

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO INC.,
Petitioner,

v.

CUPP COMPUTING AS,
Patent Owner.

IPR2021-01236
Patent 10,951,632 B2

Before THOMAS L. GIANNETTI, GARTH D. BAER, and
SHARON FENICK, *Administrative Patent Judges*.

GIANNETTI, *Administrative Patent Judge*.

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

I. INTRODUCTION

A. Background

Trend Micro Inc. (“Petitioner”) filed a Petition requesting *inter partes* review of claims 1, 9, 16, and 24 (the “challenged claims”) of U.S. Patent No. 10,951,632 B2 (Ex. 1001, the “’632 patent”). Paper 1 (“Pet.”). CUPP Computing AS (“Patent Owner”) filed a Preliminary Response. Paper 9. Pursuant to 35 U.S.C. § 314, we instituted this *inter partes* review as to all of the challenged claims and all grounds raised in the Petition. Paper 16 (“Institution Dec.”).

Following institution, Patent Owner filed a Response. Paper 25 (“PO Resp.”). Subsequently, Petitioner filed a Reply to Patent Owner’s Response (Paper 28, “Pet. Reply”), and Patent Owner filed a Sur-reply (Paper 30, “PO Sur-reply”).

On October 18, 2022, we held a consolidated oral hearing with IPR2021-01237, also involving the ’632 patent. A transcript of the hearing is included in the record. Paper 36 (“Hearing Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This decision is a Final Written Decision issued pursuant to 35 U.S.C. § 318(a). For the reasons we discuss below, we determine that Petitioner has proven by a preponderance of the evidence that all challenged claims of the ’632 patent are unpatentable.

B. Related Proceedings

The parties identify the following district court proceeding concerning the ’632 patent: *CUPP Cybersecurity LLC v. Trend Micro, Inc., et al.*, No.

3:20-cv-03206 (N.D. Tex.). Pet. 1–2; Paper 7. In addition, Petitioner challenges claims 1, 7, 9, 16, 22, and 24 of the '632 patent in IPR2021-01237 (the “1237 IPR”). A Final Written Decision in the 1237 IPR is being entered concurrently with this Decision.

A closely related patent, U.S. Patent No. 9,843,595 (the “'595 patent”),¹ was before the Board in IPR2019-00765 (the “765 IPR”). A Final Written Decision in the 765 IPR, finding all challenged claims of the '595 patent unpatentable, was entered on August 25, 2020. Ex. 1003. That Decision was appealed to the Federal Circuit and affirmed on November 16, 2022. *CUPP Computing AS v. Trend Micro Inc.*, 53 F.4th 1376 (Fed. Cir. 2022).

C. Real Party-in-Interest

The Petition identifies Trend Micro as the real party-in-interest. Pet. 1. Patent Owner identifies CUPP Computing AS as the real party-in-interest. Paper 7, 1.

D. The '632 Patent

The '632 patent describes a system and method for providing data and device security between external and host devices. Ex. 1001, 1:30–33. According to the patent, mobile devices are more vulnerable to attacks by malicious code when traveling outside an enterprise network. *Id.* at 1:61–65. The patent thus describes “a small piece of hardware [a ‘mobile security system’] that connects to a mobile device and filters out attacks and

¹ The '632 patent is a continuation (through a chain of continuations) of the '595 patent (Ex. 1004), and shares a common specification with the '595 patent.

malicious code.” *Id.* at 5:45–47. The patent explains that “[u]sing the mobile security system, a mobile device can be protected by greater security and possibly by the same level of security offered by its associated corporation/enterprise.” *Id.* at 5:49–52.

This system is illustrated in Figure 3 of the ’632 patent, which follows:

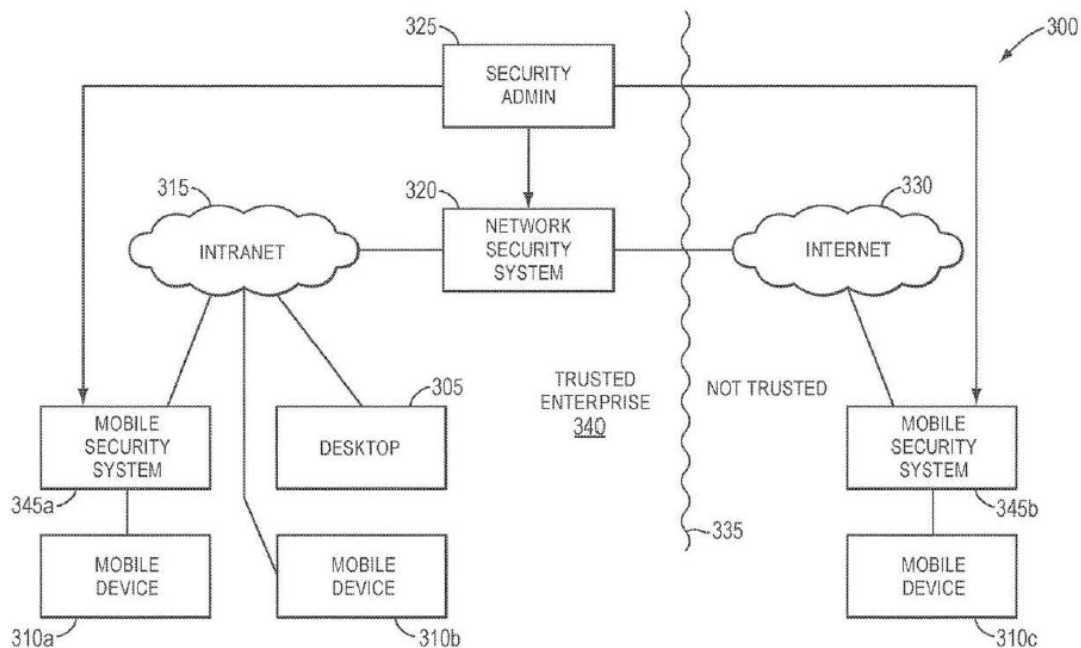


FIG. 3

Figure 3 of the ’632 patent is a block diagram of a network system.

Ex. 1001, 5:53–54. Network system 300 includes desktop 305, first mobile device 310a, and second mobile device 310b. *Id.* at 5:54–56. First mobile device 310a is within trusted enterprise network 340 and is coupled to the enterprise’s intranet 315 via mobile security system 345a. *Id.* at 5:56–59.

Figure 3 further shows mobile device 310c that has travelled outside trusted enterprise network 340 and is coupled to untrusted internet 330 via mobile

security system 345b. *Id.* at 6:3–5. This mobile device may be in use by an employee of trusted enterprise network 340 who is currently on travel. *Id.* at 6:6–7. Security administrator 325 manages mobile security systems 345a and 345b and network security system 320 to assure that they include the most current security protection. *Id.* at 6:7–11.

The '632 patent also describes a wake module configured to wake a mobile device from a power management mode. Ex. 1001, 21:63–64, Fig. 18. According to the patent, a power management mode “is a mode wherein the mobile device conserves power, usually after a predetermined period of inactivity (e.g., no input from a mouse and keyboard).” *Id.* at 21:64–67. During power management mode, the mobile device may reduce or eliminate power to one or more mobile device components such as a display and/or hard drive. *Id.* at 21:67–22:3.

E. Illustrative Claim

Claims 1 and 16 are independent. Claim 1 is representative of the challenged claims. Claim 1 recites²:

- [1.0] A security system, comprising:
 - [1.1] security system memory;
 - [1.2.a] a communication interface configured to communicate with a mobile device and configured to communicate over a network with a security administrator device,
 - [1.2.b] the mobile device including a mobile device processor and including a security agent configured to cooperate with the security system,
 - [1.2.c] the security administrator device having a security administrator processor different than the mobile device

² Paragraph numbering provided by Petitioner has been added.

processor, the mobile device being remote from the security administrator device,

[1.2.d] the mobile device being a first computer system, the security system being a second computer system, the security administrator device being a third computer system, the first computer system, the second computer system and the third computer system being separate computer systems; and

[1.3] a security system processor being different than the mobile device processor and different than the security administrator processor, the security system processor being configured to:

[1.4.a] store in the security system memory at least a portion of wake code, the wake code being configured to detect a wake event and to send a wake signal to the mobile device in response to detecting the wake event,

[1.4.b] the security agent of the mobile device being configured to receive the wake signal, the security agent of the mobile device being configured to wake at least a portion of the mobile device from a power management mode in response to receiving the wake signal, the security agent of the mobile device being configured to perform security services after the at least a portion of the mobile device has been woken;

[1.5] detect a particular wake event;

[1.6] prepare a particular wake signal in response to detecting the particular wake event; and

[1.7.a] send the particular wake signal to the mobile device in response to detecting the particular wake event,

[1.7.b] the security agent of the mobile device being configured to wake the at least a portion of the mobile device in response to receiving the particular wake signal and being configured to perform particular security services after the at

least a portion of the mobile device has been woken.

Ex. 1001, 31:15–58.

F. References and Other Evidence

The Petition relies on the following references:

U.S. Patent App. Pub. No. 2008/0120423 (Ex. 1007, “Hall”).

U.S. Patent App. Pub. No. 2006/0101277 (Ex. 1008, “Meenan”).

U.S. Patent App. Pub. No. 2010/0218012 (Ex. 1009, “Joseph”).

In addition, Petitioner submits the Declaration of Dr. Markus Jakobsson (Ex. 1020, “Jakobsson Decl.”). Patent Owner submits the Declaration of Michael T. Goodrich, Ph.D. (Ex. 2011, “Goodrich Decl.”). The parties also submitted deposition transcripts for those witnesses. Ex. 1026 (“Goodrich Dep.”); Ex. 2015 (“Jakobsson Dep.”). In addition, the parties have submitted expert declarations and deposition transcripts from the 765 IPR.³

G. Asserted Grounds of Unpatentability

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

³ Patent Owner has submitted Dr. Jakobsson’s declaration from the 765 IPR. Ex. 2007. In addition, Petitioner has submitted a deposition transcript of Nenad Medvidovic, Ph.D., from the 765 IPR. Ex. 1027. Dr. Medvidovic testified for Patent Owner in the 765 IPR.

Claims Challenged	Basis (35 U.S.C.) ⁴	Reference(s)
1, 9, 16, 24	§ 103(a)	Hall
9, 24	§ 103(a)	Hall, Meenan
1, 16	§ 103(a)	Joseph
9, 24	§ 103(a)	Joseph, Meenan

Pet. 4.

II. PRELIMINARY MATTERS

A. Level of Ordinary Skill

Petitioner contends “[a] person of ordinary skill in the art at the time of the alleged invention of the ’632 patent (*i.e.*, August 4, 2008) . . . would have had a bachelor’s degree in computer science, electrical engineering, or a comparable field of study, plus at least two years of professional experience with computer security systems, or the equivalent.” Pet. 12 (citing Jakobsson Decl. ¶ 60).

Patent Owner contends “[a] person of ordinary skill in the art of the ’632 Patent would be someone with a bachelor’s degree in computer science or a related field and either (1) two or more years of industry experience and/or (2) an advanced degree in computer science or a related field.” PO Resp. 7 (citing Goodrich Decl. ¶ 30). These formulations are similar, differing mainly in the specific reference, in Patent Owner’s formulation, to

⁴ Because the parties agree that the challenged claims of the ’632 patent have an effective filing date before March 16, 2013, we apply the pre-AIA (“America Invents Act”) version of § 103. Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011).

“an advanced degree in computer science or a related field” as a possible alternative to experience in the field.

We adopt Patent Owner’s description as it is consistent with the prior art and patent specification before us and supported by credible expert testimony. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (prior art itself may reflect an appropriate level of skill). However, our decision would be the same under either formulation.

B. Claim Construction

In an *inter partes* review, the claims of a patent shall be construed using the same claim construction standard that would be used to construe the claims in a civil action under 35 U.S.C. § 282(b), including construing the claims in accordance with the ordinary and customary meaning of such claims as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. 37 C.F.R. § 42.100(b); *see also Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005). Under that standard, and absent any special definitions, we give claim terms their ordinary and customary meaning, as would be understood by one of ordinary skill in the art at the time of the invention. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). Any special definitions for claim terms must be set forth with reasonable clarity, deliberateness, and precision. *See In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

We construe claim terms only as relevant to the parties’ contentions and only to the extent necessary to resolve the issues in dispute. *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999);

Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co., 868 F.3d 1013, 1017 (Fed. Cir. 2017).

1. power management mode (all challenged claims)

This term has been construed in the 765 IPR and in district court litigation involving the '595 patent as “a mode where the mobile device conserves power.” Pet. 12; PO Resp. 18–19. There is no dispute over this construction. *See* Ex. 1006, 6.⁵ The construction is supported by the '632 patent specification. *See* Ex. 1001, 21:62–64 (“A power management mode is a mode wherein the mobile device conserves power.”). We, therefore, agree with this construction, and we adopt it for this decision.

2. security administrator device (all challenged claims)

Petitioner contends “the plain and ordinary meaning of this term includes a device that performs security administration.” Pet. 13 (citing Jakobsson Decl. ¶ 65). Petitioner asserts that “[t]his is consistent with the '632 patent’s disclosure that the security administrator device 325 may perform various security administration tasks.” *Id.*

Patent Owner responds that “[t]his term is defined in the '632 Patent as a device that manages the security of a security system.” PO Resp. 15 (citing Ex. 1001, 6:7–11) (emphasis omitted). Patent Owner asserts that “Petitioner’s proposed construction includes the phrase ‘security administration,’ but it is unclear as Petitioner leaves unsaid what ‘security administration’ does and does not encompass.” *Id.* at 17.

⁵ Unless otherwise indicated, citations to exhibits use the page numbers assigned by the parties, not the original page numbers.

We are persuaded to adopt Petitioner’s construction. Petitioner’s construction reflects its position that “[i]n no place do the claims recite that the ‘security administrator device’ must manage the ‘security system,’ let alone manage the security of the security system.” Pet. Reply 12. We agree that a security administrator device need not “*manage*” the security of a security system as Patent Owner asserts. PO Resp. 15. Our construction is consistent with the term’s plain language as well as the ’632 patent claims and is supported by expert testimony. Jakobsson Decl. ¶ 65.

As Petitioner points out, the claims themselves make no mention of managing the security of a security system. Pet. Reply 12. Claim 1 recites that the security system is “configured to communicate over a network with a security administrator device.” Ex. 1001, 31:18–19. Claim 16 recites that the security administrator device is “a third computer system,” but does not recite a relationship between the security administrator device and the security system. *Id.* at 32:61–63; *see also* Jakobsson Decl. ¶ 65 (“The plain and ordinary meaning of this term includes a device that performs security administration.”).

Petitioner’s construction also is consistent with the ’632 patent’s disclosure that the security administrator device may perform various security administration tasks. Pet. 13; Ex. 1001, 24:55–57 (describing security administrator 325 as an “administrator device”). As Petitioner points out, “[a]lthough management is a type of administration, administration includes other activities more broadly related to running a system, such as maintaining routing tables.” Pet. Reply 13 (citing Ex. 1001, 12:28–30; Ex. 1024, 3).

We do not agree with Patent Owner’s argument that Petitioner’s proposed construction is “unclear.” PO Resp. 17. As Petitioner points out, the relationship between the security system and the security administrator device is recited in the claims. Pet. Reply 12. The claims do not recite that the security administrator device manages the security device, “let alone manage[s] the security of the security system.” *Id.*

We do not agree with Patent Owner’s argument that the term “security administrator device” is “defined in the ’632 Patent.” PO Resp. 15 (citing Ex. 1001, 6:6–11). We are not convinced that the reference to this phrase in the ’632 patent specification cited by Patent Owner sets forth with sufficient “clarity, deliberateness, and precision” a lexicographic definition. *See Renishaw PLC v. Marposs Societa’ per Azioni*, 158 F.3d 1243, 1249 (Fed. Cir. 1998); *In re Paulsen*, 30 F.3d at 1480. Instead, Patent Owner’s argument is an attempt to incorporate limitations from a particular embodiment that are not recited in the claims. *See* Pet. Reply 13–14.

We, therefore, do not adopt Patent Owner’s proposed construction for this term. Adopting Petitioner’s construction, we construe the term as “a device that performs security administration.” Pet. 13; Jakobsson Decl. ¶ 65.

3. *particular wake event/particular wake signal/particular security services (all claims)*

Patent Owner contends that “[t]aken as a whole, these claim elements recite a technique whereby a wake event triggers a particular *type* of wake signal, which triggers the mobile device’s security for a particular *type* of security service.” PO Resp. 7–8. Citing Merriam-Webster’s dictionary, Patent Owner contends that “[t]his interpretation is consistent with the plain

and ordinary meaning of the word ‘particular,’ which is ‘of, relating to, or being a single person or thing’” *Id.* at 8 (citing Ex. 2012, 3).

Petitioner responds that a “particular” wake signal includes one that is distinguishable from other wake signals, such as a wake signal that occurs at a specific time.” Pet. Reply 1. Therefore, “[a] wake signal that occurs at a specific time is a specific, single, and individual wake signal, distinguishable from wake signals that occurred at other times. Thus, it is a ‘particular’ wake signal.” *Id.* at 2. Petitioner argues that the Board should reject Patent Owner’s argument “that these claim terms should be limited to a ‘particular type of’ wake signal, wake event, and security service.” *Id.* at 4–5.

We agree with Petitioner that the claims should not be limited to a particular *type* of wake event or signal. The claims themselves recite a “particular wake signal,” not a particular *type* of wake signal. The same is true for wake events. Patent Owner’s argument would, therefore, require us to rewrite the claims to make a distinction between what Patent Owner refers to as “generic” wake signals and events and “particular” wake signals and events. *See* Hearing Tr. 38:26–39:7, 41:6–19. This distinction is not reflected in the claims or specification.

At the oral hearing, Patent Owner’s counsel was questioned by the panel exploring the differences between particular and generic wake events. Hearing Tr. 50:10–51:3. Ultimately, Patent Owner’s counsel acknowledged that a wake event occurring at every hour could be a particular wake event:

[THE BOARD:] What if there was a wake event that was wake at noon and a wake event that was wake at midnight? . . . [W]ould one of those qualify as a particular wake event?

[PATENT OWNER'S COUNSEL:] Yeah. I believe each one because that's the -- what's described and what's claimed is that you -- there is a particular wake event which has to be detected. It's not limited to only one, so it could be -- it could be every hour. *There could be a particular wake event which is each hour.* So, you know, *that's the particular wake event.* Or it could be just, like you said, at noon -- or at noon or at midnight. *Those would each be a particular wake event.*

And then what the claim says or requires is that for each particular wake event, there has to be a particular wake signal that's associated with that particular. And it could be that what you do at noon or what you do at midnight *are the same*, or it could be different. And then from whatever that particular wake signal is for that particular wake event, then you have a particular security service that's offered.

Hearing Tr. 50:10–51:3 (emphasis added).

Patent Owner argues that “[u]nder Petitioner’s interpretation, the Challenged Claims would have the same meaning with and without the word ‘particular’ because *every* detected wake event would occur at some point in time.” PO Resp. 11; *see also* PO Sur-reply 1 (“Petitioner’s proposal . . . should be rejected because it renders the word ‘particular’ superfluous.”). We disagree that under Petitioner’s construction, the term “particular” would be meaningless or superfluous. We agree with Petitioner and find that “[a] signal sent at time T_1 is not the same signal sent at time T_2 .” Pet. Reply 2. As Petitioner explains, “[a]lthough the signals may have the same form, each is individually identifiable.” *Id.* Two wake signals of the same form sent at the same time would not be “particular” wake signals because they would not be distinguishable on the basis of time. *Id.* at 2–3. Thus, we find that Petitioner’s interpretation provides a meaningful

identification of particular wake events and wake signals. For the reasons given we adopt Petitioner's construction of these claim elements.

This construction will be further discussed in Section III.B, *infra*, in connection with our consideration of the prior art.

4. security agent (all claims)

Patent Owner contends that “[t]he plain and ordinary meaning of the term ‘security agent’ is a security system situated within and a part of an environment that senses that environment and acts on it, over time, in pursuit of its own agenda and so as to effect what it senses in the future.” PO Resp. 12 (emphasis omitted). For support, Patent Owner relies on a paper by Franklin titled “Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents.” *Id.* (citing Ex. 2013, 1).

Petitioner responds that “Patent Owner’s construction comes from Franklin’s definition of ‘autonomous agent,’ not ‘security agent’ or ‘agent.’” Pet. Reply 6. Petitioner explains that “Franklin . . . acknowledges that some agents may not be autonomous.” *Id.* (citing Ex. 2013, 6). Petitioner presents several “broader” dictionary definitions of “agent.” *Id.* at 7–8 (citing Exhibits 1023 (from “Barron’s Dictionary of Computer and Internet Terms”), 1014 (from “Concise Oxford English Dictionary”) and 1025 (from “Merriam-Webster’s Collegiate Dictionary”)). Petitioner contends that Merriam-Webster’s definition (“a computer application [sic⁶] designed to

⁶ The correct quote from the dictionary is “a computer *program* designed to automate certain tasks.” Ex. 1025, 3 (emphasis added). We do not regard this minor error as affecting our analysis.

automate certain tasks”) has been adopted as an “accepted, ordinary meaning” in another proceeding. *Id.* at 8.

Petitioner contends that Patent Owner’s construction is unsupported by the intrinsic evidence. Pet. Reply 9–10. Petitioner explains that in the ’632 patent, the cited security agent does not act “in pursuit of its own agenda” because it sometimes acts on behalf of the mobile security system. *Id.* at 9 (citing Ex. 1001, 28:25–28, 28:44–53).

We agree with Petitioner that Patent Owner’s construction based on Franklin is not supported by the intrinsic evidence. First, neither the written description nor the claims of the ’632 patent themselves recite “autonomous agent.” Nor do Patent Owner’s references to the specification demonstrate that the agent described in the ’632 patent acts “in pursuit of its own agenda.” PO Resp. 12–13. In addition, Franklin presents “autonomous” as a property of a special type of agent, one where the agent “exercises control over its own actions.” Ex. 2013, 5–6. For the reasons given, we are not persuaded that the “security agent” recited in the ’632 patent claims and described in the specification is an “autonomous” agent as discussed in Franklin. We, therefore, do not adopt Patent Owner’s construction for “security agent.” Instead, we adopt the plain and ordinary meaning best expressed by Merriam-Webster, namely, “a computer program designed to automate certain tasks.” Ex. 1025, 3.

C. Description of the Principal Prior Art References

1. Joseph

Joseph is a published patent application titled “Methods and Systems for Providing a Wireless Security Service and/or a Wireless Technical Support Service for Personal Computers.” Ex. 1009, (54). Petitioner

contends that Joseph's effective date as prior art is at least as early as May 26, 2008. Pet. 45. Petitioner contends that this date is before the earliest possible effective filing date for the '632 patent, thus qualifying Joseph as prior art under pre-AIA 35 U.S.C. § 102(e). *Id.* Patent Owner does not challenge Joseph's availability as prior art.

Joseph is directed to “enhancing security of personal computers and facilitating recovery of stolen, lost or otherwise missing personal computers.” Ex. 1009 ¶ 7. Joseph discloses providing the laptop computer with an “integrated” security diagnostics unit (“SDU”). *Id.* ¶ 60.

The SDU provides wireless security service or wireless technical support services to the laptop computer. *Id.* The SDU communicates with a network entity referred to as a “security/technical support entity” at a remote location by sending and receiving messages via a wireless network. *Id.* ¶ 61.

The SDU is shown as element 14 in Figure 3 of Joseph, reproduced here:

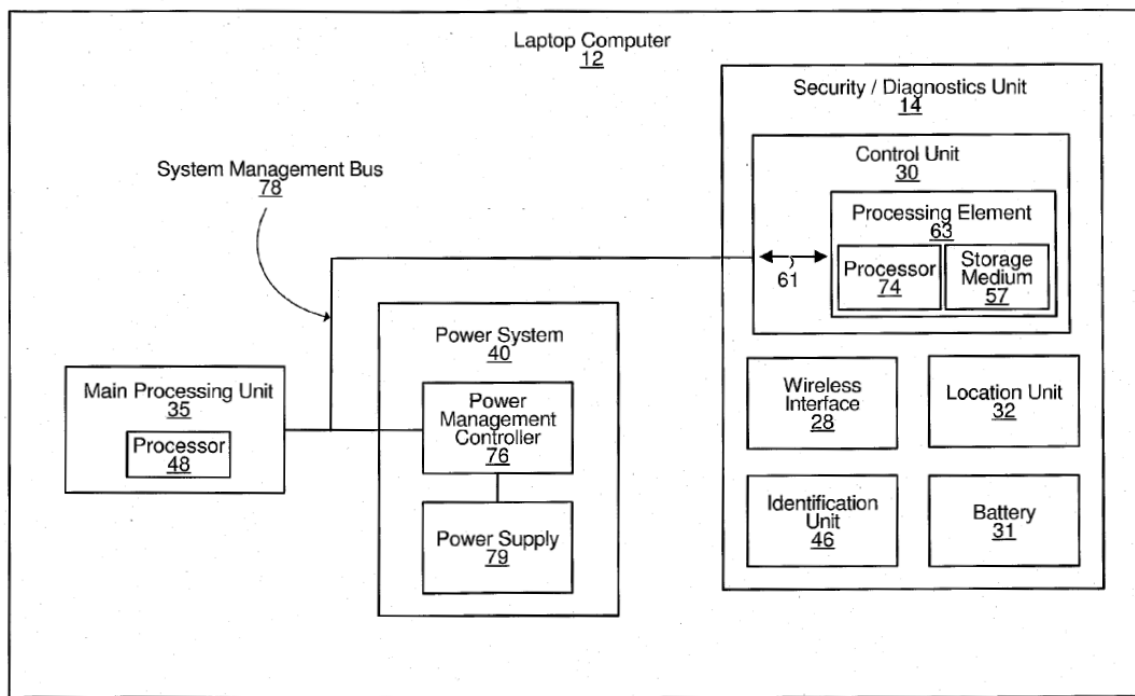


FIG. 3

Figure 3 of Joseph is a block diagram showing personal computer 12 including SDU 14. *Id.* ¶¶ 39, 79. SDU 14 is connected to power management system 40 of the personal computer through system management bus 78. *Id.* SDU 14 includes control unit 30, which contains hardware and software for implementing interface 61 and processing element 63. *Id.* ¶ 73. The processing element comprises one or more processors 74 for performing processing operations to implement the functionality of the control unit. *Id.* ¶ 74. These processors may be general purpose computers that execute code to implement the functionality of control unit 30. *Id.* As shown in Figure 3, these processors are different

from processor 48 that is part of main processing unit 35 of the laptop computer. *Id.* ¶ 54.

Figure 14 of Joseph is reproduced here:

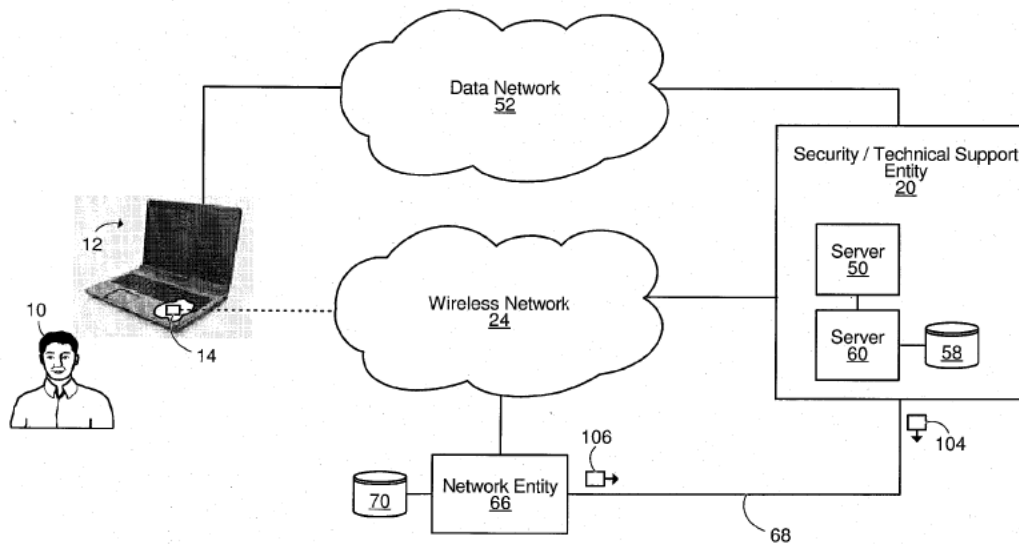


FIG. 14

Figure 14 shows a process by which a user may register for and activate the wireless security service or the wireless technical support service. Ex. 1009 ¶ 200. Security/technical support entity 20 includes server 50 connected to data network 52 (e.g., the Internet). *Id.* ¶ 201. User 10 uses laptop computer 12 to interact with the network site implemented by server 50 to register for the wireless security service and the wireless technical support service. *Id.* ¶ 202.

The network site implemented by server 50 prompts user 10 to enter registration information. *Id.* ¶ 205. Server 60 causes transmission of message 104 to network entity 66 operated by the wireless network provider. *Id.* ¶ 207. Message 104 is a request to obtain from the wireless network

provider “activation information,” to be subsequently transmitted to SDU 14 via wireless network 24 in order to activate the SDU on the personal computer. *Id.* ¶ 208.

Having obtained the activation information, network entity 66 sends message 106 conveying the activation information to server 60 via communication link 68. *Id.* ¶ 212. Server 60 passes this information to server 50. *Id.* ¶ 213. Upon completion of the registration phase, the network site implemented by server 50 informs the user that registration is completed and instructs the user to proceed to the activation phase. *Id.* ¶ 215.

An objective of the activation phase is to activate SDU 14, i.e., to cause the SDU to be granted access to wireless network 24 by the wireless network provider such that the SDU can communicate with security/technical support entity 20 via wireless network 24. *Id.* ¶ 217. During the activation process, server 60 transmits a message to SDU 14 via wireless network 24. *Id.* ¶ 229. Prior to transmission of this message, the SDU is in sleep mode. *Id.* This message conveys a command to put the sleeping SDU in wake mode. *Id.*

In response to receiving this message, SDU 14 puts itself in wake mode. *Id.* ¶ 230. SDU 14 also sends a message to server 60 via wireless network 24 to acknowledge receipt of the “wake up” message and confirm that it is in wake mode. *Id.* Upon receiving this message, server 60 determines that the SDU has received message 148 and placed itself in wake mode. *Id.* ¶ 231. The server proceeds to transmit a message to the SDU via

wireless network 24 that conveys a command to put the SDU in sleep mode. *Id.*

In response to receiving this message, the SDU puts itself back in sleep mode. *Id.* ¶ 232. SDU also sends a message to server 60 via wireless network 24 to acknowledge receipt of the message and confirm that it is in sleep mode. *Id.*

Upon receiving this message, the server determines that the SDU has received the message and placed itself in sleep mode. *Id.* ¶ 233. The server concludes that the SDU is operating correctly and that the wireless security service and the wireless technical support service have been activated. *Id.*

2. *Hall*

Hall is a published patent application titled “System and Method of Actively Establishing and Maintaining Network Communications for One or More Applications.” Ex. 1007, (54). Petitioner contends that Hall’s effective date as prior art is at least as early as May 22, 2008. Pet. 14. Petitioner contends that this date is before the earliest possible effective filing date for the ’632 patent, thus qualifying Hall as prior art under pre-AIA 35 U.S.C. §§ 102(a) and (e). *Id.* Patent Owner does not challenge Hall’s availability as prior art.

Figure 1 of Hall follows:

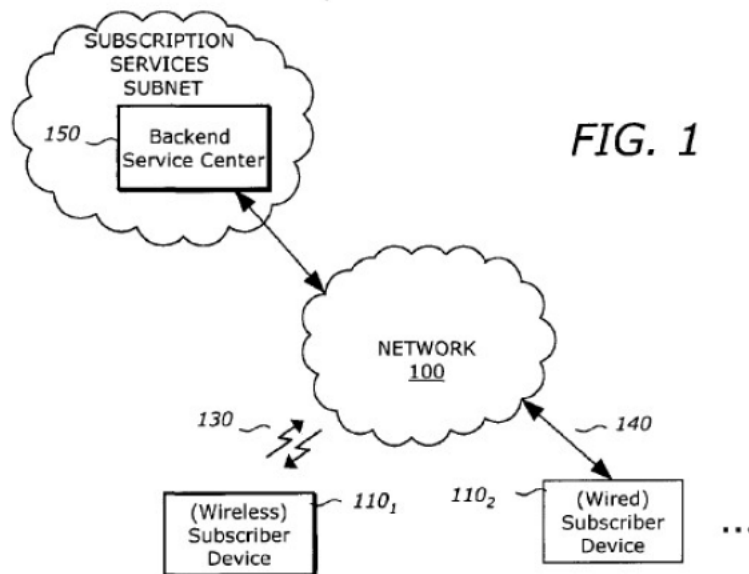


Figure 1 illustrates a network with subscribers 110₁ and 110₂ implemented with backend service center 150. Ex. 1007 ¶ 7. As shown in Figure 1, subscriber device 110₁ is in communication with backend service center 150, which includes a collection of one or more databases and/or network servers. *Id.* ¶ 33.

Each subscriber device is provided with a communication module (referred to as “MySync module”), which is a series of instructions that run as a Windows Service. *Id.* ¶ 37. The MySync module communicates with the backend service center and performs various services on the laptop, including security services. *Id.* ¶¶ 42–45. For example, the backend service center may send a wake-up signal to the laptop and instruct the laptop to perform security services if the laptop has been reported stolen. *Id.*, Fig. 12, ¶¶ 100–104.

III. ANALYSIS OF THE CHALLENGED CLAIMS

The Petition challenges claims 1, 9, 16, and 24 of the '632 patent. Petitioner asserts unpatentability of the claims based on obviousness. Pet. 3–4.

A. Obviousness

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007).

The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) so-called “secondary considerations,” including commercial success, long-felt but unsolved needs, failure of others, and unexpected results. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966) (“the *Graham* factors”). Neither the Petition nor the Patent Owner Response presents evidence on the fourth *Graham* factor. We therefore do not consider that factor in this decision.

B. Challenges Based on Joseph

Petitioner contends claims 1 and 16 would have been obvious over Joseph and claims 9 and 24 would have been obvious over Joseph and Meenan. Pet. 4.

1. Claim 1

Petitioner asserts that each element of claim 1 is disclosed or suggested by Joseph. Pet. 45–64; Jakobsson Decl. ¶¶ 134–172. Petitioner's

element-by-element analysis of claim 1 in relation to Joseph appears at pages 47–63 of the Petition. Petitioner supports its analysis with testimony by its expert, Dr. Jakobsson. Jakobsson Decl. ¶¶ 139–172.

Patent Owner’s principal argument challenges Petitioner’s assertion that Joseph teaches “particular” wake events and wake signals as claimed. PO Resp. 32–33. Patent Owner contends that “Petitioner only argues that *Joseph* teaches ‘particular’ wake events and wake signals because they ‘would occur at a specific time’ or ‘sent at a specific time,’ respectively.” *Id.* at. 32. Patent Owner continues that “[b]ecause the word ‘particular’ cannot refer merely to a something that occurs at a specific time, Petitioner’s arguments about how *Joseph* allegedly teaches these limitations necessarily fails.” *Id.* We do not agree with this argument by Patent Owner because it is based on a construction of the terms “particular wake event” and “particular wake signal” that we do not adopt. *See* Section II.B.3, *supra*.

For the reasons that follow, we determine that Petitioner has demonstrated by a preponderance of evidence that Joseph teaches or suggests each element of claim 1.

a. Preamble [1.0]

The preamble of claim 1 recites a “security system.” Petitioner contends this element is found in Joseph’s security/technical support entity 20. Pet. 47 (citing Ex. 1009, Fig. 14, ¶ 61). Patent Owner’s Response does not challenge this contention.

We find that for the reasons given, Petitioner demonstrates that Joseph teaches the preamble of claim 1.⁷

b. Claim element 1.1

Claim element 1.1 calls for a “security system memory.” Petitioner contends this element is met by the memory “inherently and necessarily” present in server 50, server 60, and database 58 in Joseph. Pet. 48–49 (citing Jakobsson Decl. ¶ 141). Patent Owner’s Response does not challenge this contention.

We find that for the reasons given, Petitioner demonstrates that Joseph teaches element 1.1 of claim 1.

c. Claim element 1.2.a

This claim element calls for “a communication interface configured to communicate with a mobile device and configured to communicate over a network with a security administrator device.” Petitioner identifies network entity 66 in Joseph as the claimed “security administrator device.” Pet. 49. According to Petitioner, “[t]he network entity 66 is a security administrator device because it is used for administrative tasks such as user registration and security service activation for Joseph’s security services.” *Id.* at 49–50 (citing Ex. 1009 ¶¶ 205–212, 222–227, Figs. 14, 15). *See also* discussion of registration and activation in Joseph, *supra*, Section II.C.1.

Patent Owner challenges Petitioner’s identification of network entity 66 in Joseph as the claimed “security administrator device.” PO Resp. 39–40. According to Patent Owner, “*Joseph*’s network entity 66 does not

⁷ We do not express an opinion on whether the preambles of the ’632 patent claims are limiting.

manage the security engines and security policies and data of a security system, as required by the claim language.” *Id.* at 39. For reasons that follow, we do not agree with Patent Owner’s contention.

Referring to the petition in the 595 IPR, Patent Owner contends that “[n]owhere did Petitioner mention that network entity 66 is part of *Joseph’s* architecture that maps to a security administrator device.” PO Resp. 39. Petitioner responds that this observation regarding the 595 IPR “is irrelevant.” Pet. Reply 25. We agree. As we stated in our Institution Decision, a petitioner may analyze a prior art reference differently in two different proceedings, including identifying different elements of the prior art with similar elements of different claims. Institution Dec. 35. We therefore analyze the disclosure of the reference to determine whether it supports the Petitioner’s contentions in this proceeding.

Patent Owner contends “*Joseph’s* network entity 66 does not manage the security engines and security policies and data of a security system, as required by the claim language.” PO Resp. 39. Patent Owner explains that “the network entity merely processes message requests.” *Id.* Further, “the network entity 66 merely retrieves activation information that is intended for the SDU 14; it does not manage the security of a security system.” *Id.* at 40.

We do not agree with Patent Owner’s argument because it is based on a construction of “security administrator device” that we did not adopt. *See supra*, Section II.B.2. Patent Owner’s construction would require “a device that manages the security of a security system.” PO Resp. 15 (emphasis omitted). Instead, we adopt Petitioner’s construction based on plain and ordinary meaning, which is “a device that performs security administration.” Pet. 13 (citing Jakobsson Decl. ¶ 65). Under this construction, *Joseph’s*

network entity 66 is a security administrator device because it performs user activation and user registration, which are administrative tasks. *Id.* at 49–50; *see* description in Section II.C.1, *supra*.

Further, Petitioner contends Joseph meets the “network interface” limitation of this claim element because “security/technical support entity 20 (a security system) includes a network interface (a communication interface) to communicate with laptop 12 (a mobile device) and network entity 66 (a security administrator device) over a network.” Pet. 50 (citing Ex. 1009, Fig. 14). Petitioner reasons that in order to communicate over a network, security/technical support entity 20 “necessarily and inherently includes a network interface (a communication interface) to communicate with both laptop 12 and network entity 66.” *Id.* at 51–52 (citing Jakobsson Decl. ¶ 145). Patent Owner does not challenge this contention.

We find that for the reasons given, Petitioner demonstrates that Joseph teaches element 1.2.a of claim 1.

d. Claim element 1.2.b

This claim element calls for “the mobile device including a mobile device processor and including a security agent configured to cooperate with the security system.” Petitioner asserts Joseph discloses this element. Pet. 52–53; Jakobsson Decl. ¶¶ 146–148. Referring to Figure 2 of Joseph, Petitioner asserts “[a]t least processor 48, power system 40, and SDU 14 together are the claimed ‘security agent.’” Pet. 52.

Patent Owner challenges Petitioner’s identification of the claimed “security agent” in Joseph. PO Resp. 34–38. Referring to the language of claim element 1.7.b, Patent Owner contends that Joseph does not disclose a security agent configured to “wake the at least a portion of the mobile device

in response to receiving the particular wake signal” and “perform particular security services after the at least a portion of the mobile device has been woken” because Joseph does not disclose any “particular wake signal” or “particular security services.” *Id.* at 34. We do not agree for the reasons given in Section III.B.1.i, *infra*.

Patent Owner contends also that “[i]n the embodiments [of Joseph] in which the SDU wakes itself, neither it nor any other components of the mobile device perform security services . . . in response to receiving a particular wake signal.” PO Resp. 34–35. We disagree. As Petitioner points out, the claims require performing the particular security services *after* at least a portion of the mobile device has been woken (not *in response to* a particular wake signal as Patent Owner asserts). Pet. Reply 22. We agree with Petitioner that the claims require a temporal relationship between the security services and wake event, not a causal one. *Id.* at 17 (“‘After’ recites a temporal relationship, not a causal relationship.”) Petitioner demonstrates that the SDU, once awakened, performs a variety of security services. *Id.* at 61–62 (citing Ex. 1009 ¶¶ 75, 134–135, 144; Jakobsson Decl. ¶ 164). *See also* the discussion in Section III.B.1.h, *infra*. Petitioner shows that these security services occur after SDU 14 receives a wake signal (message 148). Pet. 62; Jakobsson Decl. ¶ 166 (citing Ex. 1009 ¶¶ 228–229).

Patent Owner further contends that Joseph’s power system and processor are not part of the security agent. PO Resp. 36–38. Relying on its proposed construction for “security agent” (which we do not adopt, *see* Section II.B.4, *supra*), Patent Owner contends that “[a person of ordinary skill] also would recognize that the ‘power system’ and ‘processor 48’ in

Joseph are not components that operate consistent with how a [person of ordinary skill in the art] would interpret the term security agent.” *Id.* at 37.

We do not agree with these arguments by Patent Owner. Petitioner demonstrates that Patent Owner’s arguments are not supported by the claims or specification. Pet. Reply. 24. The claims do not indicate that a “security agent” cannot include multiple modules, and the specification discloses that the security agent may have multiple components. *Id.* (citing Ex. 1001, 28:11–20, 28:25–32, Fig. 19).

Petitioner responds (and we agree) that “Patent Owner’s argument that *Joseph* does not disclose a ‘security agent’ because it does not disclose a ‘particular wake signal’ or ‘particular security services’ fails because it is based on an incorrect claim construction.” Pet. Reply 23; *see* Section II.B.3, *supra*. We find that *Joseph* discloses the claimed “particular” wake event and wake signal. *See* Section III.B.1.i, *infra*.

Nor do we agree with Patent Owner’s other arguments, for example, that the SDU is “already awake” when it sends that control signal, or that the power system “is in a coma until it is called and returns to a coma once it finishes running.” PO Resp. 35–37. The “already awake” argument is unavailing because it suggests that the SDU is not awakened before the security services are performed. Pet. Reply 22. As Petitioner points out, however, the SDU switches to wake mode in response to a wake command before processing the commands for various security services. *Id.* Similarly, Patent Owner’s “in a coma” argument fails because “running continuously is not [a] requirement of a security agent” under Patent Owner’s proposed construction or under our adopted construction. *See supra*, Section II.B.4.

We find that for the reasons given, Petitioner demonstrates that Joseph teaches element 1.2.b of claim 1.

e. Claim element 1.2.c

This claim element calls for “the security administrator device having a security administrator processor different than the mobile device processor, the mobile device being remote from the security administrator device.” Petitioner refers back to its analysis of element 1.2.a. Pet. 54. Petitioner contends “Joseph’s network entity 66 (security administrator device) necessarily and inherently includes a processor because network entity 66 performs a number of tasks, including receiving, processing, and sending messages for user registration and security service activation.” *Id.* (citing Ex. 1009 ¶¶ 211–216). Petitioner contends the processors of laptop 12 and network entity 66 are “different” because they are “distinct devices” and are “remote” because they are separated. *Id.* at 54–55.

Patent Owner does not challenge this particular assertion by Petitioner although, as discussed *supra*, in Section III.B.1.c, Patent Owner does challenge Petitioner’s identification of the security administrator device in Joseph. *See* PO Resp. 39. This argument challenging Petitioner’s identification of a security administrator device in Joseph is discussed in Section III.B.1.c, *supra*. For the reasons given there, we do not agree with this argument by Patent Owner.

We find that for the reasons given, Petitioner demonstrates that Joseph teaches element 1.2.c of claim 1.

f. Claim element 1.2.d

This claim element calls for “the mobile device being a first computer system, the security system being a second computer system, the security administrator device being a third computer system, the first computer system, the second computer system and the third computer system being separate computer systems.” Petitioner asserts that Joseph discloses this element because “Joseph’s laptop 12 (mobile device), security/technical support entity 20 (security system), and network entity 66 (security administrator device) all are separate computer systems.” Pet. 55–56 (citing Ex. 1009, Fig. 14).

Patent Owner addresses the “separate computer” limitation only briefly in discussing the related ’595 patent and the pending Federal Circuit appeal of the 765 IPR involving the ’595 patent. PO Resp. 5 & n.1. Beyond stating that the “architecture” of Joseph “does not include or contemplate such separate computer systems,” Patent Owner does not provide any further explanation or evidence on that point in the course of its analysis of Joseph. *Id.* at 6. Accordingly, we do not further consider this statement.⁸

⁸ Patent Owner states that “[t]his additional [‘separate computer’] limitation directly addresses the ’595 FWD’s reasoning that the claims of the ’595 Patent did not limit the mobile device and security system to separate systems and thus were unpatentable. *See, e.g.*, ’595 FWD at 23, 28-29, 38.” PO Resp. 6. If by this statement Patent Owner is attempting to rely in this proceeding on its “separate computer” arguments in the 765 IPR, we consider that an improper incorporation by reference and do not consider those arguments. *See* 37 C.F.R. § 42.6(a)(3) (prohibiting incorporating arguments by reference from one document into another).

We find that for the reasons given, Petitioner demonstrates that Joseph teaches element 1.2.d of claim 1.

g. Claim elements 1.3 and 1.4.a

These claim elements, together, call for “a security system processor being different than the mobile device processor and different than the security administrator processor, the security system processor being configured to store in the security system memory at least a portion of wake code, the wake code being configured to detect a wake event and to send a wake signal to the mobile device in response to detecting the wake event.”

Petitioner identifies Joseph’s server 50, server 60, and database 58 as having processors that, “individually and collectively,” are the claimed “security system processor.” Pet. 57. Petitioner asserts the processors of security/technical support entity 20 and network entity 66 are different processors “because these two systems are separate from one another.” *Id.* at 58.

Petitioner explains that in Joseph, during security service activation, security/technical support entity 20 sends a wake signal to SDU 14, initially in sleep mode, to put the SDU in wake mode. *Id.* (citing Ex. 1009 ¶¶ 229–230). *See* discussion in Section II.C.1, *supra*. Petitioner identifies this as a wake signal because it changes the SDU from sleep mode to wake mode. Pet. 58–59.

Petitioner identifies the authorization in Joseph as a wake event “because it is the event that triggers security/technical support entity 20 to send message 148 (wake signal) to wake up SDU 14.” *Id.* at 59. Petitioner describes other wake signals in Joseph including the waking of a stolen laptop after being recovered. *Id.* (citing Ex. 1009 ¶¶ 96–97, 126–127, 158–

160). Petitioner explains that “every wake signal sent by the security/technical support entity 20 necessarily is in response to the occurrence of some well-defined state (in response to detecting a wake event) because it does not send the wake signals randomly.” Pet. 59 (citing Jakobsson Decl. ¶ 159).

Petitioner asserts also that Joseph discloses the recited “wake code.” Because the security/technical support entity sends wake signals to the laptop containing the SDU, that entity “necessarily and inherently includes instructions stored in its memory to perform this functionality, and those instructions are wake code.” *Id.* at 59–60 (citing Jakobsson Decl. ¶ 160).

Patent Owner does not challenge the assertion that Joseph meets claim elements 1.3 and 1.4.a in this proceeding.

We find that for the reasons given, Petitioner demonstrates that Joseph teaches elements 1.3 and 1.4.a of claim 1.

h. Claim element 1.4.b

This claim element calls for “the security agent of the mobile device being configured to receive the wake signal, the security agent of the mobile device being configured to wake at least a portion of the mobile device from a power management mode in response to receiving the wake signal, the security agent of the mobile device being configured to perform security services after the at least a portion of the mobile device has been woken.”

Petitioner contends Joseph discloses this “security agent” element by describing a laptop containing an SDU configured to receive messages (wake signals) because on receiving the messages, the laptop wakes up from a sleep mode to a wake mode. Pet. 60; Jakobsson Decl. ¶ 161. Petitioner contends Joseph’s sleep mode is a “power management mode” because it is

a low-power mode of operation. Pet. 60 (citing Ex. 1009 ¶ 158). Petitioner explains that when the SDU receives the wake signal, it wakes “at least a portion” of the laptop (“namely itself”). *Id.* at 61 (citing Ex. 1009 ¶¶ 229–230).

Patent Owner challenges Petitioner’s identification of a security agent in Joseph. PO Resp. 36–38. This argument is discussed in Section III.B.1.d, *supra*. For the reasons stated there and in Section II.B.4, we do not agree with Patent Owner’s construction of “security agent” or its argument that Joseph does not teach a security agent. Nor do we agree that the security agent in Joseph does not perform security services as claimed. *See* PO Resp. 34–35.

Petitioner demonstrates that the SDU, once awakened, performs a variety of security services. Pet. 61–62 (citing Ex. 1009 ¶¶ 75, 134–135, 144; Jakobsson Decl. ¶ 164). For example, after SDU 14 has woken in response to message 148, the security agent performs security services such as erasing, encrypting, and otherwise preventing access to data stored in one or more memory elements (e.g., a hard drive) of memory system 42. Pet. 61; Jakobsson Decl. ¶ 164 (citing Ex. 1009 ¶¶ 75, 134–135). These services are performed by the laptop’s processors 48, which are part of the recited “security agent.” Pet. 61–62; Jakobsson Decl. ¶ 165 (citing Ex. 1009 ¶ 75). These security services occur after SDU 14 receives a wake signal (message 148). Pet. 62; Jakobsson Decl. ¶ 166 (citing Ex. 1009 ¶¶ 228–229).

We find that for the reasons given, Petitioner demonstrates that Joseph teaches element 1.4.b of claim 1.

i. Claim elements 1.5, 1.6, 1.7.a, and 1.7.b

These claims elements call for the following:

[1.5] detect a particular wake event;

[1.6] prepare a particular wake signal in response to detecting the particular wake event; and

[1.7.a] send the particular wake signal to the mobile device in response to detecting the particular wake event,

[1.7.b] the security agent of the mobile device being configured to wake the at least a portion of the mobile device in response to receiving the particular wake signal and being configured to perform particular security services after the at least a portion of the mobile device has been woken.

Petitioner demonstrates that each of these limitations is disclosed by Joseph. Pet. 63–64; Jakobsson Decl. ¶¶ 167–172. Petitioner refers back to its analysis of claim element 1.4.a, *supra*, describing receipt of a wake signal by the SDU and the subsequent waking of the SDU. Pet. 63. Petitioner points out that the security system in Joseph (security/technical support entity 20) detects “particular” wake events distinguishable from other wake events. *Id.* See also discussion of “particular” wake events and signals in Section II.B.3, *supra*.

Petitioner explains that “[a]ny wake signal sent to laptop 12 is a particular wake signal because it is distinguishable from the other wake signals that security/technical support entity 20 may send.” Pet. 63. Moreover, according to Petitioner, “Joseph discloses performing a variety of security services, and each of these services is a particular service at least because it is distinguishable from the other specific services.” *Id.* at 64.

Patent Owner characterizes the “alleged” wake signal in *Joseph* as “generic, not particular” because “the alleged wake signal in *Joseph* is sent whether or not the SDU is actually in sleep mode.” PO Resp. 32–33. Again, we disagree. This argument ignores Joseph’s disclosure of the SDU being in that wake mode because it received a wake signal. Pet. Reply 22 (citing Ex. 1009 ¶¶ 158–160).

Patent Owner contends that “a wake signal that wakes a device but which is not distinguishable by its nature from any other possible wake signal is *generic*, not *specific* or ‘particular.’” PO Sur-reply 3. We disagree that the ’632 patent claims require a wake signal that is distinguishable “by its nature.” This is a variation on Patent Owner’s argument that the claims require a particular “type” of wake event or wake signal, which we rejected as contrary to the language of the claims. See discussion in Section II.B.3, *supra*.

We find that Joseph’s message 148 is a particular wake signal because it is distinguishable from other wake signals on the basis of the time it was sent and on the event that caused it to be sent (selecting between activation of security services and response to a stolen laptop). Pet. Reply 20–21.

Even under Patent Owner’s construction of “particular,” which we have not adopted, Joseph’s wake signal (message 148) is “particular” because it wakes “at least a portion of the mobile device in response to receiving the particular wake signal.” Pet. Reply 21. Specifically, Joseph discloses a wake signal that wakes the SDU. *Id.* As Petitioner points out, Joseph also discloses other particular types of wake events, e.g., detecting that the SDU is authorized to use wireless network 24, and a customer service technician sending a wake signal and security services, e.g., erasing

and encrypting data, upgrading software, and diagnostic and maintenance operations. *Id.* (citing Joseph ¶¶ 96–97). Thus, Joseph discloses the claimed “particular” wake signal, even under Patent Owner’s construction.

As discussed *supra*, Patent Owner also challenges Petitioner’s identification of the security agent in Joseph. PO Resp. 34–38. This argument is discussed *supra*, in Section III.B.1.d. For reasons discussed there, we do not agree with this argument.

We find that for the reasons given, Petitioner demonstrates that Joseph teaches elements 1.5, 1.6, 1.7.a, and 1.7.b of claim 1.

2. Claim 16

Claim 16 is directed to “[a] non-transitory computer readable medium in a security system,” but is otherwise similar to claim 1. Petitioner’s analysis of claim 16 relies on its analysis of claim 1. Pet. 64–66. Patent Owner does not address claim 16 separately, but combines its analysis of common elements in claim 16 with its analysis of claim 1. *See, e.g.*, PO Resp. 39–40. Taking into account the entire record, we determine that Petitioner has demonstrated by a preponderance of the evidence that claim 16 of the ’632 patent would have been obvious in light of Joseph for the reasons given for claim 1.

3. Summary – Claims 1 and 16

We have considered Petitioner’s analysis of claims 1 and 16 in relation to Joseph and the relevant arguments and evidence presented by Patent Owner. Taking into account the entire record, including the Petition, Patent Owner’s Response, Petitioner’s Reply, and Patent Owner’s Sur-reply, as well as the evidence presented by the parties, we determine that Petitioner

has demonstrated by a preponderance of the evidence that claims 1 and 16 of the '632 patent would have been obvious in light of Joseph.

4. Claims 9 and 24

Claims 9 and 24 depend from claim 1 and claim 16, respectively, each adding the limitation “wherein the performing the particular security services includes removing unauthorized data from the mobile device.” Petitioner provides an element-by-element analysis of these claims in light of Joseph and Meenan. Pet. 66–67; Jakobsson Decl. ¶¶ 179–184. Petitioner relies on Meenan for teaching the additional limitation of “performing a particular security service that includes removing unauthorized data from the mobile device.” Pet. 67.

Petitioner provides a rationale for combining the references. According to Petitioner, “[a person of ordinary skill] also could have removed unauthorized programs after a Joseph laptop receives a wake signal, just as Joseph discloses performing other security services after receiving a wake signal.” *Id.* (citing Jakobsson Decl. ¶ 180).

Patent Owner’s response to this challenge presents no additional arguments, referring back to its prior arguments addressing claims 1 and 16. PO Resp. 40. For the reasons given, we find that Petitioner has demonstrated a motivation to combine Joseph and Meenan with a reasonable expectation of success. Pet. 67–69; Jakobsson Decl. ¶¶ 180–183. Furthermore, we find that Petitioner has demonstrated that each element of claims 9 and 24 is taught by that combination of references. Pet. 66, 68; Jakobsson Decl. ¶¶ 179, 184. For the reasons given, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 9 and 24 would have been obvious in light of Joseph and Meenan.

C. Challenges Based on Hall

Petitioner contends claims 1, 9, 16, and 24 would have been obvious over Hall and claims 9 and 24 would have been obvious over Hall and Meenan. Pet. 4.

1. Claim 1

Petitioner’s element-by-element analysis of claim 1 in relation to Hall appears at pages 17–38 of the Petition. Petitioner supports its analysis with testimony from its expert, Dr. Jakobsson. Jakobsson Decl. ¶¶ 67–115. For the reasons given by Petitioner and those that follow, we find that Petitioner has demonstrated that each element of claim 1 is disclosed or suggested by Hall.

We focus our discussion here on the claim elements that are challenged by Patent Owner. We adopt Petitioner’s analysis for the remaining claim elements.

a. sending a particular wake signal in response to detecting a particular wake event (claim elements 1.5, 1.6, 1.7.a)

The term “particular wake event” appears in claim elements 1.5, 1.6, and 1.7.a. Petitioner contends that Hall discloses this limitation: “Any wake event that backend service center 150 (a security system) detects is a particular wake event because it is distinguishable from the other wake events that backend service center 150 may detect.” Pet. 36. Petitioner further explains that “[f]or example, a wake event would occur at a specific time and therefore be a wake event particular to at least that time.” *Id.*; see also Pet. Reply 15–16.

Patent Owner contends that “[t]aken as a whole, these claim elements recite a technique whereby a wake event triggers a particular *type* of wake

signal, which triggers the mobile device’s security for a particular *type* of security service.” PO Resp. 7. For reasons discussed *supra*, in Section II.B.3, we do not agree with this construction and do not adopt it. Nor do we agree with Patent Owner’s argument that “[b]ecause the word ‘particular’ cannot refer merely to a something that occurs at a specific time, Petitioner’s arguments about how *Hall* allegedly teaches these limitations necessarily fails.” *Id.* at 21.

Patent Owner contends “there is no concept in *Hall* of preparing a ‘particular wake signal’ in response to receiving a ‘particular wake event.’” *Id.* As we have discussed *supra*, the distinction Patent Owner attempts to draw between “particular” and “generic” wake signals (*see id.* at 22) is not supported by the language of the claims or the specification. *See, e.g.*, discussion in Section III.B.1.i, *supra*.

We find that Petitioner demonstrates that this limitation is met by Hall under the construction we have adopted. *See* Pet. 36 (“Any wake event that backend service center 150 (a security system) detects is a particular wake event because it is distinguishable from the other wake events that backend service center 150 may detect.”); Jakobsson Decl. ¶ 110. Similarly, for limitations referring to a “particular” wake signal, Petitioner demonstrates that Hall discloses this element. Pet. 36–37; Jakobsson Decl. ¶¶ 111–112.

We find, also, that Petitioner demonstrates that Hall discloses this limitation even under Patent Owner’s construction. Pet. Reply 16. Petitioner shows that Hall discloses a particular type of wake signal (resulting in the laptop entering the “S0” state, citing Ex. 1007 ¶¶ 34, 100) and a particular type of wake event (status of the laptop being set to stolen, citing Ex. 1007 ¶ 26). *Id.*

For the reasons given above and in our discussion of claim construction, we find that Petitioner demonstrates that Hall teaches or suggests “a particular wake event” and “a particular wake signal,” as claimed in the ’632 patent. *See supra*, Section II.B.3.

b. performing particular security services (claim element 1.7.b)

Patent Owner contends that “*Hall* does not teach performing particular security services in response to receiving a particular wake signal for the same reasons established above, namely that the word ‘particular’ is used to distinguish between different *types* of ‘wake events,’ ‘wake signals,’ and ‘security services,’ and not just those that occur at different moments in time.” PO Resp. 22. We disagree for reasons previously discussed.

In the preceding section, we discuss Hall’s teaching of “particular” wake events and wake signals. Petitioner demonstrates also that Hall discloses “multiple particular types of security services.” Pet. Reply 16; Pet. 37 (citing Ex. 1007, Fig. D); *see also* Jakobsson Decl. ¶ 115. These include “security services such as ‘Logoff user,’ ‘Force shutdown,’ ‘Delete files,’ ‘Initiate audible alarm,’ and ‘Encrypt files.’” Pet. 37. Petitioner explains that “[e]ach of these services is a particular service at least because it is distinguishable from the other defined services and a user can specifically select each of these services.” *Id.*

Patent Owner’s argument that Hall does not teach performing particular security services “in response to receiving a particular wake signal” is incorrect for an additional reason. As Petitioner points out, and as we discuss above, the claims recite that the security agent of the mobile device is configured to perform security services *after* the at least a portion of the mobile device has been woken. Pet. Reply 17. The claims do not

require performing security services “in response to” receiving a wake signal. *Id.* Thus, Patent Owner’s argument is unavailing.

For the reasons given, we find that Petitioner demonstrates that Hall teaches performing particular security services.

c. security agent (claim elements 1.2.b, 1.4.b)

Claim element 1.2.b calls for “the mobile device including a mobile device processor and including a security agent configured to cooperate with the security system.” Claim element 1.4.b recites “the security agent of the mobile device being configured to receive the wake signal, the security agent of the mobile device being configured to wake at least a portion of the mobile device from a power management mode in response to receiving the wake signal, the security agent of the mobile device being configured to perform security services after the at least a portion of the mobile device has been woken.”

Petitioner identifies the MySync module in Hall and the same module combined with the MyGuard application in Hall as the security agent. Pet. 22–31. Petitioner explains that “[t]he MySync module is a security agent because it provides security services, such as ‘services that are used by security-based applications to protect unauthorized access of stored data from or unauthorized usage of the subscriber device.’” *Id.* at 23 (citing Ex. 1007 ¶ 27). Furthermore, “[t]he MyGuard application includes a number of processes directed to security shown in Figure 2B, such as a password manager 280, a remote desktop manager 285, an auxiliary display manager 290, and a shutdown manager 295.” Pet. 23 (internal quotation marks omitted).

Patent Owner responds that Hall does not disclose a security agent as claimed because it does not disclose a “particular wake signal” or “particular security services.” PO Resp. 23. We disagree. As Petitioner points out, this argument is based on Patent Owner’s proposed claim constructions for those terms that we rejected. Pet. Reply 18. We find that under the construction we have adopted, Hall discloses both a particular wake signal and particular security services. *See* discussion in Sections III.C.1.a and III.C.1.b, *supra*.

Patent Owner further contends that Hall “fails to disclose a *security agent* that performs the recited functions.” PO Resp. 23–25. Patent Owner explains that Hall “explicitly states that its applications, *not* the MySync module, are responsible for providing services.” *Id.* at 25 (citing Goodrich Decl. ¶ 72).

Petitioner replies that the MySync module “establishes network connectivity with the backend service center to receive incoming security-related messages, parses the messages, and routes them to the appropriate application.” Pet. Reply 18 (citing Ex. 1007 ¶¶ 93, 41, 52). Petitioner contends that “[b]ecause these services help the security-based applications provide security, they are security services.” *Id.*

We disagree with Patent Owner that the MySync module is not responsible for providing security services. As Petitioner explains, “[t]he MySync module is a security agent because it provides security services, such as ‘services that are used by security-based applications to protect unauthorized access of stored data from or unauthorized usage of the subscriber device.’” Pet. 23 (quoting Ex. 1007 ¶ 27). We agree.

Petitioner demonstrates that the MySync module receives a wake signal from the backend service center. Pet. 32 (citing Ex. 1007 ¶ 102). In

response to receiving the wake signal it wakes at least a portion of the laptop 110₁ from one of the power management modes. *Id.* (citing Ex. 1007 ¶ 34). Petitioner explains that the wake message is processed by the MySync module, which performs the awakening. *Id.* at 33 (citing Ex. 1007 ¶ 109).

Further, Petitioner demonstrates that “the MySync module and MyGuard application (together, a security agent) perform actions such as ‘Shutdown’ using the ‘remote desktop manager 285’ process.” Pet. 34 (citing Ex. 1007 ¶ 86, Fig. 2B).

Patent Owner acknowledges Petitioner’s contention that the MyGuard application may be part of a security agent. PO Resp. 26. But we disagree with Patent Owner’s contention that Petitioner has failed to “demonstrate how the claims, as properly construed, are disclosed in the art.” *Id.* at 27. To the contrary, the Petition identifies both MySync and MyGuard and their relation to challenged claim 1 in its analysis. *See, e.g.*, Pet. 23 (“The MySync module together with the MyGuard application 2701 also are the claimed ‘security agent.’”).

Moreover, Patent Owner’s argument that MyGuard “is not an ‘agent’ or part of an ‘agent’” is based on a claim construction for “agent” proposed by Patent Owner and rejected by the Board. PO Resp. 27. The fact that the MySync module may rely on applications such as MyGuard to provide certain services does not mean that MySync does not perform services itself, such as providing services that are used by security-based applications to protect unauthorized access of stored data from, or unauthorized usage of, the subscriber device. Pet. Reply 18–19 (citing Ex. 1007 ¶¶ 7, 27).

We disagree with Patent Owner that Petitioner is “kluging together the distinct MySync and MyGuard modules to reach the claimed security

agent.” PO Resp. 27. Patent Owner’s “kluging” argument is unavailing because, as Petitioner demonstrates, “[t]hese two modules together being a ‘security agent’ is consistent with the ’632 patent embodiment where the security agent includes two modules—‘mode module 1904’ for waking components from a power management mode and ‘component manager 1906’ for conducting security services.” Pet. 24. In addition, Figure 2B of Hall and the accompanying text demonstrate that the MySync module and MyGuard application communicate with each other and work together. Ex. 1007 ¶ 45. Thus, XML messages received by MySync module 240 are parsed and security-based instructions are routed to MyGuard application 270₁, which includes a number of processes directed to security. *Id.* In light of this close connection between the MySync module and the MyGuard application, we find that they are properly considered together as a security agent.

For these reasons, we find that Petitioner demonstrates that Hall discloses the claimed security agent.

d. security administrator device (claim elements 1.2.a, 1.2.c)

Claim element 1.2.a calls for “a communication interface configured to communicate with a mobile device and configured to communicate over a network with a security administrator device.” Petitioner identifies the second subscriber device 110₂ in Hall as the claimed security administrator device: “The second subscriber device 110₂ is a security administrator device because it lets a user perform security-related administration of his or her devices, including indicating whether a device has been stolen and what corresponding actions to take with respect to the stolen device.” Pet. 18–19.

Patent Owner responds that Hall's second subscriber device 110₂ is not a security administrator device because it "does *not* manage the security of a security system." PO Resp. 38

We do not agree with Patent Owner's argument because it is based on a construction of "security administrator device" that we did not adopt. *See supra*, Section II.B.2. We have adopted, instead, Petitioner's construction, which is "[t]he plain and ordinary meaning of [security administrator device] includes a device that performs security administration." Pet. 13 (citing Jakobsson Decl. ¶ 65). Hall discloses that a user can use subscriber device 110₂ to access a user interface and report the status of a subscriber device as "stolen." Pet. 18–20; Ex. 1007 ¶¶ 64–66, Fig. 6D. Under our construction, Hall's subscriber device 110₂ is a security administrator device because it performs administrative tasks, e.g., establishing an account, configuring an account, and setting status of a device to "stolen." Pet. 18–19; *see* Ex. 1007, Figs. 6A–6D.

We find that Petitioner demonstrates that Hall discloses the claimed security administrator device.

2. Claim 16

Petitioner's analysis of claim 16 relies on its analysis of claim 1. Pet. 38–40. Patent Owner does not address claim 16 separately, but combines its analysis of claim 16 with its analysis of claim 1. *See, e.g.*, PO Resp. 31–39. For the reasons given for claim 1, we find that Petitioner has demonstrated that Hall discloses the limitations of claim 16.

3. Summary – Claims 1 and 16

We have considered Petitioner's analysis of claims 1 and 16 in relation to Hall and the relevant arguments and evidence presented by Patent

Owner. Taking into account the entire record, including the Petition, Patent Owner's Response, Petitioner's Reply, and Patent Owner's Sur-reply, as well as the evidence presented by the parties, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1 and 16 would have been obvious based on Hall.

4. Claims 9 and 24

Petitioner provides an element-by-element analysis of these dependent claims in light of Hall (Pet. 37–38, 40) and Hall and Meenan (*id.* at 42–45). *See also* Jakobsson Decl. ¶¶ 116, 121–133. In its analysis of the ground based on Hall and Meenan, Petitioner relies on Meenan for teaching “performing a particular security service that includes removing unauthorized data from a mobile device.” Pet. 42–43.

Petitioner provides a persuasive rationale for combining Hall and Meenan. For example, according to Petitioner, “[a person of ordinary skill] also could have removed unauthorized programs [as described by Meenan] using Hall's MySync module and MyGuard application (together, a security agent) because they already perform other security services.” *Id.* at 43.

Patent Owner's response to this challenge presents no new arguments, referring back to its arguments addressing claims 1 and 16. PO Resp. 31. For the reasons given by Petitioner, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 9 and 24 would have been obvious over Hall and over Hall and Meenan.

IV. CONCLUSION

For the foregoing reasons, we determine Petitioner has demonstrated by a preponderance of the evidence that all challenged claims of the '632

patent would have been obvious and are, therefore, unpatentable. Our conclusions are summarized in the following table.

Claims	35 U.S.C. §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not shown Unpatentable
1, 9, 16, 24	103(a)	Hall	1, 9, 16, 24	
9, 24	103(a)	Hall, Meenan	9, 24	
1, 16	103(a)	Joseph	1, 16	
9, 24	103(a)	Joseph, Meenan	9, 24	
Overall Outcome			1, 9, 16, 24	

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1, 9, 16, and 24 of the '632 patent are unpatentable; and

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

IPR2021-01236
Patent 10,951,632 B2

PETITIONER:

James Heintz
Michael Burns
Robert Buergi
DLA Piper LLP (US)
jim.heintz@dlapiper.com
michael.burns@dlapiper.com
robert.buergi@dlapiper.com

PATENT OWNER:

Jonathan Caplan
Jeffrey Price
KRAMER LEVIN NAFTALIS &
FRANKEL LLP
jcaplan@kramerlevin.com
jprice@kramerlevin.com