

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SQUARE, INC.,
Petitioner,

v.

4361423 CANADA INC.,
Patent Owner.

IPR2019-01651
Patent 9,443,239 B2

Before JAMESON LEE, ROBERT WEINSCHENK, and
KEVIN C. TROCK, *Administrative Patent Judges*.

LEE, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

We have authority to hear this *inter partes* review under 35 U.S.C. § 6. This Final Written Decision issues pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. We determine that Square, Inc. (“Petitioner”) has proved by a preponderance of the evidence that claims 1–6 of U.S. Patent 9,443,239 B2 (Ex. 1001, “the ’239 patent”) are unpatentable. *See* 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d).

A. *Background*

Petitioner filed a Petition for *inter partes* review of claims 1–6 (“challenged claims”) of the ’239 patent. Paper 2 (“Pet.”). 4361423 Canada Inc. (“Patent Owner”) filed a Preliminary Response. Paper 8. We instituted review on May 8, 2020. Paper 9 (“Decision on Institution”). Patent Owner filed a Patent Owner Response. Paper 22 (“PO Response”). Petitioner filed a Reply. Paper 25 (“Reply”). Patent Owner filed a Sur-Reply. Paper 27 (“Sur-Reply”). Oral hearing was consolidated with the oral hearings in IPR2019-01652, IPR2019-01653, and IPR2019-01654 (Paper 30), and was held on February 10, 2021. A copy of the hearing transcript has been entered into the record as Paper 34 (“Tr.”).

B. *Real Parties-in-Interest*

Each party identifies itself as the only real party in interest. Pet. 1; Paper 4, 2.

C. *Related Matters*

The parties indicate the ’239 patent is the subject of: *4361423 Canada Inc. v. Square, Inc.*, No. 4:19-cv-04311 (N.D. Cal.). Pet. 1; Paper 4, 2. Petitioner indicates that related patents are the subject of other petitions for *inter partes* review filed by Petitioner in IPR2019-01625, IPR2019-01626,

IPR2019-01627, IPR2019-01628, IPR2019-01629, IPR2019-01630,
IPR2019-01649, IPR2019-01650, IPR2019-01652, IPR2019-01653,
IPR2019-01654. Pet. 2–3.

D. The '239 Patent

The '239 patent relates to an apparatus and system “for commercial transactions using a transaction card via a communication device in audio communication with a remote processor assembly.” Ex. 1001, 2:28–30. It is also related to a method “for commercial transactions using a transaction card via a communication device.” *Id.* at 2:31–33. Specifically, the '239 patent describes a transaction apparatus, such as a portable point of sale (“POS”) device, linked to a communication device, such as a mobile phone. *Id.* at 5:66–6:3; 6:13–16; 7:35–40. Figure 2 illustrates an embodiment of an assembly according to the '239 patent and is reproduced below.

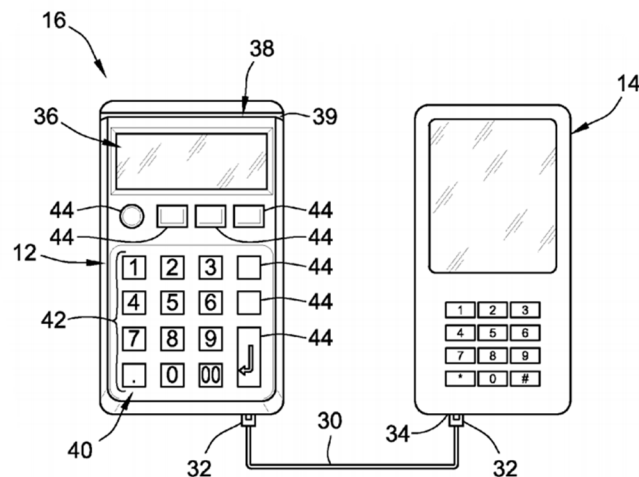


FIG. 2

Figure 2 shows a front view of a “transaction/communication assembly” according to an embodiment of the '239 patent. *Id.* at 5:36–38.

Assembly 16 in Figure 2 includes POS device 12 linked to a communication device in the form of mobile phone 14 via cable 30. *Id.* at 7:35–40. POS device 12 includes input device 38 such as card reader slot 39 for swiping or inserting transaction card 24 and capturing information from the transaction card. *Id.* at 7:44–51. The '239 patent explains that a user swipes card 24 through slot 39, and that analog information on magnetic strip 46 on card 24 is captured by an analog signal reader such as magnetic strip reader 52, and transferred to MCU 50 (microcontroller unit). *Id.* at 7:60–63, 8:8–11.

MCU 50 converts the information into an analog audio signal and transmits it via an analog communication link such as cable 30 to the communication device such as mobile phone 14. *Id.* at 8:17–23. Optionally, MCU 50 may encrypt the data. *Id.* at 8:14–16. Mobile phone 14 then transmits the information to transaction server 18 for processing. *Id.* at 8:21–15. The transaction server decrypts the received signal, converts it to a digital signal, and sends it to remote processor 20 for validation. *Id.* at 8:25–27. Remote processor 20 can reject or accept the requested transaction and send a message to transaction server 18 to indicate that determination. *Id.* at 8:28–33. Transaction server 18, after receiving the message from remote processor 20, converts the received information to an audio signal and sends it back to mobile phone 14. *Id.* at 8:34–37.

E. Illustrative Claims

Claims 1 and 4 are independent and reproduced below:

1. [Preamble] A portable smart card reader device for reading a smart card having recorded information stored on an integrated circuit incorporated into the card, the device comprising:

- [1.A] A sensor for reading said recorded information stored on said integrated circuit incorporated into said card;
- [1.B] a controller coupled to said sensor for converting the recorded information stored on said integrated circuit into an encrypted signal indicative of the recorded information, and
- [1.C] a communication link for coupling said portable smart card reader device to a mobile communication device for the transmission of said encrypted signal indicative of the recorded information therebetween;
- [1.D.1] wherein when said sensor reads the recorded information stored on said integrated circuit, said controller converts the recorded information read by said sensor into said encrypted signal and
- [1.D.2] transmits said encrypted signal via said communication link to said mobile communication device; and
- [1.E] said mobile communication device transmits the encrypted signal indicative of the recorded information to a remote transaction server for processing a commercial transaction.

Id. at 12:7–29 (bracketed section headings added to correspond to Petitioner’s claim listing (Ex. 1002)).

4. [Preamble] A method for reading a smart card having recorded information stored on an integrated circuit incorporated into the card, the method comprising the steps of:

- [4.A] providing a portable card reader device comprising a sensor for reading the recorded information stored on the integrated circuit,
- [4.B] a controller coupled to said sensor for converting the recorded information into an encrypted signal indicative of the recorded information stored on said integrated circuit incorporated

- [4.C] and a communication link for coupling said portable smart card reader device to a mobile communication device;
- [4.D] wherein when said sensor reads the recorded information stored on the integrated circuit, said controller converts the recorded information read by said sensor into said encrypted signal and
- [4.E] transmits said encrypted signal via said communication link to said mobile communication device; and
- [4.F] providing said encrypted signal indicative of the recorded information stored on the integrated circuit to said mobile communication device for further processing by circuitry contained in said mobile communication device; and
- [4.G] said mobile communication device transmits the encrypted signal indicative of the recorded information to a remote transaction server for processing a commercial transaction.

Id. at 12:38–63 (bracketed section headings added to correspond to Petitioner’s claim listing (Ex. 1002)).

F. Evidence — Prior Art References and Declarations

Petitioner relies on the following prior art references and Declarations:

Evidence	Exhibit No.
Declaration of Michael Shamos (“Shamos Declaration”)	1003
U.S. Patent No. 6,234,389 B1, issued May 22, 2001 (“Valliani”)	1005
U.S. Patent Application Publication No. 2005/0236480 A1, published Oct. 27, 2005 (“Vrotsos”)	1006
U.S. Patent Application Publication No. 2006/0032905 A1, published Feb. 16, 2006 (“Bear”)	1007
Rebuttal Declaration of Michael Shamos (“Shamos Rebuttal Declaration”)	1017

Patent Owner relies on the Declaration of Ivan Zatkovich. Ex. 2004.

G. Asserted Grounds of Unpatentability

Petitioner asserts that the challenged claims are unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §¹	Basis
1–6	103	Valliani, Vrotsos
1–6	103	Bear, Vrotsos
1–6	103	Vrotsos

II. ANALYSIS

A. Principles of Law

To prevail in its challenge to Patent Owner’s claims, Petitioner must demonstrate by a preponderance of the evidence that the claims are unpatentable.² 35 U.S.C. § 316(e) (2018); 37 C.F.R. § 42.1(d). That burden never shifts to the patentee. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

A patent claim is unpatentable under 35 U.S.C. § 103 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

¹ The Leahy-Smith America Invents Act, Pub. L. No. 112–29, 125 Stat. 284, 287–88 (2011) (“AIA”), revised 35 U.S.C. §§ 102 and 103 effective March 16, 2013. Because the effective filing date of the ’239 patent is prior to March 16, 2013 (Ex. 1001, codes (22), (63)), we apply the pre-AIA version of § 103.

² The burden of showing something by a preponderance of the evidence requires the trier of fact to believe that the existence of a fact is more probable than its nonexistence before the trier of fact may find in favor of the party who carries the burden. *Concrete Pipe & Prods. of Cal., Inc. v. Constr. Laborers Pension Tr. for S. Cal.*, 508 U.S. 602, 622 (1993).

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 ordinary skill in the art; and (4) when in evidence, objective evidence of nonobviousness.³ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

B. Level of Ordinary Skill in the Art

Petitioner asserts that a person of ordinary skill in the art (“POSITA”), at the time the ’239 patent was filed, would have been a person with “a bachelor’s degree in electrical engineering, computer science, or an analogous field, or equivalent experience,” and would have had “at least two years of relevant experience and familiarity with the fields of embedded system implementation, mobile communications, electronic payments and encryption.” Pet. 13 (citing Ex. 1003 ¶¶ 17–25).

Patent Owner’s expert, Ivan Zatkovich, states the level slightly differently:

The POSITA may have a Bachelor of Science in Electrical Engineering or Computer Engineering, or the equivalent and have at least one to two years of relevant experience in the fields of embedded systems and mobile communication device interfaces, or otherwise equivalent industry experience in the relevant field.

Ex. 2004 ¶ 14. The articulations are essentially the same, except that Petitioner refers to at least two years of experience and Patent Owner’s

³ Patent Owner has not presented any objective evidence of nonobviousness or any argument in that regard.

expert refers to at least one to two years of experience. That distinction has not been shown by either party as making a difference in the outcome of this case. Neither party has objected to the other party's characterization of the level of ordinary skill in the art.

We are more persuaded by Petitioner's articulation. Petitioner does not use the tentative language "may have" as Patent Owner's expert does. Also, Petitioner's articulation of the pertinent fields of experience is more specific than that of Patent Owner. We adopt Petitioner's articulation of the level of ordinary skill in the art, but delete the qualifier "at least" for the level of practical experience, to keep that level from being vague and extending to a range that corresponds to the level of skill of an expert. Also, we delete the reference to "or equivalent experience" within the description of the level of education, to keep education level from being confused with practical experience, and because Petitioner separately articulates the appropriate level of experience. Thus, we regard the level of ordinary skill as being at the level of a person with "a Bachelor of Science in Electrical Engineering or Computer Engineering, or the equivalent" and "one to two years of relevant experience in the fields of embedded systems and mobile communication device interfaces, or otherwise equivalent industry experience in the relevant field."⁴

C. Claim Construction

For petitions filed on or after November 13, 2018, we use 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

⁴ Our decision in this case would be no different had Patent Owner's articulation of the level of ordinary skill been adopted.

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. *See* 37 C.F.R. § 42.100 (2019). The Petition here was filed on September 30, 2019. Paper 2. We apply the claim construction standard from *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

Claim terms are generally given their ordinary and customary meaning as would be understood by one with ordinary skill in the art in the context of the specification, the prosecution history, other claims, and even extrinsic evidence including expert and inventor testimony, dictionaries, and learned treatises, although extrinsic evidence is less significant than the intrinsic record. *Phillips*, 415 F.3d at 1312–17. Usually, the specification is dispositive, and it is the single best guide to the meaning of a disputed term. *Id.* at 1315.

The specification may reveal a special definition given to a claim term by the patentee, or the specification or prosecution history may reveal an intentional disclaimer or disavowal of claim scope by the inventor. *Id.* at 1316. If an inventor acts as his or her own lexicographer, the definition must be set forth in the specification with reasonable clarity, deliberateness, and precision. *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1249 (Fed. Cir. 1998). The disavowal of claim scope, if any, can be effectuated by language in the specification or the prosecution history. *Poly-America, L.P. v. API Indus., Inc.*, 839 F.3d 1131, 1136 (Fed. Cir. 2016). “In either case, the standard for disavowal is exacting, requiring clear and unequivocal evidence that the claimed invention includes or does not include a particular feature.” *Id.*

Only those claim terms that are in controversy need to be construed, and only to the extent necessary to resolve the controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

In neither the Petition nor the Patent Owner Response has either party proposed an express full construction for any claim term. However, the arguments of the parties reflect a certain reading of the claim language. To the extent necessary to reach a decision, we discuss a party's proposed reading in our analysis of each party's arguments below.

D. Obviousness of Claims 1–6 over Valliani and Vrotsos

1. Overview of Valliani

Valliani relates to portable computer systems including personal digital assistants (“PDA”) for performing point of sale transactions. Ex. 1005, 1:16–20. Specifically, Valliani discloses a PCMCIA-compliant generic laptop computer or PDA device “with an add-on module that provides point of sale functionality.” *Id.* at 2:41–44. “[T]he module converts the device to a portable inexpensive point of sale transaction terminal.” *Id.* at 2:45–47. The module includes a card reader and has a housing member which slides into the PCMCIA slot of the computer or PDA. *Id.* at 2:48–52. The computer or PDA executes software which allows the device to read and process information read by the module. *Id.* at 2:52–55.

Valliani describes that typically payment for a transaction is made with a credit card that includes a magnetic stripe carrying the cardholder's information, and such cards are read by a module with a magnetic stripe reader unit. *Id.* at 2:56–60. Valliani further describes that transactions may

involve a smartcard instead, in which memory internal to the card retains data, and such cards are read by a module having a *smartcard reader/writer unit*. *Id.* at 2:62–65. Valliani states that when equipped with an appropriate module, the computer or PDA device “becomes a portable point of sale transaction terminal.” *Id.* at 2:65–67.

Figure 1 of Valliani is a block diagram of Valliani’s system and is reproduced below:

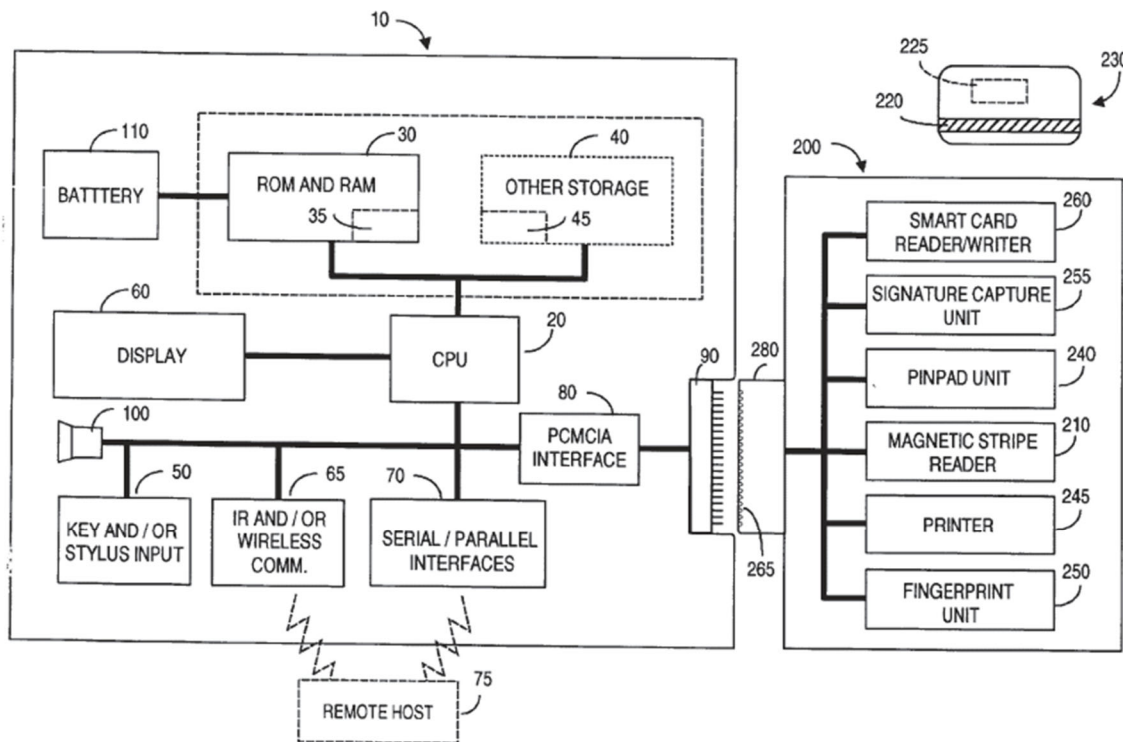


FIG. 1

Figure 1 is a block diagram of a computer or PDA combined with a module to implement a point of sale transaction terminal system. *Id.* at 3:17–20.

Device 10 in Figure 1 shows a generic portable computer or PDA device. *Id.* at 4:34–37. The right-hand portion of Figure 1 shows module 200 the housing of which includes projecting snout-like member 280 that includes connector edge 265 which slides into and matingly engages slot socket 90 in device 10. *Id.* at 4:51–54. Module 200 includes magnetic stripe

reader 210 that reads information encoded and stored on magnetic stripe 220 on credit card 230, and optionally may provide “a pinpad unit 240, a printer unit 245, a fingerprint reader unit 250, a signature capture unit and/or virtual pinpad unit 255, and/or a *smartcard reader unit 260*.”⁵ *Id.* at 4:41–44 (emphasis added). “Smartcard reader unit 260 is utilized if card 230 is a smartcard storing data in memory 225.” *Id.* at 4:45–47.

Figure 2 of Valliani illustrates an embodiment in which only a magnetic strip reader is provided in module 200. *Id.* at 5:1–2. Figure 3 of Valliani illustrates an embodiment including both a magnetic stripe reader and a pinpad unit. *Id.* at 6:16–18. Valliani describes that typically, information embedded in magnetic stripe 220 of the card includes at least the card owner’s credit account company and account number, and owner identification information. *Id.* at 5:25–28. Valliani also describes that software routines, either provided through module 200 or made available through another source, would be loaded into device 10. *Id.* at 6:4–7.

Regarding such software, Valliani specifically states:

These routines would include point of sale software and software driver(s) for the PCMCIA-implemented magnetic stripe reader 210 and can further include driver(s) for pinpad unit 240, printer unit 245, fingerprint unit 250, signature capture unit 255, and smartcard reader/writer unit 260. Such routines can also provide DES encryption, signature capture and signature compression, among other useful functions. These routines would be executed by central processor unit 20 within device 10. *Id.* at 6:8–16.

⁵ Sometimes Valliani refers to “smartcard reader/writer unit 260” and not “smart card reader unit 260.” Ex. 1005, 6:12, 8:9. For consistency, we refer to unit 260 as smart card reader/writer unit 260 as shown in Figure 1 above.

Device 10 communicates with host 75 through port 75, a modem, and telephone lines, or such communication may be by infrared or wireless telephony, “which further promotes portability.” *Id.* at 6:47–50. If a card is stolen, an individual attempting to transact business with module 200 will be unable to have a PIN confirmed by the remote host system communicating with device 10. *Id.* at 6:49–53. Absent such confirmation, for example as shown on a display in device 10, the transaction would not be allowed. *Id.* at 6:54–57.

2. Overview of *Vrotsos*

Vrotsos is directed to a system and method for transmitting transaction data over a wireless communication network. Ex. 1006 ¶ 26. In an embodiment, the system is used to transmit credit card information during a point-of-sale transaction. *Id.* An “attachment” is coupled to a wireless communication device having a transceiver for establishing a communication link with a wireless communication network. *Id.* *Vrotsos* states that the “attachment” may also be referred to “as a peripheral or peripheral device.” *Id.*

The “attachment” includes a processor and an input device. *Id.* When the attachment device receives data from the input device, it transmits that data over the wireless communication network using the transceiver in the wireless communication device. *Id.* *Vrotsos* describes that the input device may be a magnetic strip reader or a smartcard reader. *Id.* ¶ 28. In one embodiment, the attachment includes a combined magnetic stripe reader and smartcard reader. *Id.* ¶ 41. In that embodiment, “[a] card 51 having a magnetic stripe 52 and/or smartchip 53 may be inserted into the slot 22 [of the attachment].” *Id.* The slot has a shallow channel portion suitable for reading a magnetic stripe on a card, and also a deeper channel portion. *Id.*

Vrotsos describes as follows: “A smartcard read/write head may be positioned within a surface of the deeper channel portion 55 of the slot 22 so that information may be read from or written to the smartchip 53 when the card is positioned within the deeper channel portion 55.” *Id.*

When input information is received at the input device, it is sent to a processor in the attachment device for processing and transmission to the remote computer through the communication device. *Id.* ¶ 26. The remote computer may process the received data and generate a response to be sent back to the processor in the attachment device. *Id.*

Figure 10 is a block diagram of the system of Vrotsos and is reproduced below:

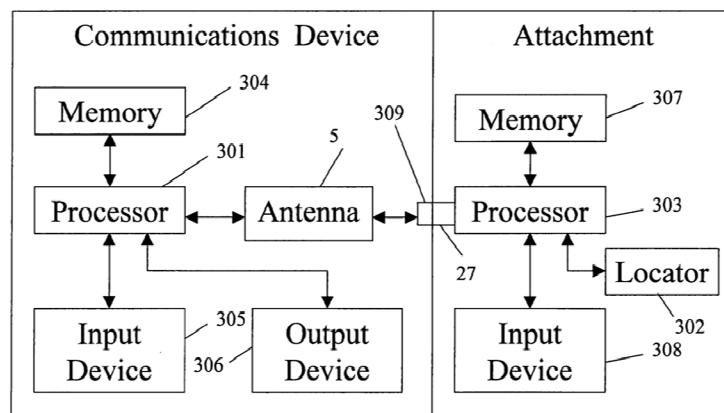


FIGURE
10

Figure 10 illustrates the components of the wireless communication device and attachment (peripheral device) disclosed in Vrotsos. *Id.* ¶ 23. The attachment includes processor 303, memory 307, and input device 308. *Id.* ¶ 75. Processor 303 receives input information from input device 308 and processes that information to generate data for transmission to a remote computer via antenna 5 of the communication device. *Id.* Vrotsos also describes that processor 303 operates to encrypt the input information. *Id.*

3. *Independent Claim 1*

a) *Preamble*

Claim 1's preamble recites "[a] portable smart card reader device for reading a smart card having recorded information stored on an integrated circuit incorporated into the card." Ex. 1001, 12:7–9. Petitioner identifies Valliani's module 200 as the portable smart card reader device. Pet. 14–15. Petitioner cites to Valliani's disclosure which states that smart card reader/writer unit 260 "is utilized if card 230 is a smartcard storing data in memory 225." *Id.* at 14 (citing Ex. 1005, 4:45–46). Petitioner explains that information stored in memory 225 of card 230, such as user account number, maximum dollar limit of the account, user identification, and a PIN, corresponds to recorded information stored on integrated circuit incorporated into the smart card. *Id.* at 14–15 (citing Ex. 1003 ¶¶ C1–7; Ex. 1005, 6:27–29, 7:62–64).⁶ Valliani states that "a card owner's PIN is not stored, encrypted or otherwise, in magnetic stripe(s) 220 but may be stored in memory 225." Ex. 1005, 6:27–29. Michael Shamos, Petitioner's declarant, identifies Valliani's memory 225 as in integrated circuit. Ex. 1003 ¶ C1. Petitioner also cites to the following text in Valliani: "Such point of sale transaction systems should be portable, small in size, inexpensive, yet perform the necessary functions required to securely transact business." Pet. 15 (citing Ex. 1005, 2:33–36).

To the extent Patent Owner asserts an argument with regard to the preamble, it is merged with its argument directed to limitation [1.A] discussed below and related to a sensor for reading recorded information

⁶ The letter "C" in the citation to paragraph numbers in Ex. 1003 designates the paragraph numbers within Appendix C of Exhibit 103.

stored on an integrated circuit incorporated into the card. Notwithstanding Patent Owner's argument, discussed below in the context of limitation [1.A], Petitioner's assertion is supported by the cited evidence and we are persuaded that Valliani discloses "[a] portable smart card reader device for reading a smart card having recorded information stored on an integrated circuit incorporated into the card." We need not determine whether this preamble is limiting.

b) *Limitation [1.A] — a sensor*

Claim 1 further recites that the portable smart card reader device comprises "a sensor for reading said recorded information stored on said integrated circuit incorporated into said card." Ex. 1001, 12:10–11. Petitioner asserts that Valliani's smart card reader/writer unit 260 within module 200 "includes a *sensor* that reads a smart card that has *recorded information stored on an integrated circuit incorporated into said card.*" Pet. 16–17 (citing Ex. 1005, 7:61–8:6). Petitioner explains that data stored in the memory of the smart card corresponds "to *recorded information stored on said integrated circuit incorporated into said card.*" *Id.* at 17 (citing Ex. 1003 ¶¶ C12–14). Further, as noted above in the context of the preamble, Petitioner cites to Valliani's disclosure which states that smart card reader/writer unit 260 "is utilized if card 230 is a smartcard storing data in memory 225." *Id.* at 14 (citing Ex. 1005, 4:45–46). Petitioner's declarant, Michael Shamos, testifies that Valliani's smart card reader/writer 260 is the claimed sensor, and is used for reading card data stored in memory 225. Ex. 1003 ¶ C12 (citing Ex. 1005, 7:61–8:6, 4:45–47). Valliani describes:

Memory 225 within smartcard 230 can store substantially more data than can one or even three magnetic stripes. An

appropriate smartcard 230 may store user account number, present maximum dollar limit of the account, user identification as well as preferably encrypted PIN data. Generally, when a user purchases a smartcard 230, memory 225 is programmed to store the dollar value of the card, e.g., the value of the card. In a preferred embodiment, smartcard reader/writer unit 260 can both read and write to memory 225. Thus, if prior to the present transaction memory 225 stored \$1,000 as the present card balance and if the present transaction is \$200 debit, unit 260 can so debit memory 225 such that the new present card balance is \$800.

Ex. 1005, 7:61–8:6.

Notwithstanding Patent Owner’s arguments to the contrary, discussed below, Petitioner’s assertions are fully supported by the cited evidence and we are persuaded that Valliani’s module 200 includes “a sensor for reading said recorded information stored on said integrated circuit incorporated into said card.” That sensor is within smart card reader/writer 260. Further, smart card reader/writer 260 itself may be deemed the sensor.

Patent Owner asserts that “[a]lthough Petitioner identifies Valliani’s mention of a ‘smart card’ reader, Petitioner does not identify any component of Valliani that might qualify as the claimed sensor.” PO Resp. 12. That is incorrect. Petitioner’s declarant, Michael Shamos, testifies that Valliani’s smart card reader/writer 260 is the claimed sensor, and is used for reading card data stored in memory 225. Ex. 1003 ¶ C12 (citing Ex. 1005, 7:61–8:6, 4:45–47). Even if the sensor is contained within Valliani’s smart card reader/writer 260, the Petition states that Valliani’s smart card reader/writer unit 260 within module 200 “includes a *sensor* that reads a smart card that has *recorded information stored on an integrated circuit incorporated into said card.*” Pet. 16–17 (citing Ex. 1005, 7:61–8:6).

Patent Owner argues:

Nothing in the cited passage from Valliani, however, mentions any kind of sensor. In fact, nowhere does Valliani or Petitioner identify any component of Valliani that could qualify as the claimed sensor. Instead, Valliani references the unit 210 as being able to sense information from the card. Unit 210, however, is a magnetic stripe reader and not a smart card reader. Valliani proves as much when it specifies that “as magnetic stripe 220 moves through slot 290, a read head associated with **unit 210 senses magnetic charge embedded in stripe(s) 220**.”

PO Resp. 13.

Patent Owner has misread the Petition. Petitioner does not rely on magnetic stripe reader 210 either as the sensor or as containing the sensor, but, rather, on smart card reader/writer 260 as either being the sensor or containing the sensor. Ex. 1003 ¶ C12; Pet. 16–17. Petitioner’s declarant, Michael Shamos, testifies persuasively in his rebuttal declaration:

Petitioner and I never asserted that electronic[s] 210 possessed the ability to access information from the integrated circuit, but it is clear that smart card reader/writer 260 (the smartcard *sensor*) has that ability, or it would not be able to function as a smart card reader/writer. Patent Owner then goes on to denigrate the capabilities of “electronics 210,” but electronics 210 is not the basis of Petitioner’s sensor argument.

Ex. 1017 ¶ 15.

Although it is true, as Patent Owner asserts, that Valliani nowhere mentions, literally, a “sensor,” Michael Shamos persuasively testifies that the claimed sensor “is precisely the unit in Valliani that senses and reads the smart card.” *Id.* ¶ 16. The law does not require that the prior art describe a claim limitation in *ipsis verbis* in order to meet it. *Cf. In re Lukach*, 442 F.2d 967, 969 (CCPA 1971) (“[T]he invention claimed does not have to be described in *ipsis verbis* in order to satisfy the description requirement of § 112.”). Patent Owner misdirects the issue by not addressing what in

Valliani is reading integrated circuit memory 225 on the smart card, and why smart card reader/writer 260 is not or does not include such a sensor.

To the extent Patent Owner also argues that Valliani does not provide a detailed disclosure of the specific structure of smart card reader/writer unit 260, no more specific disclosure is necessary to meet the sensor limitation. Only a generic sensor is claimed, not a specific sensor having a particular structure. Even the '239 patent itself does not provide detailed disclosure of the structure of the sensor that reads an integrated circuit memory on a card. Further, Patent Owner does not contend that one with ordinary skill in the art, given Valliani's disclosure of smart card reader/writer unit 260, would not have known how to construct such a sensor for reading an integrated circuit memory on a card. Michael Shamos has testified that sensors for reading recorded information on an integrated circuit memory of a smart card were well known to one with ordinary skill in the art in 2009. Ex. 1003 ¶ D29; Ex. 1017 ¶¶ 30, 34. Patent Owner's declarant, Ivan Zatkovich, does not contend otherwise. Even according to Patent Owner, at the time of the invention, there already were industry standards which "defined the methods for reading IC chips embedded in these types of smart cards." PO Resp. 12–13. We find that sensors for reading recorded information on an integrated circuit memory of a smart card were well known to one with ordinary skill in the art in 2009.

Alternatively, Petitioner asserts that to the extent that Valliani does not explicitly describe a sensor for reading recorded information stored on an integrated circuit incorporated into a card, it would have been obvious to one with ordinary skill in the art, in light of Vrotsos, to include such a sensor in Valliani. Pet. 17–19. Petitioner asserts as follows: "[T]o the extent that Valliani does not disclose the precise configuration of how its smartcard

reader/writer unit reads the smart card, Vrotsos discloses a specific configuration that provides the same function described by Valliani.” *Id.* at 19 (citing Ex. 1003 ¶ C22). Petitioner also explains that one with ordinary skill in the art would have known to look to Vrotsos for a specific implementation, because Vrotsos, like Valliani, “is *portable* and reads information stored on a credit card (Ex. 1006, ¶ 41), processes that information (*id.* ¶ 52), and transmits it to the phone (*id.* ¶ 43), which transmits the data to a remote computer to process the credit card information and facilitate the transaction (*id.* ¶ 53).” *Id.*

Petitioner further explains:

[U]sing a smartcard read/write head was known to read recorded information stored on said integrated circuit incorporated into said card. Thus, a POSITA applying Vrotsos’s teaching to Valliani would have expected to yield the predictable result of success. Specifically, applying a smartcard read/write head to Valliani’s smart card read/write unit 260 would have enabled the unit 260 to read the data encoded by the smartcard’s memory 225. Ex. 1006, ¶41. Ex. 1003, ¶C23.

Pet. 19.

Patent Owner asserts:

[A] POSITA would recognize that Vrotsos’s cryptic mention of a “smartcard read/write head” does not disclose a smart card reader capable of reading an integrated circuit at all, and certainly not at any level of detail that would teach how to integrate Vrotsos’s card reader into Valliani’s device. Ex. 2004, ¶¶35-36.

PO Resp. 26. The argument does not defeat or undermine Petitioner’s assertions. We address and reject a similar argument in Section II.E.1.b. We determine that the smartcard read/write head as described in Vrotsos is a “sensor for reading recorded information stored on an integrated circuit incorporated into a smart card.” As for the contention that there is

insufficient teaching on how to integrate Vrotsos's read/write head into Valliani's device, the contention is without persuasion. Petitioner simply proposes to implement Valliani's smart card reader/writer unit 260 with Vrotsos's smart card read/write head. Patent Owner has identified nothing complex to be coordinated or intermixed. The smart card reader/writer unit 260 is described in Valliani at a relatively high level that Petitioner's merely proposing to implement it with Vrotsos's smart card read/write head requires no additional detail for incorporating the read/write head.

Notwithstanding Patent Owner's arguments, discussed below, regarding lack of motivation to combine teachings, we find that Petitioner's reasoning is based on rational underpinning and supports the assertion that one with ordinary skill would have had sufficient reason and motivation to use Vrotsos's read/write head as Valliani's smart card reader/writer unit 260.

First, Patent Owner asserts that Petitioner's approach "is classic hindsight misadventure," for "saying that a POSITA would have been motivated to incorporate beneficial elements of the patent claims because, well, those elements would have been beneficial." PO Resp. 26. We do not find that Petitioner has engaged in such circular reasoning. Petitioner, instead, as we discussed above, articulated a reason why one with ordinary skill in the art would have known to use Vrotsos's smartcard read/write head as a specific implementation of Valliani's smart card reader/writer unit 260, i.e., because Valliani itself does not provide more detail on the specific implementation. Also, as discussed above, Petitioner reasoned that one with ordinary skill would have used Vrotsos's smartcard read/write head so that in Valliani's device information can be read from a smart card as Valliani describes. Such reasoning is not circular. Nor is it based on hindsight.

Second, Patent Owner argues that “a POSITA would understand that no aspects of Vrotsos’ converting or communicating data between its reader and cell phone (e.g., RS232 link) are compatible with Valliani’s reader and communication device (PCMCIA Bus). Ex. 2004, ¶¶94-101.” PO Resp. 27. According to Patent Owner, Valliani’s disclosure “mentions PCMCIA-compliance throughout,” and **“the central premise and, indeed, entire point** of Valliani is to develop a mobile POS device under the PCMCIA standard - not just a POS device that happens to use [] PCMCIA interface. Ex. 2004, ¶¶ 95–97.” *Id.* at 27–28. Patent Owner further observes: “Every figure [of Valliani] is described as disclosing a PCMCIA-compliant interface, and every described disclosed embodiment is described as being PCMCIA based.” *Id.* at 28. Based on the foregoing, Patent Owner argues:

Valliani teaches-away from any solution that does not utilize a PCMCIA interface. Ex. 2004, ¶¶95-101. Therefore, a POSITA would not consider combining Valliani with any reference that does not disclose a PCMCIA compatible solution. Ex. 2004, ¶¶95–101. And as mentioned above, no aspect of the Vrotsos reference is compatible with the PCMCIA standard. Ex. 2004, ¶¶95–101.

As an example of Vrotsos incompatibility, Valliani’s PCMCIA interface requires a 68 pin electrical connection using a parallel communication protocol. Vrotsos teaches a 4 pin RS-232 connection and a serial communication protocol. . . . Vrotsos neither mentions nor implies the use of any device standards or architecture, and none of its disclosed embodiments or figures appear to be PCMCIA-compliant. . . .

Because of the PCMCIA compliance requirements, any attempt to integrate Valliani’s PCMCIA interface with the Vrotsos card reader would require an overhaul to the Vrotsos card reader or any of Vrotsos’s components that would “convert information suitable for communication,” provide “communication link with” or “transmit data to” a mobile communication device. Ex. 2004, ¶¶95–101. In other words, to

combine almost any aspect of Vrotsos with Valliani would require significant overhaul of the Vrotsos design in order to comply with the limitations of the ‘239 claims. Ex. 2004, ¶¶101. Therefore, this is clearly an endeavor based on hindsight. *Id.*

PO Resp. 28–30.

The argument is misplaced, for several reasons. First and foremost is that Valliani’s smart card reader/writer 260, the sensor, has not been shown to operate according to PCMCIA standard or interface. The PCMCIA interface pertains to the connection between Valliani’s module 200 and PCMCIA-compliant device 10, i.e., the laptop or PDA. Ex. 1005, 3:50–65, Fig. 1. Patent Owner incorrectly states that “all 20 claims of Valliani require both a “PCMCIA-compliant card slot” and a “PCMCIA-compliant connector,” erroneously suggesting that reading from a smart card is also governed by PCMCIA. PO Resp. 28. No claim in Valliani refers to a “PCMCIA-compliant card slot” in the sense of a transaction card slot in the card reader. The claims refer to a “PCMCIA-compliant card slot connector” which is the interface between module 200 and laptop/PDA 10, consistent with Valliani’s disclosure. Further, the record does not support that the standard governing reading of smart cards is PCMCIA. Ivan Zatkovich testifies regarding Vrotsos’s card as follows: “As a card that requires physical connection to a reader, it would be the EMV type of card. As stated above, an EMV type card would require a sensor which could access the contact pad of the IC chip. The International Standard that applies to EMV cards is ISO 7816.” Ex. 2004 ¶ 37 (footnote omitted).

Second, Vrotsos does not teach away from using the PCMCIA standard or interface. It simply does not refer to it, which is not the same as “criticiz[ing], discredit[ing], or otherwise discourag[ing]” anything about a

PCMCIA standard or interface. *See In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004).

Third, Petitioner has not proposed direct bodily incorporation of the physical components of Vrotsos into Valliani, without appropriate and necessary adaptations. If, as Patent Owner asserts, Valliani is all about having a PCMCIA interface between module 200 and laptop/PDA 10, then one with ordinary skill in the art would have known, based on Valliani's disclosure, to implement a PCMCIA interface for whatever component is sourced from Vrotsos for incorporation into Valliani's system. Patent Owner has not asserted that it would have been beyond the skill level of one with ordinary skill in the art to add a PCMCIA interface to components sourced from Vrotsos that are relied on by Petitioner.

For the foregoing reasons, we are persuaded that Valliani's module 200 includes "a sensor for reading said recorded information stored on said integrated circuit incorporated into said card." Alternatively, we are persuaded that one with ordinary skill in the art would have known to use Vrotsos's smartcard read/write head in Valliani's smart card reader/writer 260, and thus the combined teachings of Valliani and Vrotsos account for the claimed sensor. Either position leads to satisfaction of limitation [1.A].

c) Limitation [1.B] — a controller

Claim 1 further recites that the portable smart card reader device comprises "a controller coupled to said sensor for converting the recorded information stored on said integrated circuit into an encrypted signal indicative of the recorded information." Ex. 1001, 12:12–15. Petitioner identifies "electronics 210" in Valliani as the claimed controller. Pet. 20. This "electronics 210" is the "electronics 210" referred to in the following description of Valliani: "For security reasons, a card owner's **PIN** is not

stored magnetically on stripe **220** but may be stored electronically in memory **225**. To promote security, electronics **210** provides any card **230**-provided **PIN** information to device **10** in encrypted form using only internally stored encryption keys.” Ex. 1005, 5:29–34. Electronics 210 is not Valliani’s magnetic stripe reader 210, because the PIN is not stored on a magnetic stripe. Petitioner’s declarant, Michael Shamos makes the distinction between electronics 210 and magnetic stripe reader 210 through his testimony that “[w]hether the [electronics 210] is located within the smart card reader/writer unit 260, the magnetic stripe reader unit 210 or some other unit within the module 200 is a decision choice [for a POSITA].” Ex. 1003 ¶ C31; see also *id.* ¶ 60.

Valliani does not specifically describe the location of its electronics 210. However, based on its description that electronics 210 “provides any card **230**-provided **PIN** information to device **10** in encrypted form using only internally stored encryption keys” (Ex. 1005, 5:29–34), it is implicit that electronics 210 is within module 200 and is coupled to smart card reader/writer 260. In that regard, Michael Shamos persuasively testifies:

Accordingly, Valliani discloses storing PIN data in memory 225 (the claimed integrated circuit) on a smart card 230. The smart card reader/writer 260 (the claimed sensor) reads the data from the memory 225 (4:45–47), and the electronics 210, which is coupled to the smart card reader/writer 260, converts that data into an encrypted signal indicative of the PIN data.

Ex. 1003 ¶ C30.

Notwithstanding Patent Owner’s arguments to the contrary, discussed below, we are persuaded that Valliani’s portable smart card reader device comprises “a controller coupled to said sensor for converting the recorded

information stored on said integrated circuit into an encrypted signal indicative of the recorded information.”

Patent Owner asserts that “Petitioner does not identify anything in Valliani capable of filling these roles [of the claimed controller].” PO Resp. 16. We disagree. Petitioner has identified “electronics 210” in a specific manner and with support from the testimony of Michael Shamos, as we discussed above.

Patent Owner asserts:

[T]he purported controller, “electronics 210,” is a component of the Valliani reader’s magstripe reader – not a reader for smart cards and specifically not having a controller coupled to a sensor for reading and converting recorded information stored on the integrated circuit of a smart card. There is no reason to believe that electronics 210 has the ability to even access information from the card’s integrated circuit, as discussed above or even has the characteristics of a controller. Ex. 2004, ¶¶ 46.

PO Resp. 17. We disagree that “electronics 210” as described in Valliani is a component of Valliani’s magnetic stripe reader 210 such that it does not read and convert information stored on the integrated circuit of a smart card. That position is expressly contradicted by Valliani’s disclosure that PIN information is not stored on the magnetic strip but is stored on the memory of a smart card, and that the purpose and usage of electronics 210 is to provide to device 10 card-provided **PIN** information in encrypted form using only internally stored encryption keys. Ex. 1005, 5:29–34.

Patent Owner and Patent Owner’s declarant, Ivan Zatkovich, misread Petitioner’s position. Mr. Zatkovich testifies: “Petitioner accuses the electronics in 210, which is the Magnetic stripe reader. The Magstripe reader 210 cannot access the integrated circuit on the card, therefore the magstripe reader 210 cannot be used for converting the data from the

integrated circuit.” Ex. 2004 ¶ 46. But Petitioner identified “electronics 210,” not “the electronics in 210,” and Petitioner’s declarant, Michael Shamos, made clear distinction between “electronics 210” and “magnetic stripe reader 210.” Pet. 20; Ex. 1003 ¶¶ C30–31.

We credit the testimony of Michael Shamos over that of Ivan Zatkovich. Ivan Zatkovich’s testimony is non-responsive to the position expressed by Petitioner and Michael Shamos. Also, as explained above, Petitioner’s position is more consistent with the express disclosure of Valliani, i.e., that “electronics 210” is to provide to device 10 card-provided PIN information in encrypted form using only internally stored encryption keys, and that PIN information is not stored on the magnetic strip but on the memory of a smart card. Ex. 1005, 5:29–34. Mr. Zatkovich does not explain how his reading is consistent with the express disclosure of Valliani.

Patent Owner argues that “‘electronics 210’ does not perform any kind of conversion or encryption of recorded information stored on the integrated circuit as required for the claimed controller.” PO Resp. 17. Patent Owner further asserts that the encryption must happen before the information is transmitted to the mobile communication device. *Id.* at 18. Both of these requirements have been adequately accounted for by Petitioner. Indeed, we reiterate that in Valliani, “electronics 210” is to provide to device 10, the mobile communication device, card-provided PIN information in encrypted form using only internally stored encryption keys, and that PIN information is not stored on the magnetic strip but on the memory of a smart card. Ex. 1005, 5:29–34.

Regarding characteristics of a “controller,” the cited paragraph of Ivan Zatkovich’s Declaration states nothing. Ex. 2004 ¶ 46. We find, however, the following testimony in paragraph 48:

A POSITA would also understand that in order to convert the card information retrieved from the card reader input device 38 to an encrypted signal for transmission it would require a microprocessor, microcontroller, or a controller with similar processing power. This is because the data signals from the magnetic stripe or Integrated Circuit of the payment card must be received and validated before being passed to the mobile communication device. For example, the data fields that would need validation include the Primary account number format (which is different for different card types), a check digit to identify data transmission errors, as well as a valid country code and service code.

Ex. 2004 ¶ 48. The testimony supports Petitioner's identification of "electronics 210" as a controller.

A patent specification need not describe what already is well known. Patent Owner does not purport to have invented a microprocessor or a microcontroller. The above-quoted testimony of Patent Owner's declarant, Ivan Zatkovich, establishes that one with ordinary skill in the art would have known that Valliani's "electronics 210," the component which encrypts PIN information taken from the integrated circuit memory of a smart card and provides it to device 10, would have to include a microprocessor, microcontroller, or a controller with similar processing power. This means Valliani does not have to mention the word "controller" for one with ordinary skill in the art to understand that "electronics 210" is a microprocessor, microcontroller, or a controller with similar processing power. Further, it also establishes that it would have been obvious to one with ordinary skill in the art that Valliani's "electronics 210" is a microprocessor, a microcontroller, or a controller with similar processing power.

Ivan Zatkovich notes that inside Valliani's device 10 there is a controller which executes software routines 35 and/or 45. Ex. 2004 ¶ 50. That is true. We agree with Patent Owner that software routines 35 and/or 45 are executed by device 10 and not by anything in module 200.⁷ But that fact does not undermine "electronics 210" in Valliani's module 200 from being a controller that satisfies the limitation "a controller coupled to said sensor for converting the recorded information stored on said integrated circuit into an encrypted signal indicative of the recorded information" as discussed above. For the limitation at issue, it is sufficient that only the PIN information read from the memory of the smart card is encrypted by "electronics 210" located within module 200. The claim does not require that all data read from integrated circuit memory 225 on smart card 230 by smart card reader/writer 260 be encrypted by "electronics 210."⁸

Alternatively, Petitioner asserts that the limitation of "a controller coupled to said sensor for converting the recorded information stored on said integrated circuit into an encrypted signal indicative of the recorded information" would have been reasonably suggested by the combined teachings of Valliani and Vrotsos. Pet. 23. We do not reach this alternative argument, because Valliani itself describes, and also reasonably would have suggested, the limitation that the portable smart card reader device

⁷ Valliani describes: "Software routine(s) 35 and/or 45, which can be provided with module 200 or may be available from other sources including the manufacturer of device 10, would be loaded into device 10. . . . These routines would be executed by central processor unit 20 within device 10." Ex. 1005, 6:4–16.

⁸ We do not reach Petitioner's contention (Pet. 20) that it would have been obvious to one with ordinary skill in the art to encrypt other information read from the smart card, such as card number and expiration date, in electronics 210 within module 200.

comprises “a controller coupled to said sensor for converting the recorded information stored on said integrated circuit into an encrypted signal indicative of the recorded information.”

d) *Limitation [1.C] — a communication link*

Claim 1 further recites “a communication link for coupling said portable smart card reader device to a mobile communication device for the transmission of said encrypted signal indicative of the recorded information therebetween.” Ex. 1001, 12:16–19. Petitioner explains that in Valliani, module 200 plugs into device 10 over a PCMCIA interface, and that the PCMCIA interface or connection “is a *communication link for coupling said portable smart card reader device to the device 10, corresponding to a mobile communication device.*” Pet. 25–26 (citing Figures 1 and 7). Petitioner states that “[s]pecifically, the module 200 has a projecting member 280 that plugs into socket 90 (‘mounted in a so-called PCMCIA-slot in the housing of unit 10’) in the device 10 to effectuate transmission there between. Ex. 1005, 4:23–32, *see also id.* 4:50–54; Ex. 1003 ¶¶ C46–49.” *Id.* at 26. Petitioner further explains that the only connection between module 200 and device 10 in Valliani is the physical PCMCIA interface depicted in Figure 1. *Id.* These assertions are supported by the cited evidence.

We already have discussed above how Petitioner has adequately accounted for the requirement of a controller within Valliani’s module 200 which takes PIN information from memory 225 on smart card 230 and encrypts it to provide an encrypted PIN to device 10 which is the mobile communication device. The communication link discussed by Petitioner here constitutes the physical channel through which that encrypted information gets provided from “electronics 210” to device 10.

Patent Owner makes the same argument it made in the context of the controller limitation, i.e., that Valliani's card reader 210 does not encrypt a PIN or anything from the memory of smart card 230 because it is incapable of reading anything from smart card 230, as it is merely a magnetic stripe reader. PO Resp. 22. We have discussed and rejected this argument above, because it misreads Petitioner's argument as well as Valliani's disclosure.

Patent Owner further argues that "Petitioner wrongly assumes that Valliani's module 260 would include electronics to encrypt all of the information on the smart card's integrated circuit chip, although Valliani does not support this assumption and in fact seems to merely contemplate the encryption of PIN information." *Id.* But as we noted above, the claim does not require encryption of all data read from the integrated memory of a smart card. Mere encryption of the PIN information read from the integrated circuit memory of the smart card is sufficient to meet the encryption limitation of the claim. Further, Valliani describes that "electronics 210" encrypts the PIN information read from the memory of smart card 230 to provide the encrypted information to device 10, as we have discussed above. Ex. 1005, 5:29–34.

For the foregoing reasons, we are persuaded that Valliani describes "a communication link for coupling said portable smart card reader device to a mobile communication device for the transmission of said encrypted signal indicative of the recorded information therebetween."

e) Limitation [I.D.1] — wherein clause, part 1

Claim 1 further recites "wherein when said sensor reads the recorded information stored on said integrated circuit, said controller converts the recorded information read by said sensor into said encrypted signal."

Ex. 1001, 12:20–23. For this limitation, Petitioner relies on the same

arguments it presents for the limitations [1.A] and [1.B] of claim 1. Pet. 28. Petitioner further explains that it is the logical flow of operations for the sensor to first read the data on the card and then for other electronics to encrypt that data, because the controller cannot encrypt the recorded information until after the sensor has read that recorded information. *Id.* at 28 (citing Ex. 1003 ¶¶ 54–58).

Patent Owner has presented no arguments additional to those it has asserted in connection with limitations [1.A] and [1.B], which we already have addressed above. For reasons discussed above with respect to limitations [1.A] and [1.B] of claim 1, and based on Petitioner’s explanation that the recorded information first has to be read before it is converted by encryption, we are persuaded that the limitation “wherein when said sensor reads the recorded information stored on said integrated circuit, said controller converts the recorded information read by said sensor into said encrypted signal” is met by Petitioner’s reliance on Valliani.

In the alternative, Petitioner asserts that to the extent Valliani does not disclose the time sequence of reading data and encrypting data that has been read, then further in light of the disclosure of Vrotsos, it would have been obvious to one with ordinary skill in the art to have the data read first and then to encrypt the read data. Pet. 28–30. Petitioner explains that “[w]hen Vrotsos’s smart card read/write head in the input device 308, corresponding to the sensor, reads the smart card data, the processor 303 performs encryption of that card data. Ex. 1006, ¶ 52, *see also id.* ¶¶ 75, 78, 94.” *Id.* at 28. Petitioner further explains that it would have been obvious for one with ordinary skill in the art to implement Valliani’s smartcard reader/writer 260 with a controller according to the more specific implementation

described in Vrotsos, because Vrotsos provides the same functionality but with more details. *Id.* at 29.

We do not reach this alternative argument, because the time sequence of reading data first and then encrypting the data is expressly disclosed by Valliani. Note, in particular, Valliani describes that electronics 210 “provides any card **230**-provided **PIN** information to device **10** in encrypted form using only internally stored encryption keys.” Ex. 1005, 5:29–34. Thus, electronics 210 has to use internally stored encryption keys to encrypt the PIN information that has been read from card 230.

f) Limitation [I.D.2] — wherein clause, part 2

Claim 1 further recites “[wherein when said sensor reads the recorded information stored on said integrated circuit, said controller . . .] transmits said encrypted signal via said communication link to said mobile communication device.” Ex. 1001, 12:23–25. Petitioner explains that Valliani describes that electronics 210 in module 200 provides any card 230-provided PIN information to device 10, the wireless communication device, in encrypted form. Pet. 29–30 (citing Ex. 1005, 5:32–35). Petitioner further explains that the only connection between card reader module 200 and device 10 is the PCMCIA interface serving as the communication link, and thus any data transmission from module 200 to the PDA (device 10), and from the PDA to module 200, occurs over that PCMCIA interface. *Id.* (citing Ex. 1003 ¶¶ C61–65). We are persuaded as there is no other means described for transmitting encrypted data from module 200 to device 10.

Petitioner asserts:

It would have been obvious to implement Valliani’s system to transmit the card data (*e.g.*, PIN information) to the device 10 over the physical connection between the module 200 and the device 10. One practical benefit of transmitting the

encrypted card data over the physical connection is that the transmission would be secure, and would protect the card data from unwanted access during transmission. *Id.* ¶¶C72–73. *See* Ex. 1006, ¶¶75, 78.

Id. at 32. Petitioner additionally notes Vrotsos’s disclosure of transmitting encrypted transaction data from attachment 21 to wireless communication device 1 through a physical connection, i.e., an RS-232 connection, and asserts that one of ordinary skill in the art would have looked to a reference such as Vrotsos for further details. *Id.* at 31.

We agree with Petitioner that given Valliani’s disclosure of electronics 210 providing any card 230-provided PIN information to device 10 in encrypted form, and of the PCMCIA interface serving as the only connection between card reader module 200 and device 10, it would have been obvious to one with ordinary skill in the art to transmit card data (e.g., PIN information) to device 10 over the PCMCIA interface. Petitioner also explained practical benefits for doing so, i.e., making the transmission and protecting the card data from unwanted access during transmission. *Id.* at 32 (citing Ex. 1003 ¶¶ C72–73). The reasoning is based on rational underpinning. For this limitation, there is no need for Petitioner to rely on any teaching from Vrotsos, and we do not consider the teachings from Vrotsos in assessing Petitioner’s position for this limitation.

Patent Owner has presented no counter-arguments additional to those it has asserted in connection with limitations [1.A], [1.B], and [1.C]. Those arguments have been discussed and rejected above. They do not defeat or undermine Petitioner’s assertions for limitation [1.D.2]. In particular, we note Valliani’s description that “electronics 210” encrypts the PIN information read from the memory of smart card 230 to provide the encrypted information to device 10. Ex. 1005, 5:29–34. It is not necessary

that encryption be performed on all of the information read from the integrated circuit memory of the card.

We are persuaded that the limitation “[wherein when said sensor reads the recorded information stored on said integrated circuit, said controller ...] transmits said encrypted signal via said communication link to said mobile communication device” is adequately accounted for by Petitioner’s reliance on Valliani’s disclosure.

g) *Limitation [1.E] — transmission to remote server*

Claim 1 further recites “said mobile communication device transmits the encrypted signal indicative of the recorded information to a remote transaction server for processing a commercial transaction.” Ex. 1001, 12:26–29. Petitioner explains as follows:

Valliani further describes the device 10 transmitting information to a host server 75, which then validates that information, and is accordingly a *remote transaction server for processing a commercial transaction*. Specifically, the device 10 “communicates with host 75” to send the card data, such as “user account number, present maximum dollar limit of the account, user identification as well as preferably encrypted PIN data”, corresponding to *the encrypted signal indicative of the recorded information*, to host 75. [Ex. 1005,] 6:35–50, 7:63–65. The host system 75 “will have available PIN data from the true owner of card 230 and can rapidly confirm whether the “pinpad input PIN and the known valid PIN agree.” *Id.* 6:36–49, Ex. 1003, ¶¶ C77–83. The known valid PIN corresponds to the encrypted PIN provided by the card 230. [Ex. 1003] ¶¶ C77–83. The host system then determines whether the “pinpad input PIN and the known valid PIN agree.” (Ex. 1005, 6:36–49) and allows the transaction to proceed. Accordingly, in Valliani, the device 10 is a *mobile communication device that transmits the encrypted signal indicative of the recorded information to the host 75, which is a remote transaction server for processing a commercial transaction*. [Ex. 1003] ¶ C83.

Pet. 33. These assertions are supported by the cited evidence.

Notwithstanding Patent Owner's contrary arguments, discussed below, we are persuaded that Valliani's device 10 satisfies the limitation "said mobile communication device transmits the encrypted signal indicative of the recorded information to a remote transaction server for processing a commercial transaction."

Patent Owner argues that "Petitioner's reliance on the transmission of PIN data is misplaced and mistakes the authentication of the Valliani card user's identity for the actual processing of a commercial transaction." PO Resp. 20. Patent Owner explains:

A POSITA would understand that a commercial transaction is any transaction that involves some form of payment, or money transfer, in exchange for goods and services. This is consistent with the use of the term within the '239 patent and virtually all other usage of the term at the time of the invention. Ex. 2004, ¶82 (citing intrinsic and extrinsic evidence). But the cited portions of Valliani do not describe the exchange of payment for goods and services. Valliani's remote host 75 is only used for retrieving and verifying PIN and signature data—not for processing of the payment transaction. *Id.*, ¶¶83–85.

Id. Patent Owner's argument is unpersuasive, as explained below.

Patent Owner and its declarant Ivan Zatkovich focus on one aspect of a commercial transaction to the exclusion of everything else that also relates to the performance of the commercial transaction. The claim phrase at issue simply is "for processing a commercial transaction." Verifying the identity of a person with whom a transaction would be completed is as much a part of the commercial transaction to be completed as the transfer of money between accounts. The claim limitation at issue does not specify which aspect of the commercial transaction must be tied directly to the encrypted data that has been transmitted. Further, Valliani discloses that PIN

verification leads to learning whether the proposed sale transaction should proceed or be aborted. Ex. 1005, 6:24–46. Michael Shamos testifies that notifying a seller/buyer of an acceptance or rejection of a transaction is an example of “processing a commercial transaction.” Ex. 1017 ¶ 48. We agree. The claim does not require completion of a commercial transaction by the remote transaction server. We find that “for processing a commercial transaction” as recited in limitation [1.E] encompasses authenticating the identity of a person with whom a commercial transaction is proposed or contemplated.

For the foregoing reasons, we are persuaded that Valliani’s device 10 “transmits the encrypted signal indicative of the recorded information to a remote transaction server for processing a commercial transaction.”

h) Conclusion

Petitioner has shown by a preponderance of the evidence that claim 1 is unpatentable over Valliani and Vrotsos.

4. Independent Claim 4

Claim 4 recites “[a] method for reading a smart card having recorded information stored on an integrated circuit incorporated into the card.” Ex. 1001, 12:38–40. Petitioner relies on its discussion of the preamble of claim 1. Pet. 40. Patent Owner has not presented counter-arguments additional to those it asserts in the context of claim 1. For essentially the same reasons discussed above with respect to the preamble of claim 1, we are persuaded that this preamble in claim 4 is met by the applied prior art. We need not determine whether this preamble is limiting.

Claim 4 recites a step of “providing a portable card reader device comprising a sensor for reading the recorded information stored on the integrated circuit.” Ex. 1001, 12:41–43. Petitioner relies on its discussion

of the preamble and limitation [1.A] of claim 1. Pet. 40. Patent Owner has not presented counter-arguments additional to those it asserts in the context of claim 1. For essentially the same reasons discussed above with respect to the preamble and limitation [1.A] of claim 1, we are persuaded that this step is met by the applied prior art.

Claim 4 recites a step of “[providing . . .] a controller coupled to said sensor for converting the recorded information into an encrypted signal indicative of the recorded information stored on said integrated circuit incorporated.” Ex. 1001, 12:41–46. Petitioner relies on its discussion of limitation [1.B] of claim 1. Pet. 40. Patent Owner has not presented counter-arguments additional to those it asserts in the context of limitation [1.B]. For essentially the same reasons discussed above with respect to limitation [1.B] of claim 1, we are persuaded that this step is met by the applied prior art.

Claim 4 recites a step of “[providing . . .] a communication link for coupling said portable smart card reader device to a mobile communication device.” Ex. 1001, 12:41–48. Petitioner relies on its discussion of limitation [1.C] of claim 1. Pet. 40. Patent Owner has not presented counter-arguments additional to those it asserts in the context of limitation [1.C]. For essentially the same reasons discussed above with respect to limitation [1.C] of claim 1, we are persuaded that this step is met by the applied prior art.

Claim 4 recites “wherein when said sensor reads the recorded information stored on the integrated circuit, said controller converts the recorded information read by said sensor into said encrypted signal.” Ex. 1001, 12:49–52. Petitioner relies on its discussion of limitation [1.D.1] of claim 1. Pet. 40. Patent Owner has not presented counter-arguments for this

limitation additional to those it asserts in the context of limitation [1.D.1]. For essentially the same reasons discussed above with respect to limitation [1.D.1] of claim 1, we are persuaded that this limitation is met by the applied prior art.

Claim 4 recites “[wherein when said sensor reads the recorded information stored on the integrated circuit, said controller . . .] transmits said encrypted signal via said communication link to said mobile communication device.” Ex. 1001, 12:49–54. Petitioner relies on its discussion of limitation [1.D.2] of claim 1. Pet. 40. Patent Owner has not presented counter-arguments for this limitation additional to those it asserts in the context of limitation [1.D.2]. For essentially the same reasons discussed above with respect to limitation [1.D.2] of claim 1, we are persuaded that this limitation is met by the applied prior art.

Claim 4 recites a step of “providing said encrypted signal indicative of the recorded information stored on the integrated circuit to said mobile communication device for further processing by circuitry contained in said mobile communication device.” Ex. 1001, 12:55–59. Relying on its discussion of limitation [1.D.2] of claim 1, Petitioner asserts that the applied prior art already teaches providing the encrypted signal indicative of the recorded information stored on the integrated circuit to the communication device. Pet. 41. Petitioner further asserts that Valliani additionally discloses the claimed “*for further processing by circuitry contained in said mobile communication device.*” *Id.* Petitioner explains as follows:

Valliani discloses that the *mobile communication device* 10 includes a central processor unit 20, corresponding to circuitry. Ex. 1005, 4:4–12. “Software routine(s) 35 and/or 45 . . . may be loaded into device 10.” *Id.* 6:5–7. “These routines would include point of sale software, software driver(s) for . . .

smart card reader/writer unit 260 . . . DES encryption, signature capture and signature compression.” *See id.* 6:8–13. The software routines “would be executed by central processing unit 20 within device 10.” *Id.* 6:14–15. Thus, *the mobile communication device* in Valliani is equipped with software 35 and 45 that can process the encrypted signal from the card reader. It was necessary to process that data into a form suitable for transmission via the appropriate communication protocols. Ex. 1003, ¶¶ C127–132.

Id. These assertions are rational and supported by the cited evidence.

Patent Owner has not presented counter-arguments for this limitation additional to those it asserts in the context of limitation [1.D.2] of claim 1. For essentially the same reasons discussed above with respect to limitation [1.D.2] of claim 1, and further based on Petitioner’s above-quoted explanation, we are persuaded that this limitation relating to further processing in the mobile communication device is met by the applied prior art.

Claim 4 recites “said mobile communication device transmits the encrypted signal indicative of the recorded information to a remote transaction server for processing a commercial transaction.” Ex. 1001, 12:60–63. Petitioner relies on its discussion of limitation [1.E] of claim 1. Pet. 43. Patent Owner has not presented counter-arguments additional to those it asserts in the context of limitation [1.E] of claim 1. For essentially the same reasons discussed above with respect to limitation [1.E] of claim 1, we are persuaded that this limitation is met by the applied prior art.

For the foregoing reasons, Petitioner has shown by a preponderance of the evidence that claim 4 is unpatentable over Valliani and Vrotsos.

5. *Dependent Claims 3 and 6*

Claims 3 depends directly from claim 1 and further recites “wherein said mobile communication device receives transaction validation information from said remote transaction server.” Ex. 1001, 12:35–37. Claim 6 depends directly from claim 4 and further recites the same additional limitation. *Id.* at 13:2–4.

Petitioner explains:

In Valliani, when the host system validates the user’s PIN, the device 10, corresponding to *said mobile communication device*, receives *transaction validation information* from the host system 75 indicating the transaction is allowed to proceed. Specifically, as stated in Section IX.A.1.g, the host system 75 compares the PIN data received from the device 10 to the known valid PIN. Ex. 1005, 6:33–46. The known valid PIN corresponds to the PIN provided by the card 230. Ex. 1003, ¶¶C105-107. If the PINs match, “th[e] comparison outcome can be sent by host system 75 to device 10, whereupon an individual using device and module 210 to transact a sale rapidly learns whether the sale should proceed.” Ex. 1005, 6:39–42.

Pet. 37–38. The accounting by Petitioner is logical and supported by the cited evidence. Notwithstanding Patent Owner’s argument to the contrary, discussed below, we are persuaded that this limitation is met by the applied prior art.

Patent Owner argues:

Petitioner asserts that “validat[ing] the user’s PIN” is equivalent to transaction validation information. [Petition, p. 37]. Petitioner is incorrect, because there is much more information that must be exchanged and processed for a commercial transaction to be deemed validated *and completed*.

As described above, Valliani does not disclose processing a commercial transaction because a commercial transaction would require some form of payment in exchange for goods and services. The asserted remote host 75 in Valliani is used for

retrieving and verifying PIN and signature data—*not for processing a commercial transaction*. Although Valliani mentions that the results of this PIN or signature verification may inform the user “whether the same should proceed,” there is *no mention of transaction processor, processing a commercial transaction, or of receiving verification from a commercial transaction*. Ex. 2004, ¶¶88–91.

PO Resp. 25 (emphasis added). The argument does not undermine Petitioner’s showing because the claim recitation “transaction validation information” is read too restrictively by Patent Owner. A preliminary identity check that allows the proposed commercial transaction to proceed still constitutes a form of transaction validation. Patent Owner reads “transaction validation” as though it requires completion of the commercial transaction. But such a narrow reading of “transaction validation” is unreasonable. Patent Owner does not sufficiently explain why a preliminary identity check that would allow or disallow continuation of the transaction is not a form of transaction validation. Execution and completion of the commercial transaction simply is not required for “transaction validation.” Although the ’239 patent describes embodiments in which the transaction server interacts with a remote processor/issuer 20 of the financial institution that issued the card to accept or refuse the commercial transaction, thus completing or rejecting the transaction (Ex. 1001, 9:19–36, 10:24–44, 11:8–35, 11:40–60), the Specification nowhere specially defined “transaction validation” to require “completion” of transaction. “[A] particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment.” *SuperGuide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004) (citation omitted); *see also In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993).

For the foregoing reasons, Petitioner has shown by a preponderance of the evidence that claims 3 and 6 are unpatentable over Valliani and Vrotsos.

6. *Dependent Claims 2 and 5*

Claim 2 depends directly from claim 1 and further recites “in which the smart card is selected from a group consisting of a chip card, EMV card, proximity detector or NFC card, contactless card, or any combination thereof.” Ex. 1001, 12:30–33. Claim 5 depends directly from claim 4 and further recites the same additional limitation. *Id.* at 12:64–67. Petitioner accounts for the additional limitation of claim 2, relative to claim 1. Pet. 36–39. Petitioner also accounts for the additional limitation of claim 5, relative to claim 4. *Id.* at 43–44. The assertions are supported by the cited evidence. Patent Owner does not present any counter-argument for claims 2 and 5, additional to those it asserts in the context of claims 1 and 4, respectively, which we already have addressed above and rejected in discussing claims 1 and 4. Petitioner has shown by a preponderance of the evidence that claims 2 and 5 are unpatentable over Valliani and Vrotsos.

E. *Obviousness of Claims 1–6 over Vrotsos*

1. *Independent Claim 1*

a) *Preamble*

Claim 1 recites “[a] portable smart card reader device for reading a smart card having recorded information stored on an integrated circuit incorporated into the card.” Ex. 1001, 12:7–9. Petitioner identifies in Vrotsos a smart card reader having portion 55 for reading information from smartchip 53 of a credit card, and reasons that the smart card reader is portable because it is part of attachment 21 secured to a mobile phone. Pet. 45–47 (citing Ex. 1006 ¶ 41, Figs. 1D, 1E; Ex. 1003 ¶¶ 12–16). We find

Petitioner's reasoning to be supported by the cited evidence, and we need not determine whether this preamble recitation is limiting.

Patent Owner does not specifically address this preamble recitation and Vrotsos. However, Patent Owner argues that Vrotsos does not disclose another claim limitation, i.e., limitation [1.A] — “a sensor for reading said recorded information stored on said integrated circuit incorporated into said card.” To the extent that argument applies to this preamble recitation as well, we note that that argument, as we discuss below, does not undermine Petitioner's showings that Vrotsos does disclose such a sensor. For the same reasons, we are persuaded that Vrotsos describes this preamble.

b) Limitation [1.A] — a sensor

Claim 1 further recites that the portable smart card reader device comprises “a sensor for reading said recorded information stored on said integrated circuit incorporated into said card.” Ex. 1001, 12:10–11.

Petitioner explains that, in Vrotsos, when card 51 having smartchip 53 is inserted into slot 22, a smartcard read/write head within the slot can read information from, or write information to, smartchip 53. Pet. 18 (citing Ex. 1006 ¶ 41; Ex. 1003 ¶¶ C19–20). Paragraph 41 of Vrotsos describes:

In embodiments of the invention, the attachment **21** may have a combined magnetic stripe reader and smartcard reader. In such embodiments, the slot **22** may be as shown in **FIG. 1E**. A card **51** having a magnetic stripe **52** and/or smartchip **53** may be inserted into the slot **22**. The slot may be shaped so as to include a shallow channel portion **54** of a depth suitable for reading a magnetic stripe **52** positioned parallel to a lateral surface of the card **51** as well as a deeper channel portion **55** of a suitable depth and width such that substantially all of the card **51** may be inserted into the slot **22** when a portion of the slot **51** is inserted into the deeper channel portion **55**. As shown, the deeper channel portion **55** is of a width substantially identical to the width of the card **51**, such that lateral surfaces of the deep channel

portion **55** may contact the lateral surfaces of the card **51** to ensure that the smartchip **53** is in a desired position. A magnetic stripe reader head may be located within a surface of the shallow channel portion **54** so that the magnetic stripe **52** can be read as the card **51** is swiped through the shallow channel portion **54**. *A smartcard read/write head may be positioned within a surface of the deeper channel portion 55 of the slot 22 so that information may be read from or written to the smartchip 53 when the card is positioned within the deeper channel portion 55.*

Ex. 1006 ¶ 41 (emphasis added). Petitioner identifies Vrotsos's smartchip 53 as the claimed "integrated circuit incorporated into the smart card." Pet. 18. For the claimed sensor, Petitioner states: "In Vrotsos, the smartcard read/write head is a *sensor for reading said recorded information stored on said integrated circuit incorporated into said card.*" *Id.*

Patent Owner does not dispute that Vrotsos refers to a "smartcard" inserted into a slot. Patent Owner does not dispute that the referenced "smartcard" has incorporated thereon an integrated circuit for storing information. In that regard, Patent Owner states:

A POSITA would understand that Vrotsos's mention of a "smartcard" that is inserted into a slot, [Ex. 1006, ¶41] could only refer to an EMV-type smart card. Ex. 2004, ¶37. EMV standards define the methods for reading IC chips embedded in these types of smartcards, including the sensors for accessing the contacts on the card's IC chip. *Id.* ¶¶18, 37, 40–42.

PO Resp. 15.⁹ Nonetheless, Patent Owner maintains that Vrotsos does not disclose a sensor for reading an integrated circuit on the card. *Id.* at 14.

Patent Owner asserts:

⁹ Ivan Zatkovich testifies: "As a card that requires physical connection to a reader, it would be the EMV type of card. As stated above, an EMV type card would require a sensor which could access the contact pad of the IC chip." Ex. 2004 ¶ 37.

A POSITA would understand that a read/write “head” refers to a magnetic read head used for magnetic stripe. Ex. 2004, ¶ 35. This is consistent with how Vrotsos itself refers to the magnetic stripe sensor as “read head 23,” which is a standard industry term for a magnetic read head. *Id.*, ¶ 35. A magnetic read head would not be compatible with a sensor required to read an integrated circuit within a smart card, specifically “consisting of a chip card, EMV card, proximity detector or NFC card, contactless card, mobile NFC device, or any combination thereof.” Ex. 1001, claims 2 and 5; Ex. 2004, ¶¶34–35.

Id. at 14–15. Patent Owner further asserts:

Vrotsos does not refer to industry standards, a specific type of smart card, or to any specific type of sensor other than the lone reference to a read/write head, and Vrotsos’ teachings contradict normal smart card or EMV card standards. Instead of an EMV or smart card sensor, Vrotsos proposes “a card 51 having a magnetic stripe 52 and/or smartchip 53” to be read by a “smartcard read/write head . . . positioned within a surface of the deeper channel portion 55 of the slot 22 so that information may be read from or written to the smartchip 53 when the card is positioned within the deeper channel portion 55,” Ex. 1006, ¶ 41, with the only thing described about the purported smartcard reader being the size and width, and the inclusion of a smartcard read/write head. *Id.*

Based on the entirety of Vrotsos’s disclosure and knowledge in the art, a POSITA would understand that the disclosed read/write head would only be appropriate for reading magnetically sensed information, such as from a magnetic stripe. *Id.*, ¶ 42. A POSITA would find no disclosure of a sensor for reading either an NFC or contact less smart card or electronically recorded information on an EMV card. *Id.*, ¶43. Accordingly, Vrotsos does not meet the claim limitations requiring that the card reader device include a sensor for reading information from the integrated circuit of a smart card. *Id.*, ¶44.

Id. at 15–16.

These arguments do not sufficiently undermine Petitioner’s showing. Patent Owner’s arguments stretch beyond reason. They

have an inflexible focus on the literal wording used in Vrotsos, to the exclusion of the substantive content Vrotsos would have disclosed to one with ordinary skill in the art. They overstate the consequence of Vrotsos's not using the words Patent Owner contends should have been used to describe a sensor that reads information from an integrated circuit incorporated into a smart card.

First, however, we address Patent Owner's contention, relying on testimony of Ivan Zatkovich (Ex. 2004 ¶ 35), that a read/write "head" could only be used to refer to something that reads magnetically sensed information, such as a magnetic stripe. We are not persuaded that that is true. The testimony of the party's declarants conflict in that regard. Michael Shamos, Petitioner's declarant, testifies as follows:

33. A POSITA would have understood that like "sensor," the word "head" as used in Vrotsos refers to a device that reads, records, erases, or writes data on the particular storage medium it interacts with. The word is not limited solely to magnetic heads, but would include smart card read/write devices as well. Therefore by using the term "head," Vrotsos sufficiently describes to a POSITA that its reference to smartcard read/write head refers to a sensor that reads from an integrated circuit on a smart card.

Ex. 1017 ¶ 33. Ivan Zatkovich, Patent Owner's declarant, testifies:

35. One of ordinary skill in the art would understand that a read/write "head" refers to a magnetic read head used for magnetic stripe. This is also consistent with how Vrotsos refers to their magnetic stripe sensor as "read head 23". Again, this is a standard industry term for a magnetic read head. A magnetic read head would not be compatible with a sensor required to read an integrated circuit within a card, specifically, "consisting of a chip card, EMV card, proximity detector or NFC card,

contactless card, or any combination thereof.” [Ex. 1001, 12:32–33 or Claim 2]

36. The asserted Vrotsos “sensor” is not actually a sensor for reading an integrated circuit since it is referred to as a smart card read/write head, and then only as a single isolated reference with no description or indication of what type of smart card read/write head.

Ex. 2004 ¶¶ 35–36.

On close scrutiny of the testimony of the declarants, there is not much of a genuine conflict, except for the conclusion on whether Vrotsos describes a sensor which reads recorded information from an integrated circuit incorporated into a card. Notably, Ivan Zatkovich does not testify that a read/write “head” *can only* refer to a magnetic read head used for magnetic stripe. His testimony leaves that suggestion but he actually did not so testify. We do not assume that that is his testimony. Also, Ivan Zatkovich states that a read/write head referring to a magnetic read head is consistent with how Vrotsos refers to its magnetic sensors as “read head 23.” Ex. 2004 ¶ 35. That is true, but he does not mention that that is not consistent with Vrotsos’s also referring to a “smartcard read/write head” as being used to read information from smartchip 53 incorporated into a card. Ex. 1006 ¶ 41. Ivan Zatkovich does not testify that the more restrictive reading of “head” as Patent Owner proposes is consistent with all usages contained in Vrotsos.

Further, although Ivan Zatkovich states that a read/write “head” is industry standard term for a magnetic read head used for magnetic stripe, he does not testify that any applicable industry standard precludes using “read head” to describe a device which reads information from an integrated circuit incorporated on a card. Ex. 2004 ¶ 35. Ivan Zatkovich also testifies that “[a] magnetic read head would not be compatible with a sensor required

to read an integrated circuit within a card,” *id.*, but Petitioner is relying on Vrotsos’s disclosure of a “smartcard read/write head,” not Vrotsos’s magnetic “read head 23” which is a separate component. Ivan Zatkovich does not testify that “smartcard read/write head” would not be compatible with a sensor required to read an integrated circuit incorporated into a card.

Thus, in all these respects, there is no genuine conflict. We do not see Ivan Zatkovich as having testified that a read “head” simply cannot be used to describe a device, e.g., a sensor, which reads information recorded on an integrated circuit incorporated into a card. On the one hand, we have Michael Shamos’s testimony that to one with ordinary skill in the art, a read “head” refers to a device that reads, records, erases, or writes data on the particular storage medium it interacts with, “and is not limited solely to magnetic heads, but would include smart card read/write devices as well.” Ex. 1017 ¶ 33. On the other hand, we do not have Ivan Zatkovich testifying that a read “head” simply cannot be used to describe a device, e.g., a sensor, which reads information recorded on an integrated circuit incorporated into a card. There is insufficient basis to agree with Patent Owner’s restrictive reading of a read “head,” particularly because Vrotsos itself uses the term “smart card read/write head” to refer to a component that reads information from smartchip 53 (Ex. 1006 ¶ 41). We credit the testimony of Michael Shamos (Ex. 1017 ¶ 33) that the word “head” as used in Vrotsos, would have been understood by one with ordinary skill in the art as not limited solely to magnetic heads, but would include smart card read/write devices as well, and find that the word “head” would be so understood by one with ordinary skill in the art.

A genuine conflict does exist with respect to Ivan Zatkovich’s testimony (Ex. 2004 ¶ 36) that “[t]he asserted Vrotsos ‘sensor’ is not

actually a sensor for reading an integrated circuit since it is referred to as a smart card read/write head,” and Michael Shamos’s testimony (Ex. 1017 ¶ 33) that “Vrotsos sufficiently describes to a POSITA that its reference to smartcard read/write head refers to a *sensor* that reads from an integrated circuit on a smart card.” We credit the testimony of Michael Shamos over that of Ivan Zatkovich, for several reasons.

First, as discussed above, Ivan Zatkovich never testified that a read “head” simply cannot be used to describe a device, e.g., a sensor, which reads information recorded on an integrated circuit incorporated into a card. Second, as discussed above, we have determined that “head” as used in Vrotsos would have been understood by one with ordinary skill in the art as not limited solely to magnetic heads, but would include smart card read/write devices as well. Ivan Zatkovich’s statement is inconsistent with Vrotsos’s expressly stating that “[a] smartcard read/write head” is used to read information from smartchip 53. Ex. 1006 ¶ 41.

Even assuming that Patent Owner’s restrictive reading of “head” is correct, we still would arrive at the conclusion that Petitioner has shown that Vrotsos discloses “a sensor for reading said recorded information stored on said integrated circuit incorporated into said card.” Vrotsos expressly discloses reading information from smartchip 53 of a transaction card (Ex. 1006 ¶ 41). If it is incorrect to use the word “head” to describe a sensor which reads recorded information from the integrated circuit incorporated into a card, it does not follow that Vrotsos does not disclose a sensor which reads recorded information from the integrated circuit incorporated into a card. Patent Owner’s contention focuses inflexibly on the literal

wording used in Vrotsos, to the exclusion of the substantive content Vrotsos would have disclosed to one with ordinary skill in the art.

Ivan Zatkovich testifies regarding Vrotsos's card as follows: "As a card that requires physical connection to a reader, it would be the EMV type of card. As stated above, an EMV type card would require a sensor which could access the contact pad of the IC chip. The International Standard that applies to EMV cards is ISO 7816." Ex. 2004 ¶ 37 (footnote omitted). Thus, one with ordinary skill in the art, notwithstanding the fact that Vrotsos uses the term "smart card read/write head," would have known to use a sensor that indisputably could access the contact pad of the IC chip to read information from the integrated circuit. Michael Shamos testifies that sensors for reading recorded information on an integrated circuit memory of a smart card were well known to one with ordinary skill in the art in 2009. Ex. 1003 ¶ 29; Ex. 1017 ¶¶ 30, 34. Ivan Zatkovich does not dispute that "integrated circuit readers and smart card readers were known." Ex. 1018, 25:18–20. Even according to Patent Owner, at the time of the invention, there already were industry standards which "defined the methods for reading IC chips embedded in these types of smart cards." PO Resp. 12–13.

Thus, notwithstanding that the term "smart card reader/writer head" is used in Vrotsos, and assuming that that term is incorrect for referring to a device that reads an integrated circuit on a card, one with ordinary skill in the art still would have understood that Vrotsos was disclosing "a sensor for reading said recorded information stored on said integrated circuit incorporated into said card."

For the foregoing reasons, we agree with Petitioner that by describing a “smart card read/write head” which reads recorded information from smartchip 53, Vrotsos discloses to one with ordinary skill in the art “a sensor for reading said recorded information stored on said integrated circuit incorporated into said card.”

c) Limitation [1.B] — a controller

Claim 1 further recites that the portable smart card reader device comprises “a controller coupled to said sensor for converting the recorded information stored on said integrated circuit into an encrypted signal indicative of the recorded information.” Ex. 1001, 12:12–15. Petitioner identifies processor 303 as corresponding to the claimed controller, and asserts that it encrypts transaction data captured by the card reader. Pet. 23–24. Petitioner further notes that as shown in Figure 10 of Vrotsos, processor 303 is coupled to input device 308 which includes the sensor for reading recorded information on the integrated circuit on smartchip 53. *Id.* at 23 (citing Ex. 1003 ¶¶ C35–39). Petitioner cites to paragraphs 75 and 78 of Vrotsos which describe in a general manner, non-specific to any particular embodiment, that processor 303 of attachment 21 may encrypt input information from the attachment’s input device 308. *Id.* at 24. Thus, the teaching reasonably applies to recorded information read from smartchip 53. Petitioner explains that the step of encrypting information is the same as converting that information into an encrypted signal indicative of the recorded information. *Id.* (citing Ex. 1003 ¶ C42). The assertions are rational and supported by the cited evidence. Notwithstanding Patent Owner’s arguments to the contrary, we are persuaded that Vrotsos describes this limitation of claim 1.

Patent Owner asserts that Vrotsos does not disclose “the controller with the functionality required in claims 1 and 4.” PO Resp. 18. Essentially, this argument is built on the foundation of Patent Owner’s contention that Vrotsos does not disclose reading information from an integrated circuit incorporated into a card. Patent Owner states:

As discussed above, Vrotsos’s disclosure does not support the reading of an integrated circuit. *See* discussion, *supra*. Accordingly, Vrotsos also does not disclose converting the recorded information read from an integrated circuit into an encrypted signal and transmitting a signal containing the encrypted information representing the recorded information stored on the integrated circuit.

PO Resp. 19. We have already considered and rejected the argument that Vrotsos does not disclose reading recorded information from the integrated circuit incorporated into a card in the context of the sensor limitation discussed above. Patent Owner’s assertion building on that failed argument as a foundation is also without merit.

Patent Owner further argues:

Vrotsos does disclose the encryption of the card information, but the encrypted information is derived *from Vrotsos’s magstripe 23*. Petitioner relies on its expert’s declaration for the argument that Vrotsos discloses the encryption of information from an integrated circuit, citing multiple Vrotsos excerpts suggesting that encryption occurs prior to sending information to the mobile communication device, *but always referring to the mag stripe reader 23 for capturing information* and attachment 21 for encrypting that information. Petitioner’s expert asserts, for example, that “[t]he user may move the card past the reader assembly and transaction data may be captured by the reader 23 in the attachment 21. The attachment 21 may encrypt the transaction data captured by the reader 23.” Ex. 1003, ¶C36. But again, because there is nothing in Vrotsos supporting that reader 23 can read an integrated circuit of a smart card, these arguments do nothing other than to

establish that any information being encrypted would come from Vrotsos's magstripe reader.

PO Resp. 24. But Patent Owner does not address Petitioner's assertion (1) that processor 303 is coupled to input device 308 which includes smart card reader/writer head, the sensor that reads recorded information from the integrated circuit incorporated on the smartchip (Pet. 23), and (2) that Vrotsos, without regard to whether the read information is from a magnetic stripe or from an integrated circuit of a smart card, states "processor 303 of the attachment 21 may encrypt input information received from the attachment's input device 308" (Pet. 24 (citing Ex. 1006 ¶ 78)). Patent Owner also overlooks similar testimony from Michael Shamos citing to Vrotsos's paragraphs 75 and 94, which amply supports Petitioner's assertion that information read from the integrated circuit of a smart card is then encrypted by processor 303. Ex. 1003 ¶¶ C37, C39, C41.

Vrotsos describes:

The attachment **21** may also include a processor **303**, a memory **307** and an input device **308**. The processor may execute software application (which may be stored in the attachment memory **307**) allowing the processor to receive input information from the input device **308** and process the input information to generate data for transmission to a remote computer **101** via the antenna **5** of the wireless communication device **1**. By executing the software application, the attachment may determine from which input device **308** it is receiving input information (if multiple input devices are provided), encrypt the input information, ...

Ex. 1006 ¶ 75. Indeed, Vrotsos further describes:

The processing performed by the processor **303** of the attachment **21** may include encrypting the information, dividing the input information into data packets, appending header information to the input information to indicate the identify and/or location of the user, etc. In embodiments of the invention

in which the attachment **21** includes multiple input devices, the processor of the attachment **21** may encrypt the information differently depending on from which input device the input information was received [from magstripe or smartchip].

Id. ¶ 94. Thus, Patent Owner’s arguments are misplaced.

Patent Owner further asserts: “As Petitioner concedes, Vrotsos also does not disclose transmitting data from the integrated circuit of a smart card (or an encrypted signal produced therefrom) to a mobile communication device. *See* Petition, pp. 71–72; Ex. 2004, ¶¶75–77.” PO Resp. 19. This argument is misplaced, because the controller limitation does not require transmitting data from the integrated circuit of a smart card (or an encrypted signal produced therefrom) to a mobile communication device. That is a feature of limitation [1.C] reciting a communication link. Further, it is also misplaced because Petitioner acknowledges only that there is no explicit disclosure of smart card data being transmitted over a particular communication link to a wireless communication device. Pet. 71–72. As discussed below in the context of limitation [1.C], it is still Petitioner’s contention that it would have been obvious to one with ordinary skill in the art to send smart card data encrypted by the controller to the wireless communication device over that communication link.

We are persuaded that Vrotsos discloses “a controller coupled to said sensor for converting the recorded information stored on said integrated circuit into an encrypted signal indicative of the recorded information.”

d) Limitation [1.C] — communication link

Claim 1 recites “a communication link for coupling said portable smart card reader device to a mobile communication device for the transmission of said encrypted signal indicative of the recorded information therebetween.” Ex. 1001, 12:16–19. Petitioner identifies a first Vrotsos

embodiment (Ex. 1006 ¶¶ 72–78) with attachment 21 including input device 308 having a smart card reader, where attachment 21 receives input from the smart card reader, processes it, and sends it to a cellular phone for transmission to remote computer 101. Pet. 27, 71. Figure 10 is a block diagram of that embodiment and is reproduced below:

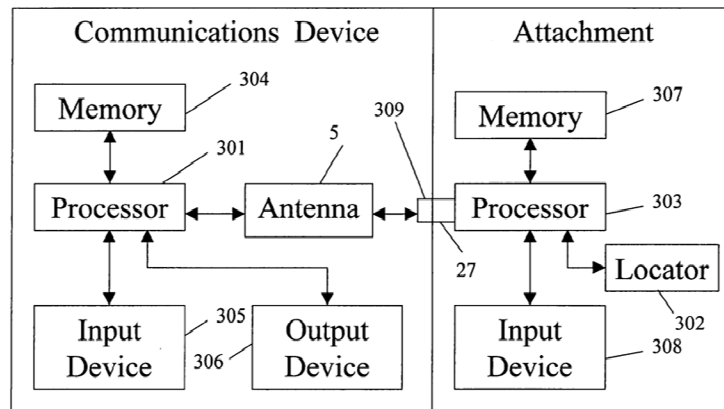


FIGURE
10

Figure 10 shows a block diagram of one embodiment of Vrotsos. Ex. 1006 ¶ 23. Vrotsos describes:

The wireless communication device 1 may have a communication port and the attachment 21 may have a corresponding connector 27 that mate when the two are coupled together, permitting electrical signals to be passed from the attachment 21 to the wireless communication device 1 and vice versa.

Id. ¶ 42. Petitioner identifies the wired physical connection between attachment 21 and the cellular phone as the communication link. Pet. 71. Petitioner states, however, that “Vrotsos does not explicitly refer to smart card data being transmitted over that link.” *Id.*

Petitioner identifies a second Vrotsos embodiment, which reads card data from a magnetic stripe on the card and in which attachment 21 communicates with the phone over a wireless connection. *Id.* at 72 (citing

Ex. 1006 ¶¶ 50–55, Fig. 7). Petitioner asserts that in that second embodiment, when a user swipes the card, attachment 21 captures transaction data, encrypts it, and transmits the encrypted transaction data to the wireless communication device over the wireless local communications network. *Id.* (citing Ex. 1006 ¶ 52). Figure 7 of Vrotsos is reproduced below:

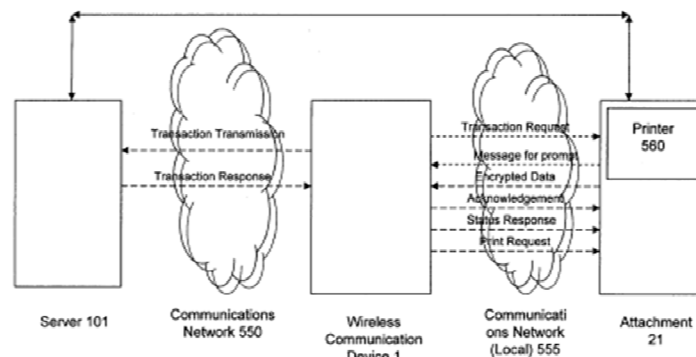


Fig. 7

Figure 7 illustrates implementation of wireless communication between a wireless communication device and an attachment according to an embodiment of Vrotsos. Ex. 1006 ¶ 20.

Petitioner explains that one with ordinary skill in the art would have known to process smart card data the same way as data read from a magnetic stripe, i.e., send it over a wireless communication link to the phone. Pet. 74. Petitioner asserts that it would have been obvious to one with ordinary skill in the art, in the second embodiment of Vrotsos, to transmit smart card data, rather than data read from the magnetic stripe of a card, to the cellular phone. *Id.* (citing Ex. 1003 ¶ E21). Petitioner asserts that one with ordinary skill in the art would have been motivated to transmit transaction data read from smartchip 53 through such a wireless communication link to complete a commercial transaction. *Id.* (citing Ex. 1003 ¶ E20).

Alternatively, Petitioner explains that one with ordinary skill in the art would have recognized physical connection as an alternative connection for sending smart card data. *Id.* at 73 (citing Ex. 1003 ¶ E16). Petitioner further explains that because the two embodiments provide the same function, it would have been obvious to one with ordinary skill in the art to send smart card data to the phone via the physical connection in the first embodiment, akin to sending magnetic stripe data to the phone via a wireless connection in the second embodiment. *Id.* at 73 (citing Ex. 1003 ¶ E14). Petitioner further notes that Vrotsos contemplates different ways that attachment 21 could connect to and communicate with the phone. *Id.* (citing Ex. 1006, Fig. 1A–1D, 3, 7, 10).

Petitioner’s assertions are rational and supported by the cited evidence. Notwithstanding the contrary arguments of Patent Owner, discussed below, we are persuaded that Vrotsos reasonably suggests this limitation of claim 1 under either alternative presented by Petitioner.

Patent Owner makes a number of counter-arguments including the same arguments we discussed and rejected above in the context of the other limitations of claim 1 and Vrotsos, i.e., (1) Vrotsos does not disclose a sensor for reading recorded information from an integrated circuit incorporated into a card; (2) Vrotsos does not disclose encrypting information read from an integrated circuit incorporated into a card; and (3) Vrotsos does not disclose sending from the smart card reader device encrypted signal indicative of recorded information on the card to a wireless communication device. PO Resp. 53. Our reasoning and analysis in that regard equally applies here.

On pages 54–57 of the Patent Owner Response, Patent Owner provides what appears to be additional arguments. PO Resp. 54–57.

However, as we discuss below, those arguments are largely built on the foundation of the already rejected arguments and are otherwise a mischaracterization of Petitioner's arguments.

Patent Owner asserts:

Petitioner asserts that Vrotsos shows two embodiments—one embodiment disclosing a smart card reader for reading card information, *but not disclosing any encryption of the card information or a communication link to a mobile device*; and a second embodiment disclosing a magnetic stripe reader and encryption of the card information, *but not disclosing a smart card reader of any kind*. [Petition, pp. 71–72] From there, Petitioner's view of obviousness essentially consists of asserting that a POSITA would have conflated the two embodiments to come up with a device that read information from a smart card, encrypt[ed] it, and transmitted it to a mobile phone.

Id. at 55 (emphasis added). Petitioner, however, has not represented that in the first embodiment, where there is a wired physical connection as the communication link between the attachment and the cellular phone, there is no encryption of information from a smart card. Petitioner also has not represented that in that first embodiment, there is no communication link between the attachment and the cellular phone.

To the contrary, Petitioner asserts for that embodiment that attachment 21 includes input device 308 having a smart card reader, where attachment 21 receives input from the smart card reader, generates encrypted data, and sends the encrypted data to a cellular phone for transmission to remote computer 101. Pet. 27, 71. Petitioner states: “Moreover, transmission of an encrypted signal between card reader and communication device over a physical connection was well-known to a POSITA, as disclosed e.g. in Vrotsos. *Id.* ¶C53; Ex. 1006, ¶¶42, 53, 93, Fig. 10.” *Id.* at 27.

In that regard, Vrotsos describes: “Generally, the processor 303 is responsible for controlling the hardware components located within the attachment 21. The processor 303 may also include software or code that enables or *executes encryption processing on any transaction data or identification data.*” Ex. 1006 ¶ 80 (emphasis added). Vrotsos further describes: “The wireless communication device **1** may package the encrypted transaction data in a transaction transmission and may send the transaction transmission including the encrypted transaction data to the server **101** over the wireless communication network **550**.” *Id.* ¶ 53. Vrotsos still further describes: “The processor **303** of the attachment **21** may then process the input information (block 405) and the resulting data may be directly transmitted to the antenna **5** of the wireless communication device for transmission to the remote computer 101.” *Id.* ¶ 93.

What Petitioner represents is only that “Vrotsos does not explicitly refer to smart card data being transmitted over that [physical] link.” Pet. 71.

Patent Owner argues:

[I]f one embodiment purportedly expressly disclosed reading, converting, encrypting, and transmitting of information read from a magnetic stripe, but intentionally removed any reference to these functions with regard to information from the integrated circuit of a smart card, that does not suggest the desirability of conflating the two embodiments so much as it suggests that Vrotsos viewed the capability to read, process, encrypt and transmit information from a magnetic stripe as something different than Vrotsos’s own perception of its device’s capabilities with regard to an integrated circuit of a smart card. Ex. 2004, ¶¶ 179–182.

PO Resp. 55. But we do not find that Vrotsos has intentionally removed any reference to the sensing, encryption, and transmission functions with respect to data from the integrated circuit of a smart card. There are numerous

instances where Vrotsos refers to: (1) sensing from the integrated circuit of a smart card, (2) encrypting sensed data from the input device regardless of whether the data comes from a magnetic stripe or an integrated circuit, and (3) transmitting encrypted data to the wireless communication device regardless of whether the data comes from a magnetic stripe or an integrated circuit. Ex. 1006 ¶¶ 41, 53, 78, 80. The circumstance does not reflect what Patent Owner suggests. Rather, Vrotsos specifically describes certain limitations involving reading recorded information from an integrated circuit of a smart card and otherwise uses broad description to cover both data read from an integrated circuit and data read from a magnetic stripe where there is no need for distinction.

For example, Vrotsos describes: “A smartcard read/write head may be positioned within a surface of the deeper channel portion 55 of the slot 22 so that information may be read from or written to the smartchip 53 when the card is positioned within the deeper channel portion 55.” Ex. 1006 ¶ 41. We have determined above that Vrotsos discloses to one with ordinary skill in the art “a sensor for reading said recorded information stored on said integrated circuit incorporated into said card.”

For example, Vrotsos describes: “The processor 303 may also include software or code that enables or executes encryption processing on any transaction data or identification data.” Ex. 1006 ¶ 80. The description covers data read from the integrated circuit of a smart card. Vrotsos also describes: “[T]he processor 303 of the attachment 21 may encrypt input information received from the attachment’s input device 308 so that the resulting attachment-processed data cannot be read off the antenna by the processor of the wireless communication device 1 (or the logical bus) for

misuse by the user.” *Id.* ¶ 78. That description also covers data read from the integrated circuit of a smart card.

For example, Vrotsos describes: “The wireless communication device **1** may package the encrypted transaction data in a transaction transmission and may send the transaction transmission including the encrypted transaction data to the server **101** over the wireless communication network **550**.” *Id.* ¶ 53. That description covers data read from the integrated circuit of a smart card.

Patent Owner’s contention that Vrotsos viewed the capability to read, process, encrypt and transmit information from a magnetic stripe as something different than Vrotsos’s own perception of its device’s capabilities with regard to an integrated circuit of a smart card simply is not supported by the record. Similarly, we also disagree with Patent Owner’s characterization (PO Resp. 56–57) that “even Vrotsos itself drew a stark distinction between a magnetic stripe embodiment and a smart card embodiment.” Patent Owner asserts that “[i]t may be that Vrotsos never intended to transmit information from an integrated circuit onward at all.” PO Resp. 56. The contention is mere speculation and also not supported by the evidence of record. As noted above, Vrotsos describes: “A smartcard read/write head may be positioned within a surface of the deeper channel portion 55 of the slot 22 so that information may be read from or written to the smartchip 53 when the card is positioned within the deeper channel portion 55.” Ex. 1006 ¶ 41. Also as noted above, Vrotsos describes: “The processor 303 may also include software or code that enables or executes encryption processing on any transaction data or identification data.” *Id.* ¶ 80. Further as noted above, Vrotsos describes: “The wireless communication device **1** may package the encrypted transaction data in a

transaction transmission and may send the transaction transmission including the encrypted transaction data to the server **101** over the wireless communication network **550**.” *Id.* ¶ 53.

Patent Owner additionally argues:

Second, Petitioner’s entire argument rests on the premise that magnetic stripe readers and smart card readers use similar reader devices to provide the same function of reading recorded information and sending that information to a mobile phone. Petition, p. 74. They do not. To the contrary, the technologies for reading and working with information from a magnetic stripe are actually very different from those for information on the integrated circuit of a smart card as evidenced at least by the very different physical components, the different ways information is stored on the cards, the different types of signals, and very different industry standards. Ex. 2004, ¶179; *see also* discussion, *supra*.

Id. at 55–56. Patent Owner has mischaracterized Petitioner’s argument. Petitioner on page 74 of the Petition did not assert that the technology for reading from a magnetic stripe is similar to technology for reading from an integrated circuit. Rather, Petitioner states: “Accordingly, regardless of the source of the data (i.e., whether it comes from a magnetic stripe or an integrated circuit), a POSITA would have recognized that Vrotsos’s card reader processes the data read from the card in a similar manner.” Pet. 74. Petitioner is referring to the sensing of data, encrypting of data, and sending of encrypted data to the wireless communication device for further sending to a remote server, not the actual technology regarding how information is read from a magnetic stripe versus how information is read from an integrated circuit. On that basis, Petitioner alternatively asserts that “[a] POSITA would have been motivated to encrypt and transmit transaction data read from a smartchip 53 to securely complete a commercial transaction.”

Pet. 74. We agree. However, we have determined above that Vrotsos discloses encrypting and transmitting transaction data read from smartchip 53.

Patent Owner further argues:

Based on Vrotsos alone, it is more logical to assume that Vrotsos would suggest virtually nothing to a POSITA about the reading and encryption of card information from an integrated circuit because Vrotsos itself does not even demonstrate the ability to read an integrated circuit from a smart card, let alone teach a POSITA how to read, encrypt, and transmit information from an integrated circuit. Ex. 2004, ¶182.

PO Resp. 57. The argument does not undermine Petitioner’s assertions, given the testimony of Michael Shamos that sensors for reading recorded information on an integrated circuit memory of a smart card were well known to one with ordinary skill in the art in 2009. Ex. 1003 ¶ 29; Ex. 1017 ¶¶ 30, 34. Patent Owner’s declarant, Ivan Zatkovich, does not contend otherwise. Even according to Patent Owner, at the time of the invention, there already were industry standards which “defined the methods for reading IC chips embedded in these types of smart cards.” PO Resp. 12–13. Vrotsos does not have to specifically describe what already was well known.

Similarly, neither Patent Owner nor Ivan Zatkovich contends that once information is read from the integrated circuit of a smart card, one with ordinary skill in the art would have lacked sufficient skill to effect encryption of the information and transmission of the encrypted information. Furthermore, Michael Shamos testified that “[e]ncrypting smart card information in the reader module was well known in 2009, because certain standards in the Payment Card Industry (PCI) required it to protect sensitive financial data that could easily be accessed if unencrypted.” Ex. 1017 ¶ 18. Ivan Zatkovich provided no rebuttal testimony in that regard. The record

also does not support any assertion that one with ordinary skill in the art would not have known how to transmit information, once encrypted, from one device to another.

For the foregoing reasons, we are persuaded by Petitioner that Vrotsos reasonably would have suggested “a communication link for coupling said portable smart card reader device to a mobile communication device for the transmission of said encrypted signal indicative of the recorded information therebetween.”

e) Limitation [1.D.1] — wherein clause, part 1

Claim 1 recites “wherein when said sensor reads the recorded information stored on said integrated circuit, said controller converts the recorded information read by said sensor into said encrypted signal.” Ex. 1001, 12:20–25. Petitioner explains that in Vrotsos, when read/write head in input device 308 reads smart card data, processor 303, the controller, performs encryption of that data. Pet. 28 (citing Ex. 1006 ¶¶ 52, 75, 78, 94; Ex. 1003 ¶ C57). The explanation is supported by the cited evidence. Patent Owner does not present arguments additional to those it presents for limitations [1.A] and [1.B]. Those arguments have been discussed and rejected above in the context of the analysis of Vrotsos for limitations [1.A] and [1.B] and need not be reiterated here. We are persuaded that Vrotsos describes this limitation of claim 1.

f) Limitation [1.D.2] — wherein clause, part 2

Claim 1 recites “[wherein when said sensor reads the recorded information stored on said integrated circuit, said controller . . .] transmits said encrypted signal via said communication link to said mobile communication device.” Ex. 1001, 12:20–25. Petitioner asserts that this

limitation is met by Vrotsos and cites to paragraph 93 of Vrotsos which, in pertinent part, describes as follows:

If input is received at the input device (decision block **404**), the processor **303** of the attachment may be awoken from a “sleep state (e.g., a lower-power wait mode) and begin to execute instructions to receive the input information. The processor **303** of the attachment **21** may then process this input information (block **405**) and the resulting data may be directly transmitted to the antenna **5** of the wireless communication device for transmission to the remote computer **101**.

Ex. 1006 ¶ 93 (cited at Pet. 75). Patent Owner does not present arguments additional to those it presents for limitation [1.C]. Those arguments have been discussed and rejected above in the context of the analysis for limitation [1.C] and need not be reiterated here. We are persuaded that Vrotsos describes this limitation of claim 1.

g) Limitation [1.E] — transmission to remote server

Claim 1 recites “said mobile communication device transmits the encrypted signal indicative of the recorded information to a remote transaction server for processing a commercial transaction.” Ex. 1001, 12:16–19. Petitioner explains that in Vrotsos, wireless communication device 1 sends encrypted transaction data indicative of recorded information from the card to remote server 101. Pet. 34 (citing Ex. 1006 ¶¶ 52–53; Ex. 1003 ¶¶ C84–88). Specifically, Petitioner states:

As depicted in Figure 7 of Vrotsos . . . , and explained by Vrotsos at ¶53, the wireless communication device 1 (**red**) sends a transaction transmission to a server 101 (**purple**) over a wireless communications network 550, using a wireless communications protocol such as “CDMA, PCS, GSM, 802.11, or any wireless protocol utilized by any wireless device.” The transaction transmission includes “the encrypted transaction data,” (Ex. 1006, ¶53) from the card (*id.* ¶52).

Pet. 34. Figure 7 of Vrotsos, color annotated by Petitioner and appearing on page 35 of the Petition, is reproduced below:

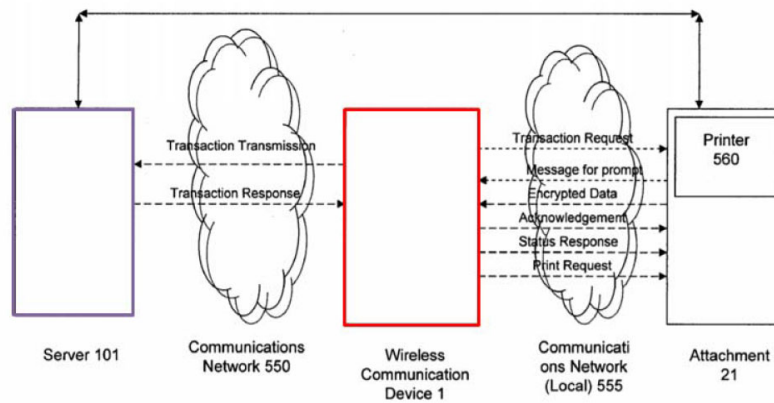


Fig. 7

Figure 7, shown above with color annotation by Petitioner, illustrates a Vrotsos embodiment implementing wireless communication between an attachment and a wireless communication device. Ex. 1006 ¶ 20.

Petitioner's annotations highlight the wireless communication device 1 in red and the server 101 in purple.

With regard to the remote transaction server performing processing of a commercial transaction, Petitioner explains:

That *remote transaction server* performs processing of a *commercial transaction*. Specifically, Vrotsos discloses the server 101 “analyze[s] the transaction transmission . . . to verify authenticity of the user and other server 101 requirements.” Ex. 1006, 54. The server 101 also “send[s] a transaction response to the wireless communication device 1.” *Id.* That response “may be a confirmation number or approval number, a transaction denied request, or a request asking a user or the wireless communication device 1 for additional information.” *Id.* Accordingly, the server 101 *processes a commercial transaction*. Ex. 1003, ¶¶ C89-91.

Pet. 35. Petitioner's assertions are rational and supported by the cited evidence.

Patent Owner does not present counter-argument for this limitation. We are persuaded that Vrotsos describes this limitation of claim 1.

h) Conclusion

For the foregoing reasons, Petitioner has proved by a preponderance of the evidence that claim 1 would have been obvious over Vrotsos.

2. Independent Claim 4

Claim 4 is very similar to claim 1. For instance, claim 1 recites “[a] portable smart card reader device . . . the device comprising: [a] sensor for reading said recorded information stored on said integrated circuit incorporated into said card,” and claim 4 recites “[a] method for reading a smart card having recorded information stored on an integrated circuit incorporated into the card, the method comprising the steps of: providing a portable card reader device comprising a sensor for reading the recorded information stored on the integrated circuit.” Claim 1 recites “[the device comprising . . .] a controller coupled to said sensor for converting the recorded information stored on said integrated circuit into an encrypted signal indicative of the recorded information,” and claim 4 recites a step of “[providing . . .] a controller coupled to said sensor for converting the recorded information into an encrypted signal indicative of the recorded information stored on said integrated circuit incorporated.”

For claim 4, Petitioner relies on its discussion of claim 1. Pet. 75 (citing to Section IX.B.1 of the Petition). Patent Owner similarly relies on its arguments presented for claim 1. PO Resp. 14–16, 18–19, 23–24, 33, 35, 43, 53–57. Our discussion of claim 1 above with respect to the disclosure of Vrotsos equally applies to the preamble and limitations [4.A] through [4.E] and also [4.G] of claim 4. Petitioner has not accounted for, in the context of claim 1, limitation [4.F] of claim 4 which has no corresponding counterpart

in claim 1. However, there is discussion in the Petition, in a different section concerning claim 4, of how limitation [4.F] of claim 4 is met by disclosure in Vrotsos. It appears on pages 40–42 of the Petition. In the Decision on Institution, we determined that it is appropriate to consider it. Paper 9, 35.

Limitation [4.F] reads as follows: “providing said encrypted signal indicative of the recorded information stored on the integrated circuit to said mobile communication device for further processing by circuitry contained in said mobile communication device.” Petitioner explains: “Vrotsos explicitly discloses the wireless communication device packaging data before sending it to a server.” Pet. 43. The assertion is supported by the disclosure of Vrotsos. Indeed, Vrotsos states: “The wireless communication device **1** may package the encrypted transaction data in a transaction transmission and may send the transaction transmission including the encrypted transaction data to the server **101** over the wireless communications network **550**.” Ex. 1006 ¶ 53.

Patent Owner argues, however, that “Vrotsos discloses packaging, but not processing.” PO Resp. 38 (citing Ex. 2004 ¶¶ 149–157). Patent Owner asserts:

“Packaging” does not require any interpretation of the recorded information. Vrotsos makes that clear when it states that the wireless communication device need not be utilized for processing information to be sent to the server. Ex. 1006, ¶80. Presumably, if the wireless device is optional to Vrotsos’s invention, one could assume that the processing of payment information happens independently from the wireless device.

Id. The argument is misplaced. The pertinent part of paragraph 80 of Vrotsos is introducing an embodiment in which information is transmitted to remote server 101 through a local area network rather than through the wireless communication device. Ex. 1006 ¶ 80. In that embodiment, “[t]he

local area network may include or may be coupled to a server or remote computer 101.” *Id.* Petitioner, however, is relying on embodiments which use wireless communication device 1 for transmission to remote computer 101 and thus the associated processing in wireless communication device 1 is not optional. Pet. 43.

Patent Owner further asserts:

The language of claim 4 requires that the information stored on the integrated circuit be “further processed” by circuitry of the mobile communication device before transmitting that information to a transaction server. The limitation of “further processing” is not just reformatting, repackaging or relaying the encrypted signal to the transaction server. The claimed processing requires at a minimum that the information from the card must be extracted from the encrypted signal in order to be processed. Ex. 2004, ¶¶149–157.

The ‘239 patent explains how a mobile communication device is equipped with a “software application . . . used to convert between audio and digital signal.” *See* Ex. 1001, 10:66–11:2, Figs. 7–8. Specifically, “[t]he analog signal from the magnetic card 24 is sent via the hands-free interface 41 where the software application of the controller [in the cell phone] converts the received signal back to binary data for example as stored on the magnetic card 34.” *Id.*, 11:11–14. In fact, this embodiment was also cited by Square to the board as an example of “further processing by circuitry contained in the cell phone.” [citing Ex. 2001, 52–53 (Corrected Petition in IPR2019-00312)]

PO Resp. 38–39. In summary, Patent Owner states: “As the ‘239 patent shows, the limitation of ‘further processing’ minimally requires the data to be extracted in order to be processed.” *Id.* at 39.

Patent Owner’s arguments do not persuade us that “further processing” as recited in claim 4 requires extracting the original data from the encrypted signal. That is an unreasonably restrictive reading of “further processing” in light of the Specification of the ‘239 patent. Indeed, the cited

portion of the Specification is describing only an embodiment, and the introductory sentence, omitted in the above quotation provided by Patent Owner, referring to the software applications identified by Patent Owner, is this: “As such, *in this embodiment*, installation of a software application controller 51 is necessary.” Ex. 1001, 10:65–66 (emphasis added). Nothing indicates that extraction of original data from encrypted data is required to meet the “further processing” limitation. Further, even according to Patent Owner, Petitioner no more than identified the embodiment as an example of what can meet the “further processing” limitation. PO Resp. 39.

We see nothing in the Specification to support the restrictive reading of “further processing” as urged by Patent Owner. “[A] particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment.” *SuperGuide Corp.*, 358 F.3d at 875; *see also In re Van Geuns*, 988 F.2d at 1184.

For the foregoing reasons, Petitioner has proved by a preponderance of the evidence that claim 4 is unpatentable over Vrotsos.

3. *Dependent Claims 2, 3, 5, and 6*

Claim 2 depends directly from claim 1 and further recites “in which the smart card is selected from a group consisting of a chip card, EMV card, proximity detector or NFC card, contactless card, or any combination thereof.” Ex. 1001, 12:30–33. Claim 5 depends directly from claim 4 and further recites the same additional limitation. *Id.* at 12:64–67. Petitioner accounts for the additional limitations of claims 2 and 5, relative to the independent claim from which each claim depends. Pet. 36–37, 43, 66–67, 71.

Claims 3 depends directly from claim 1 and further recites “wherein said mobile communication device receives transaction validation information from said remote transaction server.” Ex. 1001, 12:35–37. Claim 6 depends directly from claim 4 and further recites the same additional limitation. *Id.* at 13:2–4. Petitioner accounts for the additional limitations of claims 3 and 6, relative to the independent claim from which each claim depends. Pet. 37–38, 43–44, 67–68, 71. For instance, Petitioner explains:

Vrotsos describes a server or remote computer 101 transmitting a transaction response to a wireless communication device 1. Ex. 1006, ¶54. The transaction response can be a “confirmation number or approval number.” *Id.* The response may also be “that the transaction could not be completed . . . or that additional information is required from the purchaser or user.” *Id.* ¶96. That transaction response corresponds to transaction validation information that is received by the phone from the server. Accordingly, Vrotsos discloses this claim element. Ex. 1003, ¶¶C108–111.

Pet. 38.

Patent Owner does not present any counter-argument for claims 2 and 3 additional to those it asserts for independent claim 1, and those arguments have been discussed and rejected above in the context of claim 1. Patent Owner does not present any counter-argument for claims 5 and 6 additional to those it asserts for independent claim 4, and those arguments have been discussed and rejected above in the context of claim 4.

We find Petitioner’s reasoning for the additional limitations of claims 2, 3, 5, and 6 to be rational and supported by the cited evidence. Petitioner has shown by a preponderance of the evidence that claims 2, 3, 5, and 6 are unpatentable over Vrotsos.

F. Obviousness of Claims 1–6 over Bear and Vrotsos

We do not reach the alleged ground of unpatentability of claims 1–6 as obvious under U.S.C. § 103 over Bear and Vrotsos, because we conclude that each of these claims is unpatentable on the two other grounds discussed above.

III. CONSTITUTIONAL CHALLENGE

Patent Owner argues that the appointment of Administrative Patent Judges still violates the United States Constitution, Article II, § 2, cl. 2 (Appointments Clause), despite the “attempted cure” by the Federal Circuit in *Arthrex, Inc. v. Smith & Nephew, Inc.*, 941 F.3d 1320 (Fed. Cir. 2019) *cert. granted sub nom. United States v. Arthrex, Inc.*, 2020 WL 6037206 (Oct. 13, 2020). PO Resp. 57–58.

Patent Owner argues that “subjecting a patent filed before September 16, 2012 (date of relevant provisions of AIA), as is the case here, to IPR is an impermissibly retroactive, unconstitutional taking” and “violates the Due Process Clause of the Fifth Amendment.” *Id.* at 58.

We decline to consider Patent Owner’s constitutional challenges. The Federal Circuit has addressed the issue of APJ appointment status in *Arthrex, Inc.*, 941 F.3d at 1325, 1337–38 (“This as-applied severance . . . cures the constitutional violation.”); *see also Arthrex, Inc. v. Smith & Nephew, Inc.*, 953 F.3d 760, 764 (Fed. Cir. 2020) (Moore, J., concurring in denial of rehearing) (“Because the APJs were constitutionally appointed as of the implementation of the severance, *inter partes* review decisions going forward were no longer rendered by unconstitutional panels.”). The Federal Circuit has also addressed the 5th Amendment due process and takings issues in *Celgene Corp. v. Peter*, 931 F.3d 1342, 1362–63 (Fed. Cir. 2019).

IV. CONCLUSION¹⁰

Petitioner has proved by a preponderance of the evidence that claims 1–6 of the '239 patent are unpatentable on the grounds of unpatentability as summarized in the following table:

Claims	35 U.S.C. §	Reference(s)/ Basis	Claim Shown Unpatentable	Claim Not Shown Unpatentable
1–6	103	Valliani, Vrotsos	1–6	
1–6	103	Vrotsos	1–6	
1–6	103	Bear, Vrotsos ¹¹		
Overall Outcome			1–6	

¹⁰ 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).

¹¹ We do not reach the alleged unpatentability of claims 1–6 as obvious under U.S.C. § 103 over Bear and Vrotsos, because each of these claims is already held unpatentable on a different ground.

IPR2019-01651
Patent 9,443,239 B2

FOR PETITIONER:

David M. Tennant
Grace Wang
Bijai Vakil
Hallie Kiernan
WHITE & CASE
dtennant@whitecase.com
grace.wang@whitecase.com
bijal@whitecase.com
hallie.kiernan@whitecase.com

FOR PATENT OWNER:

Jason S. Jackson
Niall A. MacLeod
Jacob Song
KUTAK ROCK LLP
jason.jackson@kutakrock.com
niall.macleod@kutakrock.com
jacob.song@kutakrock.com