and sends information to the RFID reader. For example, in Figure 2, the RFID device counter is incremented in step 206, before the RFID device provides an encrypted identifier, routing number, and counter value to the RFID reader in step 208. Ex. 1001, 10:1–12. Similarly, for the embodiment of Figure 5, the RFID transaction device sends in-the-clear data and the counter value to the RFID reader (step 508), the RFID transaction device increments the counter (step 310), and the RFID reader creates the authentication tag (step 512). *Id.* at 13:1–13.

Patent Owner contends that we should not consider these embodiments because they do not correspond to claim 1. PO Resp. 4–5. Specifically, Patent Owner argues that, in the Figure 2 embodiment, the transaction does not involve the RFID device generating an RFID transaction device authentication tag and in the Figure 5 embodiment, the RFID reader, rather than the RFID transaction device, generates the authentication tag. *Id.*; *see also id.* at 10 (“In the Figure 2 and Figure 5 embodiments, no RFID transaction device authentication tag is generated at the RFID transaction device, and so claim 1, which requires such generation, does not read on either of the Figure 2 or Figure 5 embodiments.”). According to Patent Owner, “[i]n all of the various embodiments in which an RFID transaction device generates an RFID transaction device authentication tag using a counter value, that RFID transaction device authentication tag is generated using a pre-incrementation instance of the counter value.” *Id.* at 5; *see also id.* at 10 (“**A**ll of the disclosed embodiments in the ’181 patent in which an RFID device generates an RFID

transaction device authentication tag require creation of the RFID transaction device authentication tag before incrementing of the counter value.”). Patent Owner argues that “[s]ince there is no ‘generating’ of an RFID transaction device authentication tag at all for this embodiment, whether and when the counter value is incremented is of no moment because it is readily apparent to any person of ordinary skill in the art that this is an embodiment outside the scope of claim 1.” Sur-reply 7. These arguments do not support Patent Owner’s construction. Even if the Figure 2 and Figure 5 embodiments do not correspond directly with claim 1, they still show that the Specification assigns no particular importance to the timing of incrementing the counter, and that there is no technical reason that an authentication tag must be generated using a pre-incrementation counter value.

In the Sur-reply, Patent Owner argues that the embodiments described with respect to Figures 2 and 5 provide a contrast to those embodiments that correspond to claim 1 and, thus, “when the patentee knew different processes were possible, the patentee described those processes explicitly.” Sur-reply 5. At the oral argument, Patent Owner contended that the embodiments of Figures 2 and 5 are “specifically excluded embodiments.” Tr. 25:19–26:6. Patent Owner, however, points us to no authority to support the premise that describing an embodiment not covered by a claim constitutes an express disavowal or exclusion of the features of that embodiment from the claim. The Specification itself does not state or imply that the examples of Figures 2 and 5, or any features of those examples, are excluded from the claims.

In the Sur-reply, Patent Owner argues that the Specification describes the counter as tracking transactions completed by an RFID transaction device, and that, if a post-incrementation value were used in generating the authentication tag, the counter value would not reflect completed transactions. Sur-reply 5–6 (citing Ex. 1001, 8:28–30). Patent Owner further argues that “there are instances where the RFID transaction device disables itself after a number of transactions,” and that “[i]ncrementing a counter value prior to generating the RFID transaction device authentication tag would, therefore, disable an otherwise usable RFID transaction device prematurely.” *Id.* at 6 (citing Ex. 1001, 8:60–65). Patent Owner did not make this argument in its Response, and therefore has forfeited it. *See* 37 C.F.R. § 42.23(b) (“A sur-reply may only respond to arguments raised in the corresponding reply.”). However, even if we were to consider it, Patent Owner points only to examples in the Specification, rather than statements that could be read to limit the invention. Ex. 1001, 8:28–30 (“Counter 118 *may be useful* for tracking the number of transactions completed by a particular device 102.”), 8:60–63 (“*In accordance with one embodiment of the present invention*, a RF transaction using a RFID transaction device is secured by limiting the number of transactions which may be performed with a particular transaction device.”) (emphases added). In any case, we find that the counter would track completed transactions regardless of whether it is incremented before or after an authentication tag is generated.

Patent Owner further argues that “because the drawings illustrate only the construction of claim 1 advocated by Patent Owner, reading the claims in some other manner (e.g., the manner contemplated in the Board’s Institution Decision) is improper.” PO Resp. 12 (citing 37 C.F.R. § 1.83(a)); *see also*

Sur-Reply 3 (“**all** of the embodiments in which an RFID transaction device generates an RFID transaction device authentication tag are described as operating in this fashion.”), 4 (“[I]n the ’181 patent, **all** of the embodiments in which an RFID transaction device generates an RFID transaction device authentication tag (that is, all of the embodiments covered by claim 1) are illustrated and described as operating in this fashion.”). However, “although the specification often describes very specific embodiments of the invention, [the Federal Circuit has] repeatedly warned against confining the claims to those embodiments,” and has “expressly rejected the contention that if a patent describes only a single embodiment, the claims of the patent must be construed as being limited to that embodiment.” *Phillips*, 415 F.3d at 1323. Patent Owner has introduced no persuasive evidence to support limiting the claims to the embodiments depicted in Figures 3, 4, 6, and 7.

Petitioner also points out (Reply 4–5) that the Specification states that “the steps recited in any of the method or process claims may be executed in any order and are not limited to the order presented.” Ex. 1001, 16:33–36. Patent Owner urges us to discount this statement as “boilerplate.” PO Resp. 11 (citing *In re Rasmussen*, 650 F.2d 1212, 1215 n.7 (CCPA 1981)); *see also* Sur-reply 9–10. Petitioner argues that this statement is specific and consistent with other statements in the Specification and should be considered. Reply 6. We agree with Petitioner. This statement is more than simply a general statement that the claims should not be limited to the preferred embodiments. It directly follows the ’181 patent’s statement that “the counter may increment the total transactions counted value by the predetermined incremental value at the completion of a successful transaction.” Ex. 1001, 16:31–33. Thus, the patent’s statement that the

steps of the method claims “may be executed in any order” is directly relevant to whether the order of steps in claim 1, including the “incrementing the counter value” step, matters. Moreover, even if the statement were simply boilerplate, Patent Owner has pointed to no persuasive evidence that claim 1 should be read to have an order to its steps. Thus, the statement is consistent with and reinforces what the Specification describes.

Patent Owner further argues that we are required to construe the claims to preserve their validity. PO Resp. 12 (citing *Phillips*, 415 F.3d at 1327–28). “While [the Federal Circuit has] acknowledged the maxim that claims should be construed to preserve their validity, [it has] not applied that principle broadly, and [it has] certainly not endorsed a regime in which validity analysis is a regular component of claim construction.” *Phillips*, 415 F.3d at 1327. Instead, the Federal Circuit has “limited the maxim to cases in which ‘the court concludes, after applying all the available tools of claim construction, that the claim is still ambiguous.’” *Id.* (quoting *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 911 (Fed. Cir. 2004)). Neither party argues, and we do not find, that claim 1 is ambiguous. Thus, this maxim does not apply to this proceeding.

For these reasons, the language of the claims does not require the counter value in the generating step to be a pre-incremented instance of the counter value. Rather, in light of the logic and grammar of claim 1, and our consideration of the Specification, we follow the general rule that steps of a method claim ordinarily are not construed to require an order, and conclude that the counter value in the generating step can be either a pre- or post-incrementation instance of the counter value.

No explicit construction of any other claim term is required for the purposes of this Decision. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

B. Grounds 1 and 2: Anticipation or Obviousness of Claims 1 and 4 over Wankmueller

Anticipation requires that a prior art reference set forth each and every element of a claim as set forth in the claim. *See Verdegaal Bros. v. Union Oil Co. of Cal.*, 814 F.2d 628,631 (Fed. Cir. 1987); *see also Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008) (anticipation not only requires that each element of a claim be present in a prior art reference, but also the “arrangement or combination” of those elements).

A claim is unpatentable under 35 U.S.C. § 103 “if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” We resolve the question of obviousness 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) objective evidence of nonobviousness, i.e., secondary considerations.³ *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

³ The record does not include allegations or evidence of objective indicia of nonobviousness.

1. *Level of Ordinary Skill in the Art*

Petitioner contends that a person of ordinary skill in the art at the time of the invention of the '181 patent would have had the following education and experience:

(1) at least an undergraduate degree in computer science or closely-related field, or similar advanced post-graduate education; and (2) 1–2 years of experience with systems related to secure communications systems, particularly in the transaction context, where more experience may substitute for less education and vice versa.

Pet. 10 (citing Ex. 1015 ¶¶ 29–32). Patent Owner does not dispute this level of skill or make its own proposal. *See generally* PO Resp.

On the complete record, we adopt Petitioner’s proposal as reasonable and consistent with the prior art and supported by expert testimony. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (the prior art may reflect an appropriate level of skill in the art).

2. *Scope and Content of the Prior Art—Overview of Wankmueller*

Wankmueller describes methods and systems for conducting financial transactions using payment cards. Ex. 1008, 1:11–13. Wankmueller discloses payment card 10 having a bar code 20 and RFID chip 30. *Id.* at 4:27–29; Fig. 1. The bar code is encoded with a payment account number (“PAN”) and has other account information, including “Track 2” data, such as expiration date, stored in RFID chip 30. *Id.* at 4:30–31, 5:5–11.

A conventional POS terminal equipped with both an optical bar code reader and a RF receiver is needed to read the information from the card. *Id.* at 5:21–23. From the information read from the card, the terminal

prepares an authorization request, and the authorization request is then processed in the same manner as conventional payment cards over existing payment networks. *Id.* at 5:24–26.

Figure 2 of Wankmueller is reproduced below.

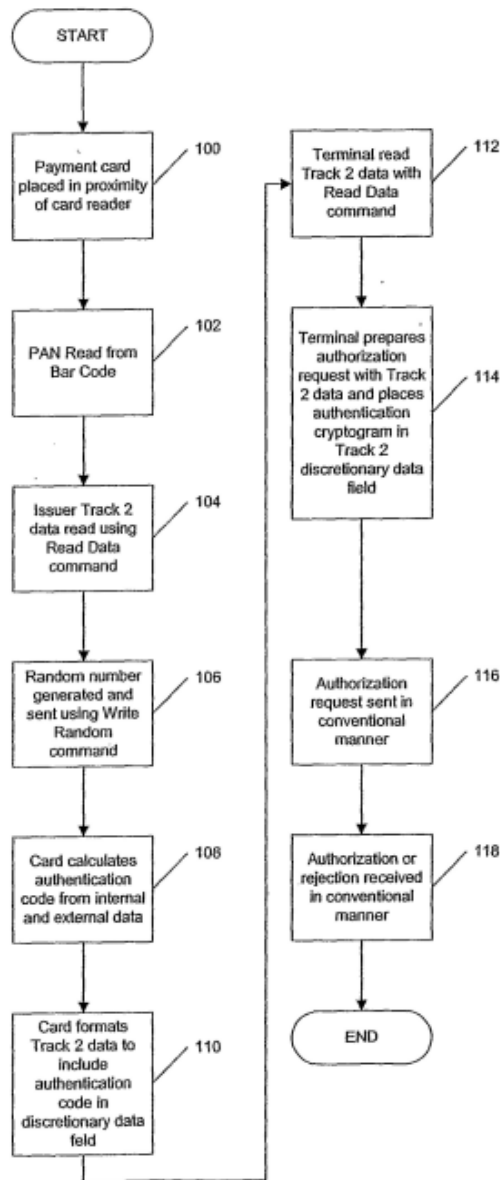


FIG. 2

Figure 2 illustrates “[a] flow chart of an authorization and authentication process between a payment card and a terminal.” *Id.* at 5:1–3, 6:6–8. First,

in step 102, the card reader reads the PAN data from the card's bar code. *Id.* at 9:23–24. “In step 104 (which could be performed before, after, or simultaneously with step 102), the terminal optionally sends a Read Data command to read the Track 2 data stored in the RF chip.” *Id.* at 9:25–27. “In step 106, the terminal sends a Write Data command with a challenge number to the payment card.” *Id.* at 9:29–30. “In step 108, the RF chip on the payment card calculates an authentication code using its cryptographic key with its internal data . . . and the challenge number sent by the terminal.” *Id.* at 10:1–3. “In step 110, the RF chip formats the Track 2 data to be sent to the terminal, replacing the discretionary data with the authentication code.” *Id.* at 10:4–6. “In step 112, the terminal performs a Read Data command and reads the new Track 2 data, [which] include[es] the authentication code . . . [and] may include a portion of the PAN.” *Id.* at 10:7–10. “In step 114, the terminal prepares an authorization request . . . [that] is generated from the PAN . . . and the remaining Track 2 data.” *Id.* at 10:13–15. The terminal then, in steps 116 and 118, processes the information to complete the transaction. *Id.* at 10:17–27.

Wankmueller also states that the RFID chip “maintain[s] a transaction counter and increment[s] the transaction counter before a predefined event, such as before each transaction or after each time a challenge number is presented to the card.” *Id.* at 6:14–17. “Upon receipt of the challenge number, the RFID device should increase its transaction counter, calculate the authentication code, and format Track 2 discretionary data with the chip authentication data. The terminal challenge number may be a random number” *Id.* at 6:24–29.

Preferably, the RF chip calculates an authentication code for verification by the issuer using its unique cryptographic authentication key and the following data:

- the PAN digits, if any, from the RF chip Track 2 data;
- the Expiry Date . . . from the RF chip Track 2 data;
- the Service Code . . . from the RF chip Track 2 data;
- the value from the counter maintained by the RF chip . . . ; and
- the challenge number . . . provided by the terminal.

Id. at 7:11–22.

3. *Claim 1*

Petitioner contends that claim 1 is anticipated by, or obvious over, Wankmueller. Pet. 22–27.

Petitioner contends that Wankmueller’s RFID device is “a radio frequency identification (RFID) transaction device,” as recited in claim 1. *Id.* at 23. Petitioner maps Wankmueller’s challenge number to “a random number”; Wankmueller’s PAN to “a transaction device identifier”; and Wankmueller’s “value from a counter” to “a counter value.” *Id.* at 23–25 (citing Ex. 1008, 6:8–30, 7:11–8:27).⁴ Petitioner contends that Wankmueller’s RFID device generates an authentication code using the PAN, challenge number, and value from the counter, and that this authentication code corresponds to “an RFID transaction device authentication tag.” *Id.* at 23–25.

⁴ We omit Petitioner’s color emphasis throughout this Decision.

According to Wankmueller,

[t]he bar code is encoded with at least one or more digits of the payment account number (PAN). Preferably, the bar code is encoded with, at a minimum, the most significant digits of the PAN, including the BIN used to identify the issuer. A BIN (bank identification number) is a unique series of numbers that identifies the issuer of a card and which is used to route authorization request messages over existing payment card networks, such as the BANKNET network from MasterCard International Incorporated.

The remaining account information is stored in the RF chip or circuitry 30. If a partial PAN is encoded in the bar code, the RF chip or circuitry 30 includes the remaining digits of the PAN.

Ex. 1008, 4:30–5:7. The '181 patent describes a transaction device identifier as including “any identifier for a transaction device which may be correlated to a user transaction account (e.g., credit, charge debit, checking, savings, reward, loyalty, or the like).” Ex. 1001, 5:34–37. We find that Wankmueller’s PAN may be correlated to a user transaction account and, therefore, is a transaction device identifier. Patent Owner does not contest Petitioner’s allegations as to this claim limitation.

Wankmueller describes “a random number” as an example of a terminal challenge number. Ex. 1008, 6:28–29, 9:1–2. Thus, we find that Wankmueller’s terminal challenge number is “a random number,” as recited in claim 1. As noted above, Wankmueller’s RFID chip “maintain[s] a transaction counter and increment[s] the transaction counter before a predefined event, such as before each transaction or after each time a challenge number is presented to the card.” *Id.* at 6:14–17. We find that the value of Wankmueller’s transaction counter is “a counter value,” as recited

in claim 1. Patent Owner does not contest Petitioner's allegations as to this claim limitation.

Wankmueller's RFID chip "calculates an authentication code for verification by the issuer using its unique cryptographic authentication key" and the PAN, challenge number, and the value of the counter. *Id.* at 7:11–22. We find that this discloses "generating, in a radio frequency identification (RFID) transaction device, an RFID transaction device authentication tag using a random number, a transaction device identifier, and a counter value, wherein the random number is received from an RFID reader," as recited in claim 1.

Claim 1 further recites "transmitting the RFID transaction device authentication tag to the RFID reader." As Petitioner points out, and as is shown in Wankmueller's Figure 2 (reproduced above), in step 112, the terminal reads data from the RFID transaction device, including the authentication code that we find corresponds to the RFID transaction device authentication tag of claim 1. Pet. 26 (citing Ex. 1008, 2:17–20, 6:22–30, 10:1–12, Fig. 2). For the terminal to read the authentication code, we find that the RFID transaction device must transmit this code. Thus, Wankmueller discloses this claim limitation. Patent Owner does not contest Petitioner's allegations as to this claim limitation.

Claim 1 further recites "incrementing the counter value." The parties dispute whether Wankmueller discloses or teaches this limitation. Wankmueller's RFID chip "maintain[s] a transaction counter and increment[s] the transaction counter before a predefined event, such as *before each transaction or after each time a challenge number is presented to the card.*" Ex. 1008, 6:14–17 (emphasis added). Thus, Wankmueller

discloses incrementing the counter value. However, the RFID chip increments the counter value before an authentication code is generated.

As explained in the Claim Construction section above, the parties dispute whether claim 1 requires the “generating” step to generate an authentication tag using a pre-incrementation instance of the counter value before the counter value is incremented in the “incrementing” step.⁵ For the reasons explained above, claim 1 does not. Thus, we find that Wankmueller discloses both the “generating” and “incrementing” steps.

Claim 1 further recites “wherein an RFID transaction is authorized in response to verification of the RFID transaction device authentication tag.” We agree with Petitioner and find that steps 114–118 of Wankmueller’s Figure 2 (reproduced above) show the terminal sending an authorization request with the authentication code and receiving an authorization for a transaction in response. Pet. 27 (citing Ex. 1008, 10:13–27, Fig. 2). Thus, we find that Wankmueller discloses this limitation of claim 1. Patent Owner does not contest Petitioner’s allegations as to this claim limitation.

On the complete record, we find that Wankmueller discloses each limitation of claim 1. Thus, Petitioner has proved, by a preponderance of the evidence, that claim 1 is anticipated by Wankmueller. Because we find anticipation, we need not determine whether claim 1 also would have been obvious over Wankmueller.

⁵ Patent Owner might articulate this as Wankmueller not satisfying the “generating” limitation, as the alleged RFID transaction device authentication tag is not generated using a pre-incrementation counter value, or as not satisfying the “incrementing step,” as Wankmueller’s incrementing does take place before the generating.

4. *Claim 4*

Claim 4 depends from claim 1 and adds “wherein the counter value is incremented a predetermined amount.” Petitioner does not contend that Wankmueller anticipates claim 4, but instead argues that claim 4 would have been obvious over Wankmueller. Pet. 28.

Wankmueller’s RFID chip “maintain[s] a transaction counter and *increment[s] the transaction counter* before a predefined event, such as before each transaction or after each time a challenge number is presented to the card.” Ex. 1008, 6:14–17 (emphasis added). Petitioner contends that, “[g]iven Wankmueller’s disclosure that the counter is a transaction counter, a [person of ordinary skill in the art] would have understood, or at least found obvious that the increment is by a predetermined amount (e.g., one) for each transaction or challenge number received, as that is how transactions would typically be counted.” Pet. 28 (citing Ex. 1015 ¶¶ 46, 52). Petitioner further argues that the provisional application to which the ’181 patent claims the benefit (U.S. Prov. App. 60/507,803) admits that the simplest approach to updating a counter value is to increment it by some value. *Id.* at 28–29 n.14 (citing Ex. 1007, 9 (“There are various ways that the counter can be updated. The simplest approach is to simply increment the counter by some value. That value can be obvious (e.g., 1) or something more obscure such as 47.”)).

Mr. McNair testifies “that the simplest approach to incrementing a counter value, or sequence number, would have been by starting it at zero and incrementing the value by one for each transaction, as transactions are incremented one at a time.” Ex. 1015 ¶ 46 (citing Ex. 1025, 95).

Mr. McNair notes that three other prior art references asserted by Petitioner

show incrementing a counter value one at a time. *Id.* (citing Johnson, Ex. 1011, 11:58–60; Walker, Ex. 1012, 8:27–30; Davis, Ex. 1013, 15:27–30). Mr. McNair acknowledges that other predetermined incrementation values could have been used, as simple counter values would be more predictable and more susceptible to attacks based on educated guesses. *Id.* (citing Ex. 1026, 1–2). However, Mr. McNair testifies, “a truly undetermined increment process would not make much sense and would therefore be unnecessarily complicated, if not impossible to duplicate and, therefore, authenticate, including before 2001.” *Id.* We credit this testimony, which is well-reasoned and consistent with the evidence in Johnson, Walker, and Davis.

Patent Owner argues that Wankmueller does not expressly state that its counter is incremented by a predetermined amount and that Petitioner improperly supplies such a teaching through expert testimony. PO Resp. 22–23. Patent Owner cites our Consolidated Trial Practice Guide (TPG)⁶ in support of an argument that expert testimony cannot take the place of required disclosure. *Id.* Patent Owner improperly crops the TPG in a way that changes its meaning, purporting to quote the TPG as follows:

Expert testimony [] cannot take the place of a disclosure in a prior art reference, when that disclosure is required as part of the unpatentability analysis. For example, . . . in an obviousness analysis, conclusory assertions from a third party about general knowledge in the art cannot, without supporting evidence of record, supply a limitation that is not evidently and indisputably within the common knowledge of those skilled in the art.

Id. (quoting TPG 36 (alterations by Patent Owner)).

⁶ Available at <https://www.uspto.gov/TrialPracticeGuideConsolidated>.

The TPG actually states:

Expert testimony, however, cannot take the place of a disclosure in a prior art reference, when that disclosure is required as part of the unpatentability analysis. For example, because “[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference,” *Verdegaal Bros., Inc. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987), a petitioner asserting anticipation cannot rely on its expert to supply disclosure of a claim element that is not expressly or inherently present in the reference. Similarly, in an obviousness analysis, conclusory assertions from a third party about general knowledge in the art cannot, without supporting evidence of record, supply a limitation that is not evidently and indisputably within the common knowledge of those skilled in the art. *K/S Himpp v. Hear-Wear Techs., LLC*, 751 F.3d 1362, 1365 (Fed. Cir. 2014).

TPG, 36. Here, the TPG states that expert testimony alone cannot supply a claim limitation when the reference asserted as anticipating is missing that limitation. As noted above, however, Petitioner does not assert that Wankmueller anticipates claim 4. Thus, Petitioner is not using expert testimony to supply an express disclosure that an anticipation analysis requires. Rather, Dr. McNair testifies as to how a skilled artisan would have read Wankmueller and the obvious inferences a skilled artisan would have drawn from the description in Wankmueller.

As to obviousness, the TPG makes clear that Petitioner could not merely assert, without record evidence, that Wankmueller’s counter is incremented by a predetermined amount. This is consistent with *K/S Himpp*, which held that the Board was correct to require a third-party requester, in *inter partes* reexamination, to offer record evidence to support its conclusory assertions that the structural features of dependent claims were known prior

art elements. 751 F.3d at 1365–66. But Petitioner does rely on record evidence, Mr. McNair’s testimony, to show what was common knowledge to those skilled in the art. Pet. 28 (citing Ex. 1015 ¶ 46). Mr. McNair, in turn, cites to several examples in the record showing that incrementing a counter by one was common knowledge. Ex. 1015 ¶ 46 (citing Ex. 1011, 11:58–60; Ex. 1012, 8:27–30; Ex. 1013, 15:27–30). As explained above, we credit that testimony.

Patent Owner also argues that it is improper hindsight to rely on disclosure in the ’181 patent’s provisional application. PO Resp. 22. However, the ’181 patent’s provisional admits that incrementing a counter by one is the obvious choice. Ex. 1007, 9 (“There are various ways that the counter can be updated. The simplest approach is to simply increment the counter by some value. *That value can be obvious (e.g., 1) or something more obscure such as 47.*” (emphasis added)). The Director has provided guidance stating that “[a]dmissions are ‘permissible evidence in an *inter partes* review for establishing the background knowledge possessed by a person of ordinary skill in the art’ and ‘provide a factual foundation as to what a skilled artisan would have known at the time of invention.’”

Katherine K. Vidal, *Updated Guidance on the Treatment of Statements of the Applicant in the Challenged Patent in Inter Partes Reviews under § 311*, 3 (June 9, 2022) (quoting *Qualcomm Inc. v. Apple Inc.*, 24 F.4th 1367, 1376 (Fed. Cir. 2022)). Patent Owner’s admission is further evidence that incrementing Wankmueller’s counter by a predetermined amount, such as one, would have been obvious.

This is also an instance where resort to common sense is appropriate. “Common sense has long been recognized to inform the analysis of

obviousness if explained with sufficient reasoning.” *Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1328 (Fed. Cir. 2009); accord *KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. 398, 421 (2007) (“Rigid preventative rules that deny factfinders recourse to common sense, however, are neither necessary under our case law nor consistent with it.”). As Petitioner observes, “[t]he idea that a counter worked by counting is so obvious that it’s in the name itself.” Tr. 15, 23–24. Mr. McNair testifies that “a truly undetermined increment process would not make much sense and would therefore be unnecessarily complicated, if not impossible to duplicate and, therefore, authenticate, including before 2001.” Ex. 1015 ¶ 46.

Patent Owner argues that a counter that increments by an amount that is not predetermined would have been more difficult for hackers to guess, and that skilled artisans might have adopted that approach instead for Wankmueller’s counter. PO Resp. 23–25. Tellingly, Patent Owner offers no evidence of the existence of such a counter that counts by amounts that are not predetermined, how such a counter would work (presumably, incrementing randomly), or how it could be used to authenticate a transaction if neither side to the transaction knows in advance what the incrementation will be. This defies logic and common sense and is not persuasive.

Petitioner’s evidence, including the testimony of Mr. McNair, the Johnson, Walker, and Davis references, and the admissions in the provisional application to the ’181 patent, shows that the simplest and most straightforward way to implement Wankmueller’s counter would have been to increment it by a predetermined value (e.g., one). We find that a skilled

artisan would have had sound reasons to implement Wankmueller's counter in that manner.

Patent Owner does not argue or introduce evidence of objective indicia of nonobviousness. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claim 4 would have been obvious over Wankmueller.

C. Ground 3: Obviousness of Claims 1, 2, and 4 over Johnson and Walker

Petitioner contends that independent claims 1, 2, and 4 would have been obvious over a combination of Johnson and Walker. Pet. 43–55. For the reasons given below, Petitioner has proved by a preponderance of the evidence that claims 1, 2, and 4 would have been obvious over Johnson and Walker.

1. Scope and Content of the Prior Art

a) Overview of Johnson

Johnson describes a secure transaction system that includes a tag 100, a POS device 200, and a host network 300. 1011, 5:48–51. In one example, “the tag is adapted to bi-directionally communicate with a POS device, preferably a fuel dispenser, which further communicates with a host network to provide authorization of the tag and carry out any desired purchases or transactions.” *Id.* at 2:63–67. “[T]he tag 100 and host network 300 are adapted to encrypt and decrypt certain communications there-between, while the POS device 200 primarily only relays the encrypted information sent between the tag 100 and the host network 300.” *Id.* at 5:59–63. POS device

200 is not able to decrypt the information. *Id.* at 5:63–65. Host network 300 maintains account and financial information associated with tag 100, which has a unique identifier. *Id.* at 2:13–15.

Figure 5 of Johnson is reproduced below:

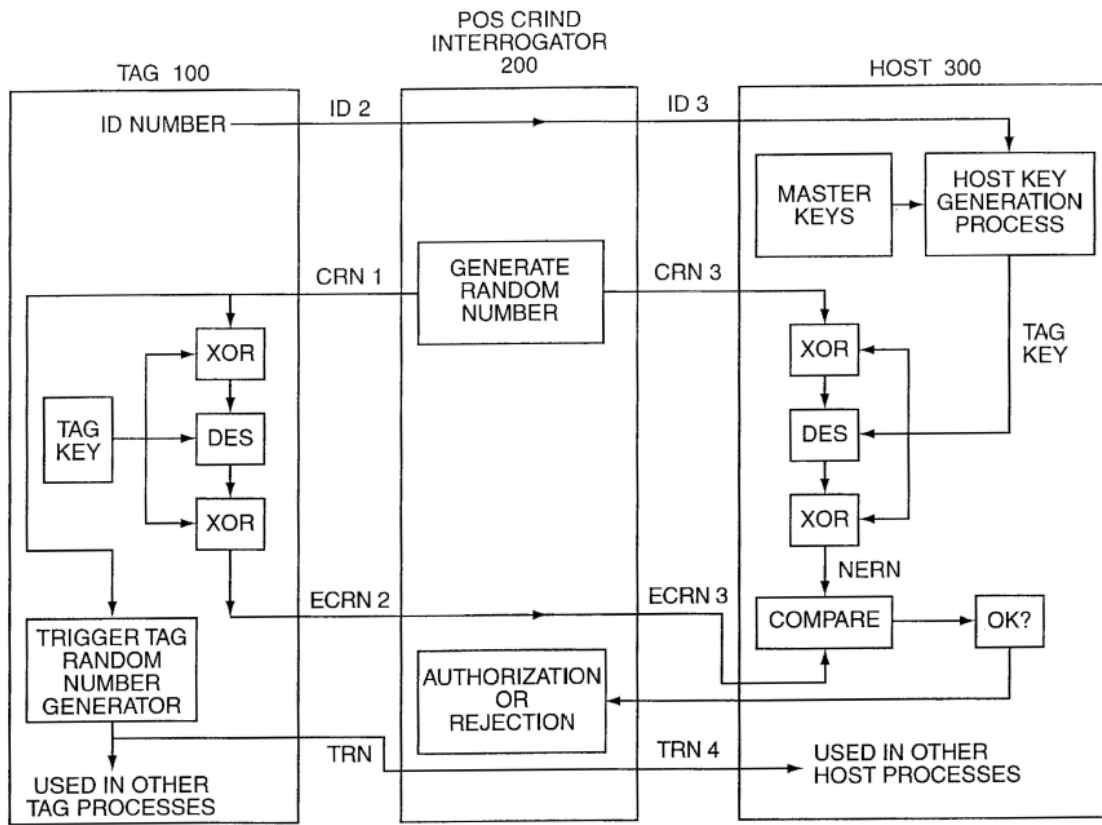


FIG. 5

Figure 5 depicts a tag authentication process. *Id.* at 5:1, 10:16. First, POS device 200 generates and sends random number CRN to tag 100 and to host network 300. *Id.* at 10:54–56. Tag 100 encrypts random number CRN to create an encrypted random number ECRN and returns encrypted random number ECRN to POS device 200. *Id.* at 10:56–59. POS device 200 relays the encrypted random number ECRN, the tag ID, and random number CRN to Host network 300. *Id.* 10:59–62. Host network 300 encrypts the random number CRN in the same manner as tag 100 and compares the result to the

encrypted random number ECRN for a match. *Id.* at 10:65–11:5. Tag 100 and Host network 300 use identical cryptography techniques known only by tag 100 and host network 300, but not by POS device 200. *Id.* at 3:22–24.

Tag 100 also sends to POS device 200 its tag ID. In the example of Figure 5, “[t]he tag 100 encrypts the random number and returns the encrypted random number (TRN) to the POS device 200 along with a tag identification number (ID) in step 2.” *Id.* at 10:19–22. In another example, in a fueling environment, POS device 200 continuously scans for tag 100 within a field or range, and tag 100 responds once inside the field by sending a command to POS device 200. *Id.* at 10:46–51. “Once the tag 100 responds, the POS device 200 will recover the tag ID from the tag 100,” after which “[t]he POS device 200 generates the random number (CRN) and sends it to the tag 100 with an appropriate command.” *Id.* at 10:53–56.

Johnson’s tag 100 also maintains a current sequence number that corresponds to a tally of transactions or operations that the tag has conducted. *Id.* at 11:47–54. The host sends a sequence number to the tag with each command, and if the sequence number sent by the host does not match the current sequence number maintained by the tag, the command is ignored. *Id.* at 11:54–58. “The sequence number adds further security by ensuring the host 300 is transmitting proper data and/or commands to the tag, that no unauthorized communications have occurred and that each previous communication between the host and tag was properly received and acted on.” *Id.* at 11:62–67.

b) Overview of Walker

Walker describes generating a single-use, transaction-specific financial account number for credit card transactions. *Id.* at Ex. 1012, 1:6–10. For example, Walker describes a device 100, such as a smartcard with a keypad, display, memory and central processor, that generates single-use credit card numbers. *Id.* at 5:49–54, Fig. 1. The device sends an encrypted single-use credit card number to a merchant, who sends the number to the card issuer, who decrypts the number and authorizes or denies the transaction. *Id.* at 6:59–7:9, Fig. 3A.

Figure 8 of Walker illustrates an example:

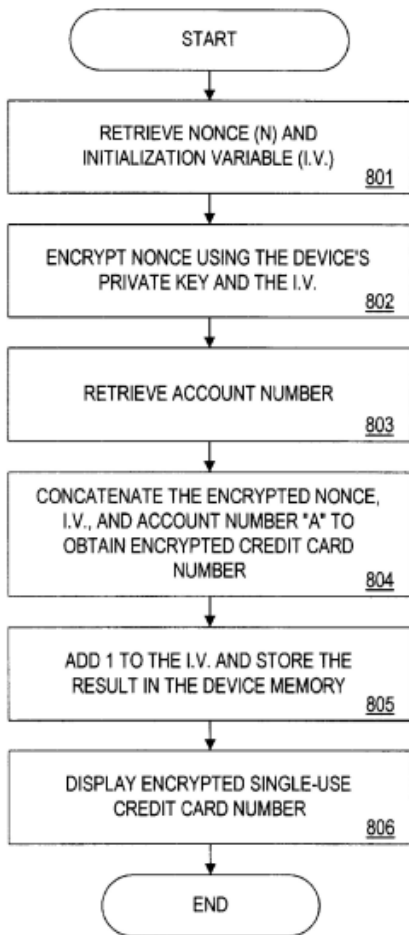


FIG. 8

Figure 8 is a flow chart of the steps for generating an encrypted single-use credit card number. *Id.* at 8:9–11. “In step 801, the device central processor 101 retrieves the nonce 602 and the initialization variable 704 from the device memory 104.” *Id.* at 8:11–13. A “nonce” is an additional piece of information associated with the account number and stored in the device’s memory. *Id.* at 7:31–34. An “initialization variable” is used to ensure that each single-use credit card number is unique to that transaction, preventing a

“replay” attack. *Id.* at 7:42–45. The initialization variable is set to zero when the card is newly issued, and is incremented each time a single use credit card number is generated. *Id.* at 7:48–51. “A credit card number consists of an m-bit initialization variable (abbreviated IV), an a-bit account number, and an n-bit nonce (abbreviated N), where $m+a+n=53$.” *Id.* at 7:60–62. “In step 802, the nonce is encrypted using the user’s private key K and the IV.” *Id.* at 8:13–14. “The central processor 101 then retrieves the account number from the device memory 104 (step 803).” *Id.* at 8:19–20. “In step 804, the encrypted nonce C, the initialization variable IV, and account number A are concatenated to form an encrypted, single-use credit card number CCN.” *Id.* at 8:20–23. Credit card number CCN is transmitted, via a merchant, to the issuer’s central processor for authorization of the transaction. *Id.* at 8:31–35.

Figures 9A and 9B of Walker are reproduced side-by-side below, and show the process that the credit card issue uses to authorize the transaction once it receives the single-use CCN.

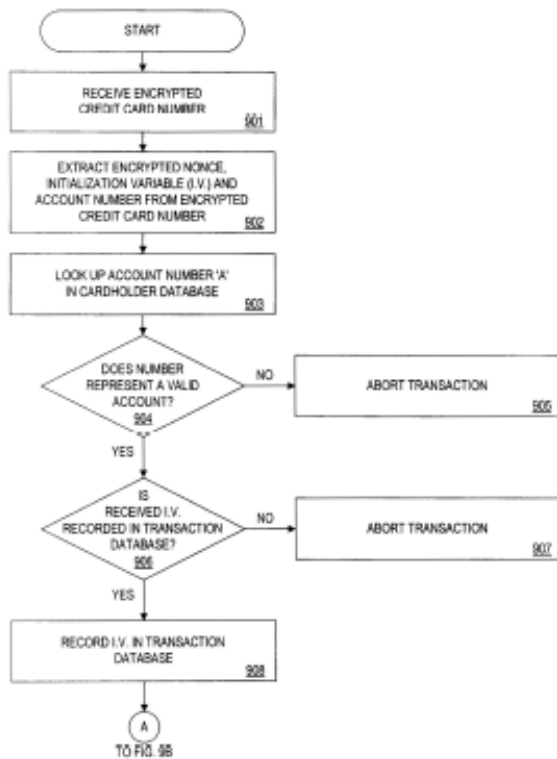


FIG. 9A

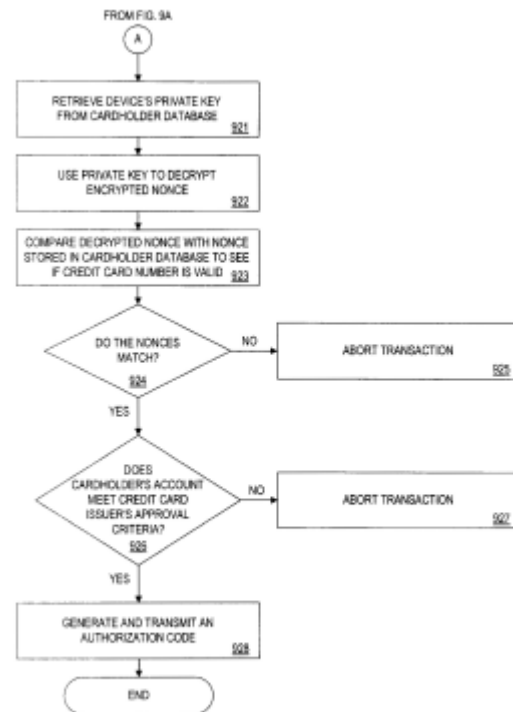


FIG. 9B

Figures 9A and 9B, collectively, depict a connected flowchart showing the central processor of a credit card issuer generating an authorization code. *Id.* at 5:24–27. The credit card issuer’s central processor verifies the card number by extracting the encrypted nonce C, the initialization variable IV, and account number A from the credit card number. *Id.* at 8:41–43, Fig. 9A, step 902. “The processor then retrieves the extracted account number from the cardholder account database 411 (step 903), and determines whether the account number is valid (step 904).” *Id.* at 8:43–46. “If the account number is valid, the processor looks up the account number in the credit card transaction database 413 to determine whether the card holder has previously used the initialization variable IV (step 906).” *Id.* at 8:47–51. “If the cardholder has done so, the transaction is aborted (step 908).” *Id.* at 8:51–52. “If the initialization variable has not been used, the incremented

initialization variable is stored in the credit card transaction database 413 (step 908).” *Id.* at 8:52–54.

“In step 921, the processor retrieves the card holder’s private key K in the private key database 412.” *Id.* at 8:55–56. “The private key K then is used to decrypt the encrypted nonce (step 922).” *Id.* at 8:56–57. “This recovers the original nonce N . . . [that] is compared against the nonce 602 stored in the account private key database 412 (step 923).” *Id.* at 8:62–63. “If they match (step 924) then the credit card number is considered valid; otherwise the transaction is aborted (step 925).” *Id.* at 8:62–64.

“If the card is found to be valid, and if the cardholder’s account meets the credit card issuer’s approval criteria (step 926), then the issuer’s central processor generates an authorization code and transmits the code to the merchant (step 928).” *Id.* at 8:66–9:3. “If not, then the transaction is aborted (step 927).” *Id.* at 8:9:3–4.

2. *Claim 1*

Claim 1 recites “generating, in a radio frequency identification (RFID) transaction device, an RFID transaction device authentication tag using a random number, a transaction device identifier, and a counter value, wherein the random number is received from an RFID reader.”

Petitioner contends that Johnson’s tag 100 is an RFID transaction device and that Johnson’s POS terminal 200 is an RFID reader. Pet. 44 n.15. Mr. McNair testifies that a skilled artisan would have recognized Johnson’s use of tags and interrogators, communicating via radio frequency transmissions, as terms of art used in RFID technology. Ex. 1015 ¶ 65 (citing Ex. 1011, 1:42–46, 5:66–6:4, 20:20–25, Figs. 2A, 2C). We credit

Mr. McNair’s uncontroverted testimony on this point and find that Johnson’s tag 100 is an RFID transaction device and that Johnson’s POS terminal 200 is an RFID reader. Patent Owner does not contest Petitioner’s allegations on these points.

Petitioner contends that the CRN Johnson’s tag 100 receives from POS device 200 is a random number; that Johnson’s tag ID number is a transaction device identifier; and that Johnson’s sequence number is a counter value, as recited in claim 1. Pet. 43–44, 46–48. Johnson states that “[t]he POS device will generate authentication check data, preferably a random number, and send it to the tag for encryption.” Ex. 1011, 3:28–30; *see also id.* at 10:17–19 (“In step 1, the POS communication electronics 204 of the POS device 200 generate and send a random number (CRN) to the tag 100 and to the host 300.”). We find that the CRN is a random number.

As to Johnson’s tag ID, “a 10 byte tag ID number comprising the standard industry code, company code and individual sequence number is directly loaded by the host 300 into the tag 100 during generation of the tag.” *Id.* at 9:64–67. This is consistent with the ’181 patent’s description of a transaction device identifier as including “any identifier for a transaction device which may be correlated to a user transaction account (e.g., credit, charge debit, checking, savings, reward, loyalty, or the like).” Ex. 1001, 5:34–37. We find that Johnson’s tag ID is a transaction device identifier.

As to Johnson’s sequence number, it corresponds to a tally of transactions or operations the tag has conducted. Ex. 1011, 11:52–54. We find that the sequence number is a counter value. Patent Owner does not contest Petitioner’s allegations that Johnson’s CRN is a random number; that

Johnson's tag ID is a transaction device identifier; or that Johnson's sequence number is a counter value.

As Petitioner notes, in Johnson, "[t]he tag 100 encrypts the random number and returns the encrypted random number (TRN)⁷ to the POS device 200 along with a tag identification number (ID) in step 2." Ex. 1011, 10:19–22; *see also* Pet. 45. As Petitioner concedes, Johnson's tag 100, however, does not send the sequence number to the POS device 200 along with the ECRN or tag ID. Reply 14 ("While Johnson does not disclose the use of the counter value and the account information as part of a single code for validating a *financial* transaction, Walker does in a similar context.").

Petitioner argues that Walker describes receiving a nonce value (not a random number) from a device reader; encrypting that value using a key and an initialization variable (IV) (which Petitioner argues corresponds to a counter value); concatenating the encrypted nonce value to an account number A (which Petitioner argues corresponds to a transaction device ID); and sending that concatenated result (a CCN) to a merchant. Pet. 48–49 (citing Ex. 1012, 7:28–62, 8:9–33). According to Petitioner, using the guidance provided by Walker, a skilled artisan would have modified Johnson such that Johnson's tag 100 would have encrypted Johnson's random number CRN using a key and the sequence number, would have concatenated the encrypted random number with the tag ID, and would have transmitted the result to POS device 200. *Id.* at 43–46. Encrypting the random number using the sequence number and concatenating the result

⁷ Petitioner notes that Johnson sometimes uses "TRN" and other times uses "ECRN" to refer to the encrypted random number. Pet. 45 n.16 (citing Ex. 1011, 10:16–22, 13:4–42).

with the tag ID would, in Petitioner’s combination, correspond to “generating . . . an RFID transaction device authentication tag using a random number, a transaction device identifier, and a counter value,” as recited in claim 1. *Id.* at 49–50.

Petitioner argues that Walker provides express motivation to include a counter value in the encryption process. Pet. 50 (citing Ex. 1012, 7:37–45⁸). According to Walker, “[t]he initialization variable 704 is used to ensure that each credit card number is unique to the particular transaction, thereby preventing a ‘replay’ attack.” Ex. 1012, 7:42–45. Reinforcing Walker’s disclosure, Mr. McNair’s testifies that, in the context of financial security systems, transaction counters were “applicable in the cryptography context to thwart what were known as ‘replay attacks’ in which a valid data transmission is fraudulently repeated or delayed.” Ex. 1015 ¶ 45 (citing Ex. 1023, 3; Ex. 1024, 3:29–33). Petitioner argues that using the sequence number, which changes in a predictable manner, in the encryption process would have provided a security benefit, and would have thwarted hackers, by adding a check on the validity of the transaction, as Walker’s IV does in its transaction. Pet. 50–51 (citing Ex. 1015 ¶¶ 44–46, 73). Petitioner contends that this combination would have involved a simple substitution of Walker’s method of encrypting a number using an initialization variable and concatenating it to a tag ID for Johnson’s encryption of a challenge random number, to obtain predictable results. *Id.* at 51 (citing Ex. 1015 ¶ 74).

⁸ Petitioner cites to Ex. 1012, 40:37–45. However, the discussion of a “replay attack” appears at column 7, lines 37–45. Thus, Petitioner’s citation appears to be a typographical error.

We credit Mr. McNair’s testimony and find that a skilled artisan would have had reasons, with rational underpinning, to incorporate Johnson’s sequence number in its encryption of the CRN in order to improve security, prevent replay attacks, and thwart hackers. *See KSR*, 550 U.S. at 417 (“[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.”).

Claim 1 further recites “transmitting the RFID transaction device authentication tag to the RFID reader.” Petitioner contends that Johnson teaches that tag 100 transmits the ECRN along with the tag ID to POS device 200 in step 2 of Figure 5. Pet. 53 (citing Ex. 1011, 3:31–33, 10:15–25, 10:56–59). According to Petitioner, “[a]s modified by Walker, the generation of the encrypted random number would include the use of a counter value, such as the current sequence number as a tally of transactions, and concatenation with a tag ID.” *Id.* According to Johnson, “[t]he tag 100 encrypts the random number and returns the encrypted random number (TRN) to the POS device 200 along with a tag identification number (ID) in step 2.” Ex. 1011, 10:19–22, Fig. 5 (step 2). We agree with Petitioner and find that Johnson teaches transmitting an RFID transaction device authentication tag to an RFID reader.

Claim 1 further recites “incrementing the counter value.” Petitioner contends that Johnson’s disclosure of a sequence number that “**corresponds to a tally of transactions**” teaches incrementing a counter value. Pet. 53 (quoting Ex. 1011, 11:49–54). Petitioner further argues that Walker discloses incrementing its IV by one. *Id.* (citing Ex. 1012, 8:27–30). We

agree, and find that both Johnson and Walker teach incrementing a counter value.

Claim 1 further recites “wherein an RFID transaction is authorized in response to verification of the RFID transaction device authentication tag.” Petitioner contends that Johnson’s host 300 “uses information associated with the tag ID number received from the POS terminal to encrypt the CRN and compare its result to the tag’s encrypted random number forwarded by the terminal—if they match, the host determines that the tag is valid and authorized.” Pet. 54–55 (citing Ex. 1011, 3:11–21, 3:34–44, 10:27–41, 10:63–11:8, 14:6–15, Fig. 5). We agree with Petitioner and find that Johnson teaches authorizing a transaction in response to verifying an RFID transaction device authenticating tag.

Patent Owner argues that Petitioner’s proposed combination “would necessarily include Johnson’s teachings concerning presentation of a tag ID to a POS device separately from and prior to forming any encrypted value that includes a challenge sent by the POS device or returning same to the POS device.” PO Resp. 28 (citing Ex. 1011, 10:46–51); *see also id.* at 30 (“As discussed above, however, a Johnson-Walker combination would not have a single-use value or other form of tag ID generated using both a random number received from an RFID reader and a counter value. Instead, the encrypted random number would be generated separately from the single-use value and the two would be provided separately to the POS device.”); Sur-reply 21 (“[I]t remains the case that in Johnson the tag ID is sent separately from the encryption payload, and is not used in generating the encryption payload.”). As noted above, Johnson describes an embodiment in which, “[i]n order for the host 300 to authenticate a tag 100,

the POS communication electronics 204 will continuously scan for a tag 100 within a particular communications field or range. The tag 100 will respond once inside the field by sending a command to POS device 200.” Ex. 1011, 10:46–51. In light of this example and a similar argument in the Preliminary Response (Prelim. Resp. 13), we stated in the Institution Decision:

Johnson’s tag 100 separately provides the tag ID to POS device 200 prior to receiving the random number CRN and after encrypting random number ECRN. *See, e.g.,* Ex. 1011, 10:53–62. This is unlike Walker, which discloses only transmitting a single-use credit card number CCN to the merchant after encryption. *See, e.g.,* Ex. 1012, 3:11–36. Given these differences in Johnson and Walker, we question whether a POSITA would have modified Johnson in the manner and for the reasons proposed in the Petition if Johnson discloses separately providing the tag ID to POS device 200 from the encrypted random number ECRN. And, in particular, why a POSITA would have modified Johnson to concatenate the ECRN with the tag ID to form a short code.

Inst. Dec. 23–24.

In the Reply, Petitioner points out that “[n]ot all embodiments of Johnson disclose sending the tag ID *prior to* receiving the challenge random number, or CRN, and at least one discloses sending the tag ID ‘along with’ the ECRN *after* receiving the CRN and performing encryption on the CRN. Johnson.” Reply 16 (citing Ex. 1011, 10:16–25). As we note above, Johnson describes another embodiment, corresponding to Figure 5, in which “[t]he tag 100 encrypts the random number and returns the encrypted random number (TRN) to the POS device 200 along with a tag identification number (ID) in step 2.” Ex. 1011, 10:19–22. Petitioner relied on this disclosure in the Petition. Pet. 45. Because Johnson describes an embodiment in which the ECRN and tag ID are sent together, we are not

persuaded by Patent Owner's argument. Instead, we find that a skilled artisan would have concatenated Johnson's encrypted random number (modified, per Walker, to be encrypted using the sequence number) with Johnson's tag ID in order to send the encrypted random number "along with" the tag ID.

Patent Owner also argues that Walker's initialization value is maintained in memory by the smart card, and not provided by the POS device, and that "[c]ombining these teachings with those of Johnson may result in Johnson-Walker employing single-use values computed using initialization values, as described by Walker, however, it would remain the case that the Johnson-Walker combination would treat this single-use value separately from the encrypted random number returned to a POS device."

PO Resp. 29. Patent Owner continues,

while a Johnson-Walker combination may replace the tag ID described by Johnson with a single-use number as described by Walker, for example to ensure the tag ID could not be imitated, that single-use number would still be treated separately from and would *not* be computed using any encrypted form of a random number received from a POS device as part of a challenge.

Id.

Petitioner responds that Patent Owner misunderstands the proposed combination and, contrary to Patent Owner's argument, "the technique used to encrypt the CRN would be Walker's technique, which encrypts some value, called a nonce, using a private key and an initialization value and then concatenates the result with a user's account information." Reply 17 (citing Pet. 49–50). Thus, Petitioner argues, "[a]s this technique is applied to Johnson's system, the CRN takes the place of the nonce and the encrypted

result is concatenated with the tag ID and communicated from the POS to a host.” *Id.* Petitioner further argues that “the Petition mapped the tag ID to the claimed ***transaction device identifier***, not the *authentication tag*.”

Id. (citing Pet. 44; PO Resp. 29–31).

We agree with Petitioner that Patent Owner appears to misunderstand Petitioner’s proposed combination. Petitioner does not contend that, in its combination, single-use values computed using an initialization value would be treated separately from the encrypted random number sent to the POS device, or that Johnson’s tag ID would be replaced with Walker’s single-use number. *Compare* Pet. 49–50, with PO Resp. 29. Instead, Petitioner contends that, in its combination, Johnson’s tag 100 would receive a random number from POS device 200, encrypt that random number using its sequence number (similar to how Walker encrypts a nonce with its IV), concatenate the encrypted random number with the tag ID, and send the result to the POS device. Pet. 49–50 (“As combined with Walker, Johnson’s tag would generate the **ECRN** (i.e., an *authentication tag*) by encrypting the **challenge random number CRN** received from the point-of sale terminal (i.e., *a random number . . . received from the RFID reader*) using the main tag key, analogous to Walker’s private key, and a **current sequence number, analogous to Walker’s initialization variable** (i.e., a *counter value*) and then concatenating this result with all or part of the **tag ID** (i.e., *the transaction device identifier*).”); Reply 15 (“In combination with Walker’s teachings, Johnson would encrypt the CRN received from the point-of-sale terminal (as opposed to a fixed nonce) with a current sequence number (analogous to the initialization variable) and the tag key (analogous to Walker’s private key) and concatenate the result with all or part of the

user's tag ID (which, like Walker's account number, is the user's account information)."). Patent Owner's argument, which does not correctly characterize Petitioner's combination, is misplaced and unpersuasive.

Moreover, to the extent that Patent Owner argues that a skilled artisan would have combined Johnson and Walker in the manner outlined in its Response, rather than as Petitioner asserts in the Petition, Patent Owner does not present any evidence to support such a position. Rather, Patent Owner presents only attorney argument, which is unpersuasive in light of Petitioner's reasoning and expert testimony.

Patent Owner also argues that

[i]n Johnson, the current sequence number, which Petitioner alleges would somehow in a Johnson-Walker combination be used to produce an encryption result, is *never* used for such a purpose nor is any such use suggested. Instead, the current sequence number is used as a check to ensure commands issued to the tag are not inadvertently repeated.

Sur-reply 19 (internal citation omitted); *see also id.* at 20 ("Johnson's sequence number is used not to create a payload for transmission to an interrogator (as is Walker's initialization variable), but instead to compare with commands received from the interrogator."). Patent Owner also argues that "the encrypted payload produced by Johnson is encrypted using a key installed in the tag at the time of its manufacture, and not one that is periodically updated by a counter or otherwise." *Id.* at 20–21. Petitioner, however, does not contend that Johnson describes its sequence number as used in encryption. Rather, Petitioner argues that Walker's teaching of using its initialization value in encryption to prevent replay attacks would have motivated a skilled artisan to use Johnson's sequence number in a similar manner. Pet. 50–51. Patent Owner's argument, which attacks Johnson

individually without considering Petitioner’s proposed combination, is unpersuasive. *See In re Keller*, 642 F.2d 413, 426 (CCPA 1981) (“[O]ne cannot show non-obviousness by attacking references individually where, as here, the rejections are based on combinations of references.”).

Petitioner argues that a skilled artisan would have had a reasonable expectation of success because the systems of Johnson and Walker are similar and no new information or hardware would be necessary to implement Walker’s encryption techniques in Johnson’s system. Pet. 51–52. Mr. McNair testifies that a skilled artisan “would have expected the combination to require only minor modifications in software.” Ex. 1015 ¶ 75. Petitioner argues that Johnson’s issuer would have had all the necessary variables to decrypt the information received from the tag and authorize the transaction. Pet. 52 (citing Ex. 1015 ¶ 76).

Patent Owner responds that “[t]he proposed modification of Johnson according to the teachings of Walker would have a person of ordinary skill in the art modify not only the purpose of the sequence number but also the very key used to perform the encryption of the payload to be returned to the interrogator,” and that “[m]odifying a key in that fashion would not only impact the tag, but also the host used to authenticate the tag because now the host would need to have some means of tracking modifications to the encryption key.” Sur-reply 21. Patent Owner offers no evidence in support of this attorney argument.

Walker, however, does not describe modifying a key, and Petitioner does not contend that keys would be modified in its combination. Rather, Walker’s “nonce is encrypted using the user’s private key K and the IV. Thus, $C = E_K(N, IV)$.” Ex. 1012, 8:13–16. At Walker’s host, “the processor

retrieves the card holder's private key K in the private key database 412," and "[t]he private key K then is used to decrypt the encrypted nonce (step 922). This recovers the original nonce N : $N=D_K(C, IV)$." *Id.* at 8:55–60. In Petitioner's proposed combination,

applying Walker's encryption technique to the CRN received from the POS device in Johnson's system would yield an encrypted code that is generated using a key, a current sequence number, and concatenated the user's tag ID. In other words, the ECRN would be generated using the Walker's technique and information that Johnson's tag already tracks.

Reply 15. As to authenticating the tag, Mr. McNair testifies

because Johnson's POS device forwards both the unencrypted challenge random number and the tag ID to the issuer, all of the necessary variables for decryption would still be in the issuer's possession, and therefore, a [person of ordinary skill in the art] would expect the resulting operation to enable Johnson's issuer to authorize a user without compromising their information. Therefore, in the proposed combination, Johnson's host would still reconstruct the original CRN or decrypt the ECRN to recover the CRN, a [person of ordinary skill in the art] would have appreciated that it is still the CRN (i.e., the *random number*) that is transmitted in encrypted form (i.e., the ECRN), just using Walker's teaching of using an initialization variable (i.e., Johnson's current sequence number) as part of the encryption process.

Ex. 1015 ¶ 76.

We credit Mr. McNair's testimony and agree with Petitioner that the modifications it proposes would have required only straightforward and minor software modifications and, therefore, we find that a skilled artisan would have had a reasonable likelihood of success in combining the teachings of Johnson and Walker.

Claim 2 depends from claim 1 and “further compris[es] transmitting unencrypted data, the counter value, and the random number to the RFID reader.” Petitioner contends that Johnson teaches transmitting an unencrypted tag ID, corresponding to “unencrypted data.” Pet. 55–56 (citing Ex. 1011, 3:15–18, 10:19–22, 10:53–56). As to transmitting the “counter value,” Petitioner contends that “Johnson discloses sending the current sequence number to the POS device (i.e., RFID reader) so that the POS device may ‘prevent a command or operation from accidentally being replicated.’” *Id.* quoting (Ex. 1011, 11:47–52). Petitioner further contends that Johnson’s ECRN, corresponding to “*the random number*,” is sent to the POS device. *Id.* (citing Ex. 1011, 10:19–22, 15:41–51, 16:1–2). Patent Owner does not contest Petitioner’s allegations as to claim 2, other than to incorporate its arguments as to claim 1. PO Resp. 30. Based on Petitioner’s evidence, we find that the combination of Johnson and Walker teaches the additional limitation of claim 2.

Claim 4 depends from claim 1 and adds “wherein the counter value is incremented a predetermined amount.” Petitioner argues that Johnson describes incrementing its sequence number by one. Pet. 56–57 (citing Ex. 1011, 11:54–60). Similarly, Petitioner argues, Walker describes incrementing its IV by one. *Id.* at 57 (citing Ex. 1012, 8:27–30 (“ $IV=IV+1$ ”). Patent Owner does not contest Petitioner’s allegations as to claim 4, other than to incorporate its arguments as to claim 1. PO Resp. 30. We agree with Petitioner and find that Johnson and Walker teach incrementing a counter value by a predetermined amount, e.g., by one.

In sum, as detailed above, a combination of Johnson and Walker teaches each limitation of claims 1, 2, and 4. A skilled artisan would have

had reasons, with rational underpinning, to combine the teachings of Johnson and Walker. Patent Owner does not argue or introduce evidence of objective indicia of nonobviousness. Upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 1, 2, and 4 would have been obvious over Johnson and Walker.

D. Grounds 4–6: Obviousness of Claims 1, 2, and 4 over Johnson, Walker, and Davis; Obviousness of Claims 1, 2, and 4 over Johnson, Walker, and Nerlikar; Obviousness of Claims 1, 2, and 4 over Johnson, Walker, Davis, and Nerlikar

According to Petitioner, “Davis is cited for its characterization of the component that tracks the number of transactions as a ‘counter,’ as in limitation[] 1.1 . . . and Claim 2, that is incremented by a predetermined amount for each transaction, as is applicable to limitation 1.3 and Claim 4.” Pet. 61. Patent Owner, however, does not contest that Johnson’s sequence number is a counter value. Thus, we need not reach whether a person of ordinary skill in the art also would have looked to Davis for a teaching of a counter value.

As to Nerlikar, Petitioner argues that

Johnson uses language consistent with RFID terminology, such as “tag” and “interrogator,” which a [person of ordinary skill in the art] would have appreciated are terms of art commonly used in referring to components of RFID systems. However, to the extent this is not sufficient to disclose the claimed RFID device and RFID reader, Nerlikar confirms the use of RFID tags and readers, including tags capable of encrypting data, and explains that such were applicable in the context of banking transactions.

Pet. 65 (internal citations omitted). Patent Owner, however, does not contest that Johnson teaches an RFID transaction device and RFID reader. Thus, we need not reach whether a person of ordinary skill in the art also would have

looked to Nerlikar for a teaching of an RFID transaction device and RFID reader.

Because Petitioner has shown, by a preponderance of the evidence, that claims 1, 2, and 4 would have been obvious over Johnson and Walker, we do not reach whether these claims also would have been obvious over Johnson, Walker, and Davis; Johnson, Walker, and Nerlikar; and Johnson, Walker, Davis, and Nerlikar.

III. CLAIMS 6 AND 7

Petitioner challenged claims 6 and 7 in the Petition. Pet. 11. On January 21, 2022, Patent Owner filed a disclaimer disclaiming claims 6 and 7. Ex. 2001. We did not institute an *inter partes* review of claims 6 and 7. Inst. Dec. 2 (citing 37 C.F.R. § 42.107(e); *Intuitive Surgical*, Paper 7 at 2 n.1, 9–10).

Nevertheless, Petitioner argues that we should consider Patent Owner's disclaimer as a request for adverse judgement under 37 C.F.R. § 42.73(b) and enter judgement against claims 6 and 7 in this Decision. Reply 13, 23. Petitioner argues that, under *Unified Patents, LLC v. Arsus, LLC*, IPR2020-00948, Paper 20 (PTAB Jan. 27, 2021), we do not lose subject matter jurisdiction over disclaimed claims. *Id.* at 13.

Patent Owner responds that *Arsus* is inapposite because, in that case, the patent owner had filed a disclaimer after institution of an *inter partes* review. Sur-reply 17. According to Patent Owner, because claims 6 and 7 were disclaimed before institution, we had no jurisdiction to consider or address them in the Final Written Decision. *Id.* (citing *Intuitive Surgical*, at 2 n.1, 9–10).

Our rules are clear. “The patent owner may file a statutory disclaimer under 35 U.S.C. 253(a) in compliance with § 1.321(a) of this chapter, disclaiming one or more claims in the patent. No *inter partes* review will be instituted based on disclaimed claims.” 37 C.F.R. § 42.107(e); *see also Intuitive Surgical*, at 10 (“[W]e treat claim 23 as having never been part of the ’969 patent, and Petitioner cannot seek *inter partes* review of that claim.”). Thus, we were not permitted to, and did not, institute an *inter partes* review of claims 6 and 7. Rule 42.73(b) and *Arsus* address the disclaimer of claims after institution, and, thus, are not pertinent to the facts of this proceeding. Accordingly, this Final Written Decision addresses only those claims on which we instituted an *inter partes* review, which do not include claims 6 and 7.

IV. PATENT OWNER’S MOTION TO EXCLUDE

Patent Owner moves to exclude Exhibit 1029 and those portions of Exhibit 1028 (Mr. McNair’s Supplemental Declaration) that cite to Exhibit 1029. Mot. Exclude 1. Because we do not rely on Exhibit 1029 or any of Mr. McNair’s testimony that cites to Exhibit 1029, we dismiss Patent Owner’s Motion to Exclude as moot.

V. CONCLUSION⁹

Petitioner has shown by a preponderance of the evidence that claim 1 is anticipated by Wankmeuller; claim 4 would have been obvious over Wankmueller; and claims 1, 2, and 4 would have been obvious of Johnson and Walker. Patent Owner's Motion to Exclude is dismissed as moot.

In summary:

Claims	35 U.S.C. §	Reference(s)/ Basis	Claims Shown Unpatentable	Claims Not shown Unpatentable
1	102	Wankmueller	1	
1, 4	103(a)	Wankmueller	4	
1, 2, 4	103(a)	Johnson, Walker	1, 2, 4	
1, 2, 4	103(a)	Johnson, Walker, Davis ¹⁰		
1, 2, 4	103(a)	Johnson, Walker, Nerlikar		
1, 2, 4	103(a)	Johnson, Walker, Davis, Nerlikar		
Overall Outcome			1, 2, 4	

⁹ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

¹⁰ As noted above, we do not reach this ground and the remaining two grounds because the previous grounds are dispositive of all the challenged claims.

VI. ORDER

In consideration of the foregoing, it is hereby:

ORDERED, based on a preponderance of the evidence, that claims 1, 2, and 4 are unpatentable;

FURTHER ORDERED that Petitioner's Motion to Exclude (Paper 18) is *dismissed as moot*;

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

IPR2022-00024
Patent 8,066,181 B2

For PETITIONER:

Michelle Aspen
Roshan Mansinghani
UNIFIED PATENTS, LLC
michelle@unifiedpatents.com
roshan@unifiedpatents.com

For PATENT OWNER:

Tarek N. Fahmi
Jonathan Tsao
ASCENDA LAW GROUP, PC
tarek.fahmi@ascendalaw.com
jonathan.tsao@ascendalaw.com