Trials@uspto.gov
571-272-7822

Paper 48
Entered: October 2, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICRON TECHNOLOGY INC.,
Petitioner,

v.

SECUREWAVE STORAGE SOLUTIONS, INC.,
Patent Owner.

IPR2019-00932
Patent 7,036,020 B2

Before JONI Y. CHANG, GARTH D. BAER, and KAMRAN JIVANI, *Administrative Patent Judges*.

CHANG, *Administrative Patent Judge.*

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

I. INTRODUCTION

Micron Technology Inc. ("Petitioner" or "Micron") filed a Petition requesting an *inter partes* review of claims 1−14 ("the challenged claims") of U.S. Patent No. 7,036,020 B2 (Ex. 1001, "the '020 patent"). Paper 1 ("Pet."). SecureWave Storage Solutions, Inc. ("Patent Owner") filed a Preliminary Response. Paper 8 ("Prelim. Resp."). Upon consideration of the Petition and Preliminary Response, we instituted the instant *inter partes* review of all of the challenged claims and on all of the grounds presented in the Petition. Paper 10 ("Dec.").

After institution, we granted a Motion for Joinder filed timely by Kingston Technology Company, Inc. ("Kingston"), joining IPR2020-00139 with the instant proceeding (Paper 22). Subsequently, Kingston and Patent Owner filed a Joint Motion to Terminate this proceeding with respect to Kingston in light of their settlement of their dispute regarding the '020 patent. Paper 45. Upon consideration, we granted the Joint Motion and terminated the proceeding with respect to Kingston only. Paper 47. The proceeding continued with Patent Owner and Micron. *Id*. at 3.

During this trial, Patent Owner filed a Response (Paper 15, "PO Resp.") and a Sur-reply (Paper 23, "Sur-reply"); Petitioner filed a Reply (Paper 20, "Reply"). An oral hearing was held on May 12, 2020, and a transcript is included in the record as Paper 44 ("Tr.").

This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a). For the reasons set forth below, we determine that Petitioner has

demonstrated by a preponderance of the evidence that claims 1−14 of the ’020 patent are unpatentable.

A. Related Matters

The parties indicate that the ’020 patent is involved in *SecureWave Storage Solutions, Inc. v. Micron Tech., Inc.*, No. 1-18-cv-1398-MN (D. Del.) and *SecureWave Storage Solutions, Inc. v. Kingston Tech. Co., Inc.*, No. 8:18-cv-01425 (C.D. Cal.). Pet. 3; Paper 4, 3. The ’020 patent also is involved in *Kingston Tech. Co. v. SecureWave Storage Solutions, Inc.*, IPR2019-00494, Paper 8 (PTAB July 11, 2019) (Denied Institution) and *Unified Patents, Inc. v. SecureWave Storage Solutions, Inc.*, IPR2019-00501, Paper 31 (PTAB July 7, 2020) (Final Written Decision holding claims 1−5 of the ’020 patent unpatentable).

B. The ’020 Patent

The ’020 patent relates to methods and systems for promoting security in a computer system. Ex. 1001, code (57). In particular, the ’020 patent discloses a simple file system that is concealed in the computer system and is managed with a processor and simple non-writeable code operating on a storage device. *Id*. at 3:26−30. In one embodiment, a computer system is provided with an operating system associated with a storage device that includes firmware and a processor for processing data stored on the storage device. *Id*. at 3:33−37. The embodiment includes creating a secured partition in, and restricting access to, a portion of the storage device by the operating system. *Id*. at 3:37−39. The embodiment also includes providing

at least one authority record and data associated with the authority record in the storage device. *Id*. at 3:41−43.

C. Illustrative Claim

Of the challenged claims, claims 1, 7, and 12 are independent. Claims 2−6 and 11 depend from claim 1; claims 8 and 9 depend from claim 7; and claims 13 and 14 depend from claim 12.

Claim 1 is illustrative:

> 1. A storage device for promoting security in a computer system, the storage device comprising:
>
> a storage medium for storing data;
>
> firmware for reading data from and writing data to the storage medium; and
>
> a partition defined on the storage medium for dividing the storage medium into a data partition and a secure data partition, the secure data partition for storing secure data and one or more authority records, wherein the one or more authority records define access permissions relating to the secure data partition and the secure data;
>
> wherein the secure data partition contains a master authority record, wherein the one or more authority records can be created and deleted as required by a user having access permissions according to the master authority record; and
>
> wherein only the firmware is permitted to access the secure data and the one or more authority records.

Ex. 1001, 12:52–13:2.

D. Prior Art Relied Upon

Petitioner relies upon the references listed below. Pet. 5−6.

Reference	Date	Exhibit No.
Hamlin[1], US 7,003,674 B1	Feb. 21, 2006	1004[2]
Fisherman, US 5,586,301	Dec. 17, 1996	1005
Silvester, US 7,155,615 B1	Dec. 26, 2006	1006
Carter, US 6,738,907 B1	May 18, 2004	1007
Mirov, US 6,138,236	Oct. 24, 2000	1008

E. Asserted Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability (Pet. 6) [3]:

	Claim(s) Challenged	35 U.S.C. §	References
1	1−3, 5, 12−14	103(a)	Hamlin, Fisherman, the knowledge of an ordinarily skilled artisan

[1] In this Decision, we refer to this asserted reference as "Hamlin" (Ex. 1004), U.S. Patent No. 7,215,771 B1 as "Hamlin II" (Ex. 1009), and U.S. Patent No. 7,155,616 as "Hamlin III" (Ex. 1010).

[2] Hamlin incorporates by reference Tygar, J. D. and Yee, B. S., "Secure Coprocessors in Electronic Commerce Applications," Proceedings 1995 USENIX Electronic Commerce Workshop (1995) (Ex. 1017, "Tygar").

[3] For purposes of this Decision, we assume the claims at issue have an effective filing date prior to March 16, 2013, the effective date of the

	Claim(s) Challenged	35 U.S.C. §	References
2	3, 11	103(a)	Hamlin, Fisherman, Silvester, the knowledge of an ordinarily skilled artisan
3	4	103(a)	Hamlin, Fisherman, Carter, the knowledge of an ordinarily skilled artisan
4	6−10	103(a)	Hamlin, Fisherman, Mirov, the knowledge of an ordinarily skilled artisan
5	7−10	103(a)	Hamlin, Fisherman, Mirov, Silvester, the knowledge of an ordinarily skilled artisan

II. ANALYSIS

A. Level of Ordinary Skill in the Art

In determining the level of ordinary skill in the art, various factors may be considered, including the "type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field." *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (quotation marks and citation omitted). Petitioner's declarant, John Levy, Ph.D., testifies that one of ordinary skill in the art would have had "at least a bachelor's degree in electrical engineering, computer engineering, computer science, or a closely related field, with two or more years of experience in

---

Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), and we apply the pre-AIA version of 35 U.S.C. § 103.

the development, design, or implementation of digital storage devices or the equivalent." Ex. 1003 ¶ 23. Dr. Levy explains that "[a]dditional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education." *Id*.

Patent Owner asserts that such an artisan would have had "at least a bachelor's degree in a discipline such as computer science, electrical engineering, computer engineering, or related disciplines or experience, and at least two years of experience in computer storage systems." PO Resp. 21. Patent Owner further explains that under either assessment, "the disclosures of the references are the same and cannot be altered by expert opinion or argument." *Id*.

Based on the evidence in this entire trial record, we adopt the level of ordinary skill as articulated by Petitioner because its assessment appears to be consistent with the '020 patent, the asserted prior art, and is supported by the testimony of Dr. Levy. We note, however, our claim construction and patentability analyses would reach the same findings and determinations if we were to adopt the level of ordinary skill in the art proposed by Petitioner or Patent Owner.

B. Claim Construction

In an *inter partes* review proceeding, a patent claim shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b). 37 C.F.R. § 42.100(b) (2019). This standard is the same as that applied in *Phillips v. AWH Corp.*,

415 F.3d 1303 (Fed. Cir. 2005) (en banc) and its progeny. Under this standard, the words of a claim are generally given their "ordinary and customary meaning," which is the meaning the term would have to a person of ordinary skill at the time of the invention, in the context of the entire patent including the specification. *See Phillips*, 415 F.3d at 1312–13.

In light of the parties' arguments and evidence, we find that it is necessary to expressly construe the terms identified below. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)) (noting that "we need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy'").

1. "firmware"

Claim 1 recites "firmware for reading data from and writing data to the storage medium." Ex. 1001, 12:55−56. Claim 12 recites "firmware disposed within the storage device adapted to limit access to the security partition by an operating system of a computer system." *Id*. at 14:23−26.

Dr. Levy testifies that a person of ordinary skill in the art would have understood the plain and ordinary meaning of the term "firmware," as used in the '020 patent, to mean "software that has been copied on (and therefore stored in) an integrated circuit, which usually may be a [read only memory ('ROM')] or other non-writable and non-volatile memory." Ex. 1003 ¶ 111. Dr. Levy explains that this construction is consistent with several dictionary definitions. For example, the Webster's New World Dictionary of

Computer Terms defines "firmware" as "[s]oftware that has been copied on integrated circuits, usually ROMs . . . which cannot be altered." Ex. 1013, 232. The IEEE Standard Dictionary of Electrical and Electronics Terms also provides a similar definition of the term firmware. Ex. 1012, 411−412.

Dr. Levy's construction also is consistent with the Specification. Figures 1 and 2 of the '020 patent are reproduced below.

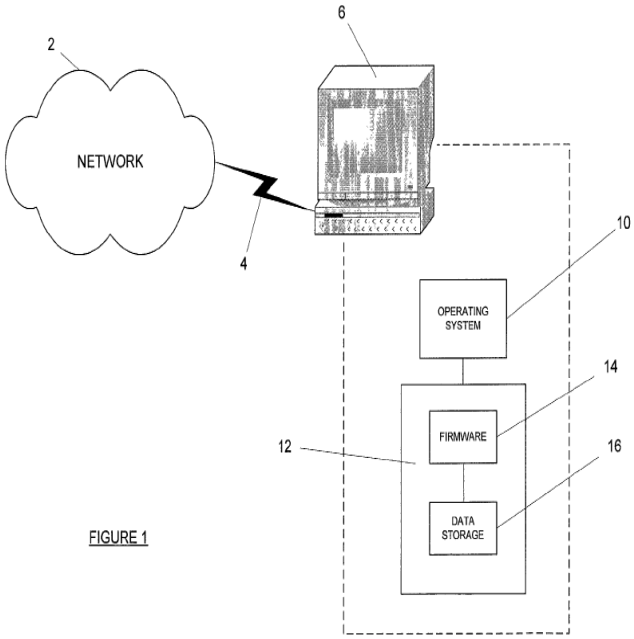

FIGURE 1

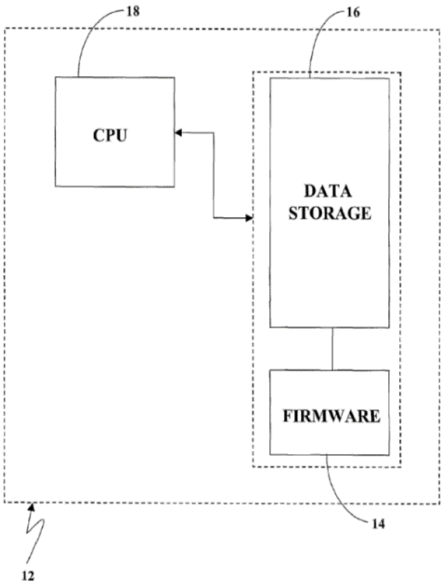

FIG. 2

Figure 1 of the '020 patent above (on the left) shows network 2 connected to computer system 6. *Id*. at 4:37−44. Figure 2 above (on the right) shows storage device 12, which contains central processing unit ("CPU") 18, data storage 16, and firmware 14 to read and write data from data storage 16. *Id*. at 4:45−65. Operating system 10 of computer system 6 relies on software and data obtained from storage device 12. *Id*. A portion of firmware 14 is "writeable firmware" that can be re-written by software

executed in the operation system. *Id*. A portion of firmware 14 is "non-writeable firmware" that "is written by using one or more of a plurality of conventional hardware methods that resist this firmware from being written by the operating system 10." *Id*.

In view of the claim language, Specification, and evidence of record, we agree with Dr. Levy and interpret "firmware" as "software that has been copied on (and therefore stored in) an integrated circuit, which usually may be a ROM or other non-writable and non-volatile memory." Ex. 1003 ¶ 111.

2. "firmware for reading data from and writing data to the storage medium"

Patent Owner argues that the claim language "firmware *for* reading data from and writing data to the storage medium" requires that "the *firmware* performs the read/write operations itself," not "facilitating the reading and writing as performed by other software, as indicated by the ordinary and customary meaning of the words of the phrase." Sur-reply 6−8.

Patent Owner's construction improperly imports a negative limitation into the claims. Nothing in the claim's plain language requires that read and write commands must originate from the firmware, or that no other component outside the firmware may play a role in reading data from and writing data to the storage medium. Similarly, the Specification does not necessitate that the firmware *alone* must perform all aspects of reading from and writing data to the storage medium.

For example, claim 1 recites a limitation "wherein the one or more authority records *can be created and deleted as required by a user*." Ex. 1001, 12:64−65 (emphasis added). Dr. Levy testifies that "to allow an authority record to be created and deleted, access must be made to the authority records at the behest of a user" and "that user is allowed to reference this data *via the firmware*." Ex. 1003 ¶ 138. The Specification also discloses "a user application external to the storage device can employ the storage device as a reliable place to conceal information and to perform cryptographic operations." Ex. 1001, 8:30−34. In short, the '020 patent makes clear that a user or an entity external to the disk drive is allowed to access, read, and write secure data or authority records via the firmware.

Therefore, neither the plain and ordinary meaning of the claim terms, nor the Specification, requires the firmware by itself performs the read/write operations. As such, we decline to adopt Patent Owner's construction that improperly imports a negative limitation into the claims. *E.I. du Pont de Nemours & Co. v. Phillips Petroleum Co.*, 849 F.2d 1430, 1433 (Fed. Cir. 1988) (holding that reading an "extraneous limitation" into a claim is improper).

3. "only the firmware is permitted to access the secure data and the one or more authority records"

Petitioner asserts that "this limitation requires that all interactions with the secure data and authority records are performed through and brokered by the firmware." Pet. 32. Dr. Levy testifies that "for the '020 Patent to be operable per its written description, and for other claim limitations to be

practicable, this limitation must mean simply that *all access to the secure data and the authority records is performed via and brokered by the firmware*." Ex. 1003 ¶ 138 (emphasis added).

Patent Owner suggests that no other component or external entity is permitted to request access to the secure data via the firmware. Sur-reply 10−17. Patent Owner argues that during prosecution, the applicant distinguished the Diamant and Aucsmith references from the claims that later issued in the '020 patent because those references allow access by a host. *Id.* at 12−13 (citing Ex. 1002, 328−329, 385).

We agree with Dr. Levy. Patent Owner's implicit construction is inconsistent with the claim language and Specification and is not supported by the prosecution history. As discussed above, claim 1 recites a limitation "wherein the one or more authority records *can be created and deleted as required by a user*." Ex. 1001, 12:64−65 (emphasis added). Dr. Levy testifies that "to allow an authority record to be created and deleted, access must be made to the authority records at the behest of a user" and "that user is allowed to reference this data *via the firmware*." Ex. 1003 ¶ 138. The Specification also discloses "a user application external to the storage device can employ the storage device as a reliable place to conceal information and to perform cryptographic operations." Ex. 1001, 8:30−34. In short, the '020 patent makes clear that a user or an entity external to the disk drive is allowed to access, read, and write secure data or authority records via the firmware.

We are not persuaded by Patent Owner's argument that during prosecution, the applicant distinguished Diamant and Aucsmith from the claims that later issued in the '020 patent because they allow access by a host. The prosecution history clearly shows that these references were distinguished because they "teach a controller external to the storage device for controlling access to the storage device." Ex. 1002, 328−29, 384−85. Therefore, the prosecution history does not support Patent Owner's implicit construction.

In light of the claim language, Specification, and prosecution history, we decline to adopt Patent Owner's construction. Rather, we construe "only the firmware is permitted to access the secure data and the one or more authority records" to mean that "all access to the secure data and the authority records is performed via and brokered by the firmware." *See* Ex. 1001, 8:30−34, 12:64−65; Ex. 1002, 328−29, 384−85; Ex. 1003 ¶ 138.

4. "authority records"

Claim 1 recites "wherein the one or more authority records define access permissions relating to the secure data partition and the secure data." Ex. 1001, 12:60−62. Claim 12 recites "a security partition containing one or more authority records." *Id.* at 14:15−16. Claim 14 depends from claim 12 and further recites "wherein each of the one or more authority records comprises a plurality of fields." *Id*. at 14:31−34.

Petitioner asserts that a person of ordinary skill in the art would have understood the term "authority record(s)" to mean "data defining an entity's access permissions." Pet. 9; Ex. 1003 ¶¶ 58−66.

In our Institution Decision, based on the record at that time, we preliminarily adopted Petitioner's construction. Dec. 10. For this Final Decision, we review the evidence and arguments presented by the parties during the entire trial.

Patent Owner maintains that the term "authority record" should be given its plain and ordinary meaning. PO Resp. 23; Prelim. Resp. 24; Ex. 2008 ¶ 24. Nevertheless, through its prior art arguments, Patent Owner implicitly imports limitations into the claims. PO Resp. 32−36; Sur-reply 24−27.

We agree with Patent Owner that the term "authority records" should be given its plain and ordinary meaning consistent with the claim language and Specification, and the term "access permissions" is "relat[ed] to the secure data partition and the secure data." However, because the term "access permissions" appears without a modifier, we decline to introduce a modifier ("entity's") into the claims as Petitioner proposes. *See Source Vagabond Sys. Ltd. v. Hydrapak, Inc.*, 753 F.3d 1291, 1299−1300 (Fed. Cir. 2014) ("[A]n analysis that adds words to the claim language . . . does not follow standard cannons of claim construction."). Furthermore, we decline to adopt Patent Owner's implicit claim construction that improperly imports limitations into the claims.

First, through its prior art arguments, Patent Owner suggests that authentication and authorization cannot be performed using the same information. PO Resp. 32−34; Sur-reply 23−24. Patent Owner argues that authorization and authentication perform different functions—namely, "[a]uthorization deals with granting and verifying a user's (or a device's) access permissions, whereas authentication deals with confirming the user's (or device's) identity." *Id.*; Ex. 2008 ¶¶ 84−85 (relying on portions of the Horak book (Ex. 2003[4])); Sur-reply 23−24.

However, Patent Owner improperly imports a negative limitation into the claims by excluding information that is used for both authentication and authorization. Nothing in the claim language excludes such information. Mr. Jay Jawadi, Patent Owner's declarant, admits that "[a]uthorization and authentication both deal with computer security." Ex. 2008 ¶ 84. Dr. Levy testifies that "authentication and authorization are interrelated concepts." Ex. 1021 ¶ 65.

Our reviewing court "has repeatedly cautioned against limiting the claimed invention to preferred embodiments or specific examples in the specification." *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1346−47 (Fed. Cir. 2015). "[I]t is the *claims*, not the written description, which define the scope of the patent right." *Id*. at 1346 (emphasis in the original).

---

[4] Exhibit 2003 contains portions of pages 222 and 540 from Ray Horak, Communications Systems and Networks, 2nd ed., M&T Books (1999) ("the Horak book"). Petitioner filed an actual copy of pages 222, 223, 540, 541 of the Horak book in Exhibit 1038.

The Specification also does not support Patent Owner's construction. Indeed, the Specification uses the term "authority record" broadly. For example, the Specification provides that "authority record 52 *can include data*, *computer programs, and other like information* and functionality in association with the SP [security partition] data 54." Ex. 1001, 5:53−56 (emphasis added). Nothing in the Specification defines the term "authority records" to exclude information that is used for both authentication and authorization.

Furthermore, Patent Owner's construction is not consistent with the understanding of an ordinarily skilled artisan. "The words of a claim are generally given their ordinary and customary meaning *as understood by a person of ordinary skill in the art* when read in the context of the specification and prosecution history." *Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (emphasis added). Here, Dr. Levy testifies that "authorization and authentication are closely related and interconnected activities that are often performed by the same process using the same data." Ex. 1021 ¶ 64. As Dr. Levy points out, under the "authorization" section in the Horak Book, the author provides that "Kerberos, *the best-known authorization software*, makes use of private-key *authentication* and a UNIX-based distributed databases." Ex. 1021 ¶ 65; Ex. 1038, 3 (emphases added). We credit Dr. Levy's testimony as it is consistent with the prior art of record (Ex. 2003; Ex. 1038).

In short, we decline to adopt Patent Owner's construction that would improperly import a negative limitation into the claims. Instead, we

determine that the claim term "authority records" does not exclude information that is used for both authentication and authorization.

Second, Patent Owner argues that "the construction of 'authority records' adopted by the Board requires multiple access permissions (plural)," in that "a single authority record defines access permission<u>s</u> (plural), such as R/W Access Rights, WriteOnce, Write Over, WriteAny, ReadCur, ReadAny, and Hidden Read." PO Resp. 25; Sur-reply 24−27; Ex. 2008 ¶¶ 121−125; Ex. 1022, 44:8−45:3.

At the outset, our claim construction set forth in the Institution Decision does not require multiple access permissions in each authority record. To be clear, our claim construction in this Final Decision also does not require multiple permissions in each record for the reasons discussed below.

Again, Patent Owner's construction improperly imports a limitation into the claims. *Williamson*, 792 F.3d at 1346−47. As Petitioner points out, Patent Owner's construction improperly injects "each of" into the claim: "where *[each of]* the one or more authority records define access permissions." Reply 13. Dr. Levy testifies that "[he has] reviewed the '020 patent and its file history, and [he has] not identified any language suggesting that invention of the '020 patent is limited to requiring multiple permissions for each authority record." Ex. 1021 ¶ 69.

Moreover, Patent Owner concedes that "[b]y the plain and customary reading of the phrase 'wherein the one or more authority records defines access permissions,' it is clear that one authority record can define multiple

access permissions, or alternatively, multiple authority records can define multiple access permissions." Sur-reply 25. Dr. Levy testifies that "the claims cover the situation when there are 10 authority records ('one or more' authority records) that each include one permission (because together, the 10 records include 10 permissions and thus 'define access permissions [10] relating to the secure data partition and the secure data')." Ex. 1021 ¶ 69.

Therefore, we find that the plain and ordinary meaning of the claim language "one or more authority records define access permissions relating to the secure data partition and the secure data" encompasses both:
(1) a single authority record that includes multiple access permissions, and
(2) multiple authority records that include multiple access permissions (each record includes at least one permission). We decline to adopt Patent Owner's implicit claim construction that improperly imports a limitation into the claims by requiring multiple permissions for each authority record.

Lastly, Patent Owner suggests that each authority record requires multiple fields. PO Resp. 34−36; Ex. 2008 ¶¶ 126−136.

Again, Patent Owner improperly imports a limitation into the claims. *Williamson*, 792 F.3d at 1346−47. Nothing in the Specification or the claim language of independent claims 1 and 12, states or implies that each authority record requires multiple fields. This is confirmed by dependent claim 14, which further recites "wherein each of the one or more authority records comprises a plurality of fields." Ex. 1001, 14:31−34. The fact that claim 14 further adds this limitation indicates that this limitation was not a necessary element of independent claims 1 and 12. *See Phillips*, 415 F.3d at

1315 ("[T]he presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim."). The intrinsic evidence does not support Patent Owner's implicit construction that requires multiple fields in each authority record. Therefore, we decline to adopt that construction.

In sum, we determine that the claim term "authority records" should be given its plain and ordinary meaning, and the claim term "access permissions" is "related to the secure data partition and the secure data."

However, we do not adopt Patent Owner's implicit claim construction that imports limitations into the claims. Rather, we determine that "authority records" does not exclude information that is used for both authentication and authorization. And the claim language "one or more authority records define access permissions relating to the secure data partition and the secure data" encompasses both: (1) a single authority record that includes multiple access permissions, and (2) multiple authority records that include multiple access permissions (each record includes at least one permission). And the term "authority records" does not require multiple fields in each authority record.

5. "master authority record"

Claim 1 recites "wherein the one or more authority records can be created and deleted as required by a user having access permissions according to the master authority record." Ex. 1001, 12:64−67. Claim 13, which depends from claim 12, recites that "the one or more authority records

comprises a master authority record including instructions for governing the one or more authority records in said storage device." *Id*. at 14:27−30.

Petitioner asserts that a person of ordinary skill in the art would have understood the term "master authority record" to mean "data defining the access permissions of an entity that can govern (e.g., create and delete) other authority records." Pet. 9; Ex. 1003 ¶¶ 58−66. In our Institution Decision, we adopted Petitioner's construction as it is consistent with the Specification (Ex. 1001, 3:25−43, 5:25−6:16, 6:20−31, 7:11−8:34, 8:51−9:21, 9:22−44, 12:60−62, Fig. 4−7). Dec. 9−10. Patent Owner does not dispute this construction. PO Resp. 22−23. Upon review of the entire trial record, we do not discern any reason or evidence that compels any deviation from our earlier construction of "master authority record." Therefore, we adopt the previous analysis and construe "master authority record" as "data defining the access permissions of an entity that can govern (e.g., create and delete) other authority records."

6. "root assurance"

Claim 6 depends from claim 1 indirectly and recites "wherein cryptographic code is authenticated with a root assurance in the firmware of the device, wherein the firmware is non-writable." Ex. 1001, 13:17−19. Apart from the claims, the Specification discusses the term "root assurance" once. In particular, the Specification discloses that the cryptographic code is authenticated with a root assurance in the non-writeable firmware of the device. *Id*. at 7:31−33.

Petitioner asserts that a person of ordinary skill in the art would have understood "root assurance" to mean "code used to authenticate other code." Pet. 12−13. Dr. Levy testifies that, with the understanding that "code" may be referred to as "software, executable computer code, computer instructions, or instructions," this construction is appropriate in view of the claims and Specification. Ex. 1003 ¶ 72.

In our Institution Decision, we adopted Petitioner's construction as it is consistent with the Specification (Ex. 1001, 7:31−33). Dec. 10. Patent Owner does not present any argument or evidence regarding this construction in its Response. PO Resp. 22−23.

Upon review of the entire trial record, we do not discern any reason or evidence that compels any deviation from our earlier construction of "root assurance." Therefore, we adopt the previous analysis and construe "root assurance" as "code used to authenticate other code."

C. Principles of Law

A patent 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 ordinary skill in the art; and (4) when in evidence, objective evidence of nonobviousness.[5] *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

D. Overview of Prior Art References

1. Hamlin (Ex. 1004)

Hamlin discloses a disk drive comprising a disk that is divided into a public area partition for storing plaintext data and a secure partition that is a "pristine area for storing encrypted data." Ex. 1004, code (57), 2:49−52.

Figure 1 of Hamlin is reproduced below.

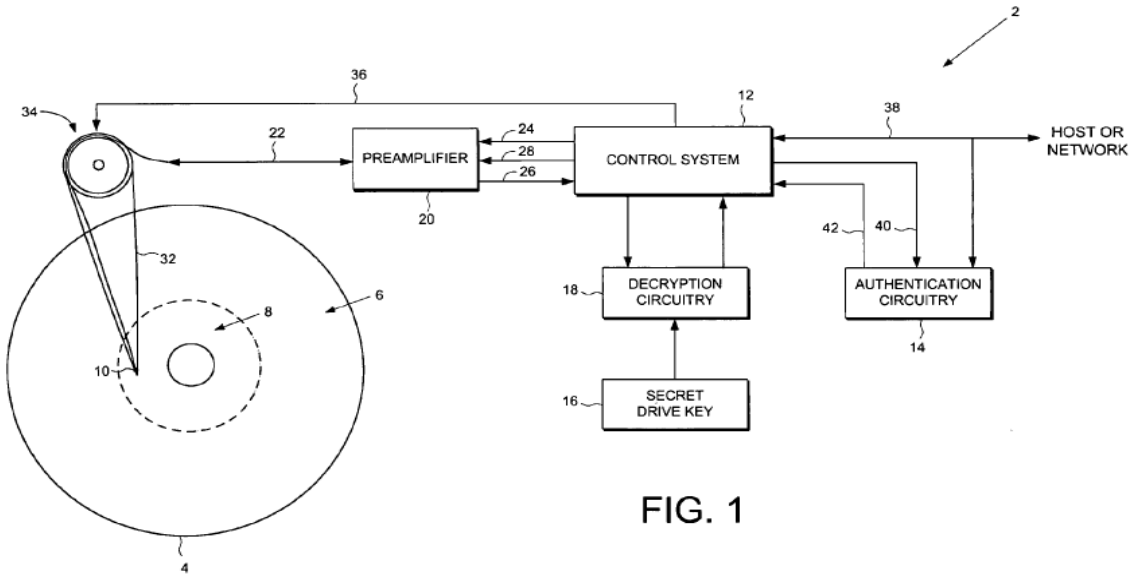

FIG. 1

Figure 1 of Hamlin above shows disk drive 2 comprising disk 4 for storing data. Ex. 1004, 4:13−14. Disk 4 includes public area 6 for storing

[5] Neither party presents evidence or arguments regarding objective evidence of nonobviousness in the instant proceeding. Pet. 77; *see generally* PO Resp.; Sur-reply.

plaintext data and pristine area 8 for storing encrypted data. *Id*. at 4:15−16. The data stored in pristine area 8 includes "sensitive information (e.g., a password, credit card number, etc.)," as well as "user/device authentication information (e.g., a password)." *Id*. at 4:65−5:1, 5:50−63.

Disk drive 2 also comprises head 10 for reading the encrypted data, and control system 12 for controlling access to pristine area 8. *Id*. at 4:18−27. Authentication circuitry 14 is for authenticating a request received from an external entity to access pristine area 8 and for enabling control system 12 if the request is authenticated. *Id*. Disk drive 2 further comprises secret drive key 16 and decryption circuity 18 for decrypting the encrypted data stored in pristine area 8. *Id*.

2. Fisherman (Ex. 1005)

Fisherman discloses a hard disk protection system ("HDPS") for protecting data stored on computer hard disks while permitting multiple user operation. Ex. 1005, code (57). Figure 1 is reproduced below.

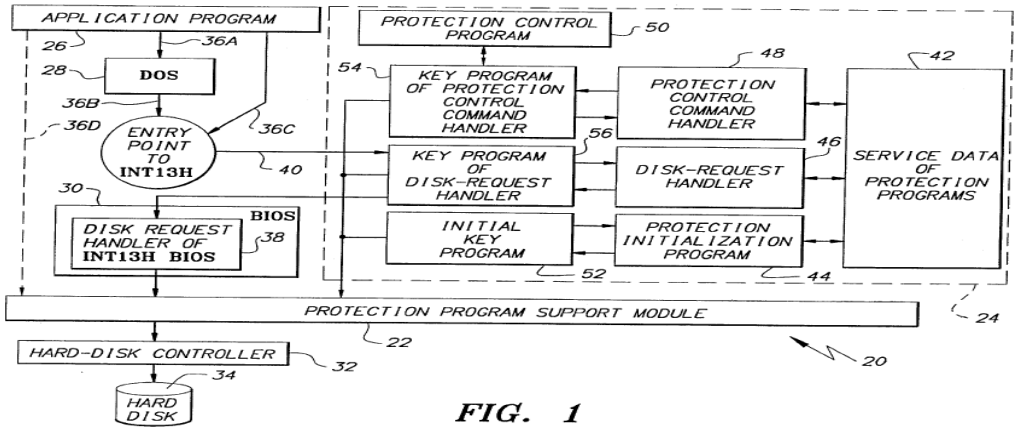

FIG. 1

Figure 1 above shows a block diagram of HDPS 20 installed in a computer. *Id*. at 2:55−56. HDPS 20 comprises protection-program support module ("PPSM") and protection software 24. *Id*. at 3:31−50.

In addition, Fisherman discloses flexible access rights and supervisor user features. Fisherman's ACCESS_FIELD has two subfields, each of which can have a value of 0 or 1, representing read and write rights. *Id*. at 8:46−60. For example, ACCESS_FIELD = (1, 1) means that the cluster is accessible for both reading and writing, and ACCESS_FIELD = (1, 0) means that the cluster is accessible for reading, but not writing. *Id.* at 8:46−60, 22:46−47. Fisherman also discloses a supervisor user who performs privileged operations. *Id*. 1:60−61 ("file-access criteria [are] established by the supervisor"), 10:19−20 ("system 20 should be installed by the supervisor")). The supervisor user can create and delete user's associated data, executing a command that "pertains to the registration of a new user, the deletion of a user, or a change in file status." *Id.* 14:37−57 ("the new user registration command"), 14:66−15:11 ("a delete user command"), 15:20−24.

3. Silvester (Ex. 1006)

Silvester discloses a secure-private partition on a storage device of a computer system. Ex. 1006, code (57). The secure-private partition is normally invisible to an operating system unless the partition is unlocked. *Id*.

Figure 4 is reproduced below.

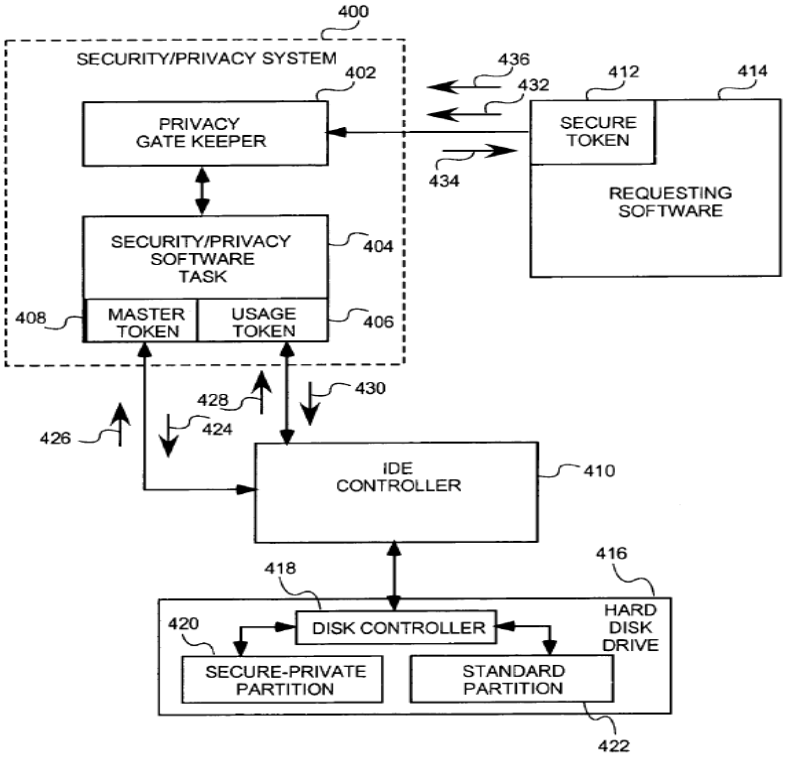

FIG. 4

Figure 4 of Silvester above shows security/privacy system 400, Integrated Device Electronics ("IDE") controller 410, hard disk drive 416, and requesting software 414. *Id*. at 2:54−3:49. Security/privacy system 400 includes privacy gatekeeper 402 and security/privacy software task 404. *Id*. Hard disk drive 416 includes disk controller 418 and is partitioned into standard partition 422 and secure-private partition 420. *Id*.

4. Carter (Ex. 1007)

Carter discloses maintaining a soft-token private key store in a distributed environment. Ex. 1007, code (57). Figures 5 and 6 are reproduced below.

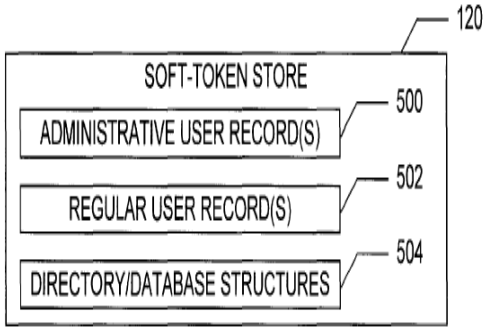

FIG. 5

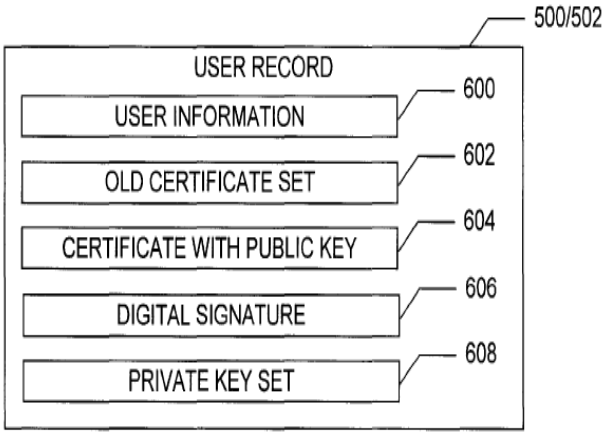

FIG. 6

Figures 5 and 6 above illustrate the structure and content of soft-token store 120, which includes administrative user records 500, regular user records 502, and directory/database structures 504. *Id*. at 8:45−55. Administrative user records 500 contain soft-token information associated with network or other computer system administrators who have responsibility for, and authority over administrative aspects of, both their own accounts and the accounts of non-administrative users. *Id*. Regular user records 502 contain soft-token information associated with non-administrative users, who have responsibility and authority for only their individual accounts. *Id*. User record 500/502 includes user information 600, old certificate set 602, certificate with public key 604, digital signature 606, and private key set 608. *Id*. at 9:9−13.

5. Mirov (Ex. 1008)

Mirov discloses a method and an apparatus for firmware authentication. Ex. 1008, code (57). Figure 2 is reproduced below.

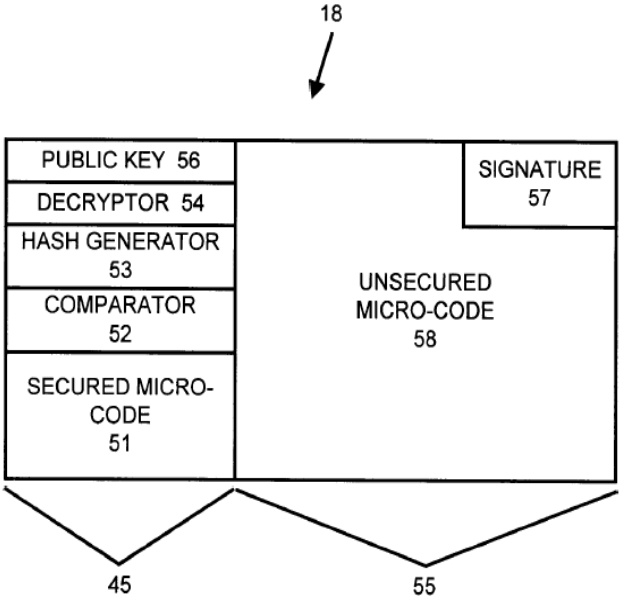

Figure 2 above shows flash programmable read-only memory ("PROM") 18 of a computer system. *Id*. at 3:56−4:55. Flash PROM 18 is divided into two main sections: authentication section 45 and programmable section 55. *Id*. Authentication section 45 authenticates programmable section 55 to verify that the micro-code instructions that boot the computer system are trusted. *Id*. Authentication section 45 includes secure micro-code 51, comparator 52, hash generator 53, decryptor 54, and public key 56. *Id*. Unsecured section 55 includes digital signature 57 and unsecured micro-code 58. *Id*. Micro-code is referred to as firmware. *Id*. at 1:15−16.

E. Ground 1: Obviousness over Hamlin, Fisherman, and the knowledge of an ordinarily skilled artisan

Petitioner asserts that claims 1−3, 5, and 12−14 are unpatentable under § 103(a) as obvious over Hamlin in combination with Fisherman and

the knowledge of an ordinarily skilled artisan, citing to Dr. Levy's Declaration for support. Pet. 20–47 (citing Ex. 1003). Petitioner relies on Hamlin to teach a storage device (disk drive) and a storage medium (disk) that has a secure data partition (pristine area) for storing an authority record (authentication information). *Id*. Petitioner also relies on Hamlin, in combination of Fisherman and the knowledge of an ordinarily skilled artisan, to teach a master authority record (supervisor's record) stored in the secure data partition. *Id*. at 28−31. Petitioner further relies on Hamlin, in view of the knowledge of an ordinarily skilled artisan, to teach or suggest the claimed "firmware," citing Dr. Levy's Declaration (Ex. 1003 ¶¶ 111−123), Hamlin II (Ex. 1009), Hamlin III (Ex. 1010), and U.S. Patent No. 6,631,453 B1 to Friday (Ex. 1011), for support. *Id*. at 22−26, 39−40.

Patent Owner argues that the asserted prior art combination fails to disclose a firmware, an authority record, and a master authority record, as required by the claims, and that a person of ordinary skill in the art would not have been motivated to combine Hamlin with Fisherman. PO Resp. 23−61; Sur-reply 1−27.

For the reasons discussed below, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1−3, 5, and 12−14 are unpatentable.

1. Claims 1, 12, and 13

a. "firmware for reading data from and writing data to the storage medium" (claim 1)

Claim 1 recites "firmware for reading data from and writing data to the storage medium." Ex. 1001, 12:55−56. As discussed above in our claim construction Section II.B.1−2, we construe "firmware" as "software that has been copied on (and therefore stored in) an integrated circuit, which usually may be a ROM or other non-writable and non-volatile memory." Ex. 1003 ¶ 111. We decline to adopt Patent Owner's claim construction that construes "firmware *for* reading data from and writing data to the storage medium" to require the firmware by itself performs the read/write operations. Sur-reply 6−8.

In its Petition, Petitioner asserts that the combination of Hamlin, Fisherman, and the knowledge of an ordinarily skilled artisan teaches the aforementioned "firmware" limitation. Pet. 22−26. Petitioner explains that Hamlin teaches "a control system for interfacing with a host computer to facilitate read and write commands *to write data to and read data from the pristine area of the disk*." *Id*. (citing Ex. 1004, code (57), 2:52−55, 3:12−16, 4:28−44, 8:64−67, 9:55−67, 10:55−11:4, 11:17−12:3) (emphasis added).

Petitioner argues that an ordinarily skilled artisan would have understood that "Hamlin discloses using firmware (*e.g.*, software that implements, *inter alia*, the 'control system 12') for reading data from and writing data to the storage medium and, at a minimum, it would have been obvious." *Id.* According to Petitioner, such an artisan would have known

that "storage devices such as the Hamlin disk drive would have used a processor running firmware (instructions)." *Id*. Dr. Levy testifies that, at the time of the invention, "it was well known to implement functional elements inside a storage device such as Hamlin's 'disk drive 2' using a processor running firmware." Ex. 1003 ¶¶ 112−123.

Upon consideration of the evidence in this entire trial record, we agree with Petitioner that the combination of Hamlin, Fisherman, and the knowledge of an ordinarily skilled artisan teaches the aforementioned "firmware" limitation recited in claim 1.

Patent Owner opposes and advances several arguments. First, Patent Owner argues that Hamlin does not teach "firmware," citing to Mr. Jawadi's testimony for support. PO Resp. 23−26; Ex. 2008 ¶¶ 38−67; Sur-reply 9−10.

To the extent that Patent Owner requires the prior art to use the exact terminology as the claims, an obviousness determination is not an *ipsissimis verbis* test. *Cf. In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009) (addressing similar concept in the context of anticipation). Instead, the test for obviousness is whether the references, taken as a whole, would have suggested the claimed subject matter to a person of having ordinary skill in the art at the time the invention was made. *See In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986).

Significantly, Patent Owner and Mr. Jawadi fail to consider Hamlin as a whole. In particular, they ignore that Hamlin expressly incorporates by reference Tygar, which discloses secure coprocessors having firmware.

Ex. 1004, 6:14−22; Ex. 1017, 1−3, 12−13. In its Sur-reply, Patent Owner concedes that Hamlin's control system and authentication circuitry may be implemented using Tygar's secure coprocessors. Sur-reply 11.

"When a document is 'incorporated by reference' into a host document, such as a patent, the referenced document becomes effectively part of the host document as if it were explicitly contained therein." *Telemac Cellular Corp. v. Topp Telecom, Inc.*, 247 F.3d 1316, 1329 (Fed. Cir. 2001). There is no dispute that Hamlin incorporates Tygar by reference in its entirety. Pet. 25; *see generally* PO Resp.; Sur-reply. As a host document, Hamlin cites to Tygar in a manner that makes clear that Tygar's disclosure regarding secure coprocessors is effectively part of Hamlin's disclosure as if it were explicitly contained therein. *Advanced Display Sys., Inc. v. Ken State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000).

As Petitioner explains, Hamlin discloses that "control system 12 . . . may be implemented using tamper resistant circuitry to protect the decrypted authentication data." Pet. 25; Reply 1−2; Ex. 1004, 6:14−22. Hamlin also refers to Tygar's secure coprocessors as an example of the tamper resistant circuitry. Ex. 1004, 6:14−22; Ex. 1017. Indeed, Hamlin states:

> In addition, all or part of the control system 12 and/or the authentication circuitry 14 may be implemented using tamper resistant circuitry to protect the decrypted authentication data. *An example discussion of tamper-resistant circuitry is provided in Tygar*, J. D. and Yee, B. S., "Secure Coprocessors in Electronic Commerce Applications," Proceedings 1995 USENIX Electronic Commerce Workshop, 1995, New York, which *is incorporated herein by reference*.

Ex. 1004, 6:14−22 (emphases added).

Tygar discloses secure coprocessors executing instructions that include those stored on a ROM (firmware). Ex. 1017, 1−3 ("A secure coprocessor is a hardware module containing (1) a CPU, (2) boostrap ROM, and (3) secure non-volatile memory."), 12, 13. In short, Tygar's secure coprocessors provide examples of Hamlin's tamper-resistant circuitry for control system 12 and authentication circuitry 14. Ex. 1017, 1−3, 12−13; Ex. 1003 ¶¶ 118−119; Ex. 1021 ¶¶ 26−29. Hence, Hamlin, which incorporates Tygar by reference, discloses using firmware in a disk drive to protect the decrypted data. Ex. 1004, 6:14−12; Ex. 1017, 1−3, 12, 13. Moreover, Dr. Levy testifies that one of ordinary skill in the art would have recognized that the behavior of Hamlin's control system (e.g., memory mapping) suggests firmware. Ex. 1003 ¶¶ 117 (citing Ex. 1004, 4:44−50; 7:63−66, 3:21−25; Ex. 1012, 823, 224, 411−412).

Therefore, Patent Owner's argument that Hamlin does not teach firmware is unavailing.

Second, Patent Owner argues that Hamlin II and Hamlin III should not be considered because Petitioner does not identify these references in its statements of the asserted grounds. PO Resp. 26 n.4. Patent Owner also contends that Hamlin, Hamlin II, and Hamlin III disclose different inventions, solve different problems, and have different implementations. *Id.* at 26−32. Patent Owner further avers that Petitioner failed to describe how and why Hamlin, Hamlin II, Hamlin III, and Fisherman are combined.

Patent Owner's arguments are misplaced. When considering whether a claimed invention would have been obvious, "the knowledge of such an

artisan is part of the store of public knowledge that must be consulted." *Randall Mfg. v. Rea*, 733 F.3d 1355, 1362 (Fed. Cir. 2013); *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1365 (Fed. Cir. 2015).

Here, Dr. Levy testifies that using a processor and firmware in a disk drive to perform disk drive operations was known in the art at the time of the invention and that a person of ordinary skill in the art would have recognized that using firmware (running on a processor) was a well-known implementation in storage devices. Ex. 1003 ¶¶ 112−123. We credit Dr. Levy's testimony (*id.*) as it is supported by Hamlin II, Hamlin III, and Friday. *See, e.g.*, Ex. 1009, 7:38−40 ("The components in the secured disk drive 20 shown in FIG. 2 may be implemented in integrated circuitry or in firmware executed by a microprocessor."); Ex. 1010, 5:18−22 ("The disk drive 22 is less susceptible to virus attacks because the firmware implemented by the disk controller 34 is essentially static, as determined by the manufacturing process, and facilities can be employed to monitor the firmware for tampering."); Ex. 1011, 5:35−38 ("The drive electronics unit 88 has a CPU 90, a memory 92 and a firmware module 94 which operate the disk drive unit 84 in the normal manner known to those skilled in the art.").

Based on the evidence in this entire trial, we are persuaded that Petitioner has shown sufficiently that the combination of Hamlin, Fisherman, and the knowledge of an ordinarily skilled artisan, teaches the claimed "firmware." Patent Owner's arguments regarding Hamlin II and Hamlin III do not undermine Petitioner's showing.

Third, Patent Owner argues that Hamlin does not disclose "firmware *for* reading data from and writing data to the storage medium" because the claim language requires the firmware by itself performs the read/write operations. PO Resp. 24−25; Sur-Reply 6−8, 14−15. According to Patent Owner and Mr. Jawadi, "Hamlin's facilitation of reading and writing is not the same thing as actually performing the reading and writing required by Claim 1." PO Resp. 24−25; Ex. 2008 ¶¶ 27−29, 31.

However, both Patent Owner and Mr. Jawadi rely on Patent Owner's improper claim construction that requires the firmware by itself performs the read/write operation. As discussed in our claim construction Section II.B.2, we decline to adopt Patent Owner's construction that improperly imports an extraneous limitation into the claims. Nothing in the claim's plain language requires that read and write commands must originate from the firmware or that no other component outside the firmware may play a role in reading data from and writing data to the storage medium.

In addition, Patent Owner and Mr. Jawadi fail to consider Hamlin as a whole and read Hamlin overly narrow. Hamlin is not limited to merely "facilitation of reading and writing," as Patent Owner and Mr. Jawadi suggest. PO Resp. 24−25; Ex. 2008 ¶¶ 27−29, 31. Indeed, Hamlin expressly discloses that the disk drive includes "control system 12 for controlling access to the pristine area of the disk 4" that stores encrypted data, "allow[ing] a write or read operation only if certain predetermined conditions are satisfied." Ex. 1004, code (57), 2:52−55, 3:12−21, 4:18−19, 4:58−60. Hamlin also discloses "a control system for interfacing with a host

computer to facilitate read and write commands *to write data to and read data from the pristine areas of the disk*." *Id.* at 8:64−66 (emphasis added). Moreover, Hamlin discloses "using the control system internal to the disk drive *to read* the encrypted data stored in the pristine area," and "*to enable servoing* the pristine area . . . wherein[] the servo bursts are *written to the disk* in encrypted form." *Id.* at 9:66−67, 10:7−12 (emphases added).

In light of Hamlin's disclosure, we agree with Dr. Levy's testimony that Hamlin's "control system is used to read data from and write data to the disk drive 2 and therefore the reading from and writing to the storage medium of Hamlin is carried out by Hamlin's firmware." Ex. 1003 ¶ 121. We credit the testimony of Dr. Levy (Ex. 1003 ¶ 121) over that of Mr. Jawadi (Ex. 2008 ¶¶ 27−29, 31). We find Dr. Levy's testimony is supported by Hamlin's disclosure. *See, e.g.,* Ex. 1004, code (57), 2:52−55, 3:12−16, 4:18−19, 4:58−60, 8:64−66, 9:66−67.

Based on the evidence in this entire trial record, we determine that Petitioner has shown sufficiently that Hamlin teaches the aforementioned "firmware" limitation recited in claim 1. Patent Owner's argument that Hamlin does not disclose "firmware *for* reading data from and writing data to the storage medium" because the claim language requires the firmware by itself performs the read/write operations (PO Resp. 24−25; Sur-Reply 6−8, 14−15) is unavailing.

b. "only the firmware is permitted to access the secure data and the one or more authority records" (claim 1) and "firmware . . . adapted to limit access to the security partition by an operating system of a computer system" (claim 12)

Claim 1 recites "wherein only the firmware is permitted to access the secure data and the one or more authority records." Ex. 1001, 13:1−2. Claim 12 recites "firmware disposed within the storage device adapted to limit access to the security partition by an operating system of a computer system." *Id.* at 14:23−26.

Petitioner asserts that "Hamlin's control system and authentication circuitry would be understood to be implemented in firmware executed by a processor," and that "Hamlin's figures show that only the control system (firmware) is directly connected (through the preamplifier or not) to the storage medium." Pet. 32−33, 39−40 (citing Ex. 1004, 4:65−5:7, 5:58−63, 6:4−8, Figs 1−3, Ex. 1003 ¶¶ 137−139, 141). According to Petitioner, "the firmware must be the internal component through which access is performed, e.g., the 'host or network' accesses the data through only the control system firmware," and "all data stored on the storage medium is only accessible via the firmware." *Id.* Petitioner explains that Hamlin's disk drive includes an authentication circuitry that uses the user/device authentication information to broker access to the pristine area, and it allows access to those users and devices found in the user/device authentication information set of data when properly verified using their corresponding authentication information (e.g., a password). *Id*. at 38−40; Ex. 1003 ¶¶ 204, 208−209; Ex. 1004, 5:50−6:3. Petitioner also explains that Hamlin's

authentication information is used by authentication circuitry 14 to grant or deny access to pristine area 8. *Id*. at 39−40.

Based on the evidence of record, we are persuaded that Petitioner has demonstrated sufficiently that Hamlin, in view of the knowledge of an ordinarily skilled artisan, discloses the aforementioned limitations recited in claims 1 and 12.

Patent Owner counters that the combination does not teach "only the firmware is permitted to access the secure data and the one or more authority records" because Hamlin does not disclose firmware. PO Resp. 31−32.

Patent Owner's argument is unavailing. As discussed above, Hamlin, which incorporates by reference Tygar, teaches implementing the control system and authentication circuitry using secure coprocessors that include firmware. Ex. 1004, 6:14−12; Ex. 1017, 1−3, 12, 13. Patent Owner also concedes that Hamlin's control system and authentication circuitry may be implemented using Tygar's secure coprocessors that include firmware. Sur-reply 11.

In its Sur-reply, Patent Owner further argues that Hamlin does not teach or suggest "*only the firmware* is permitted to access the secure data and the one or more authority records" because Hamlin's decryption circuitry and the operating system of a host computer also have access to the secure data. Sur-reply 10−17 (Ex. 1004, 4:61−5:1).

Patent Owner's argument improperly rests on its implicit claim construction that imports a negative limitation into the claims—no other component or external entity is permitted to request access via the firmware.

Sur-reply 10−17. As discussed above in our claim construction Section II.B.3, we decline to adopt Patent Owner's construction. Instead, we construe "only the firmware is permitted to access the secure data and the one or more authority records" to mean simply that "all access to the secure data and the authority records is performed via and brokered by the firmware." *See* Ex. 1001, 8:30−34, 12:64−65; Ex. 1002, 328−29, 384−85; Ex. 1003 ¶ 138.

In addition, Patent Owner's argument narrowly focuses on one portion of Hamlin and fails to consider Hamlin as a whole. Sur-reply 12, 15−16 (citing Ex. 1004, 4:61−5:1). Hamlin makes clear that the host and decryption circuitry themselves do not access the pristine area, rather they must seek access through control system 12, which includes firmware. Ex. 1004, 4:58−60 ("*The control system 12 will access the pristine area 8* and allow a write or read operation only if certain predetermined conditions are satisfied." (emphasis added)), 5:45−49 ("*The encrypted data is read from the disk 4 by the control system 12*, decrypted by the decryption circuitry 18." (emphasis added)). As Dr. Levy testifies, "the firmware (control system) is permitted to access the secure data and the authentication information, and all entities other than the firmware that attempt to access the data on Hamlin's storage medium must do so *via the firmware*." Ex. 1003 ¶ 139. We credit Dr. Levy's testimony because it is supported by Hamlin. Figure 1 of Hamlin is reproduced below.

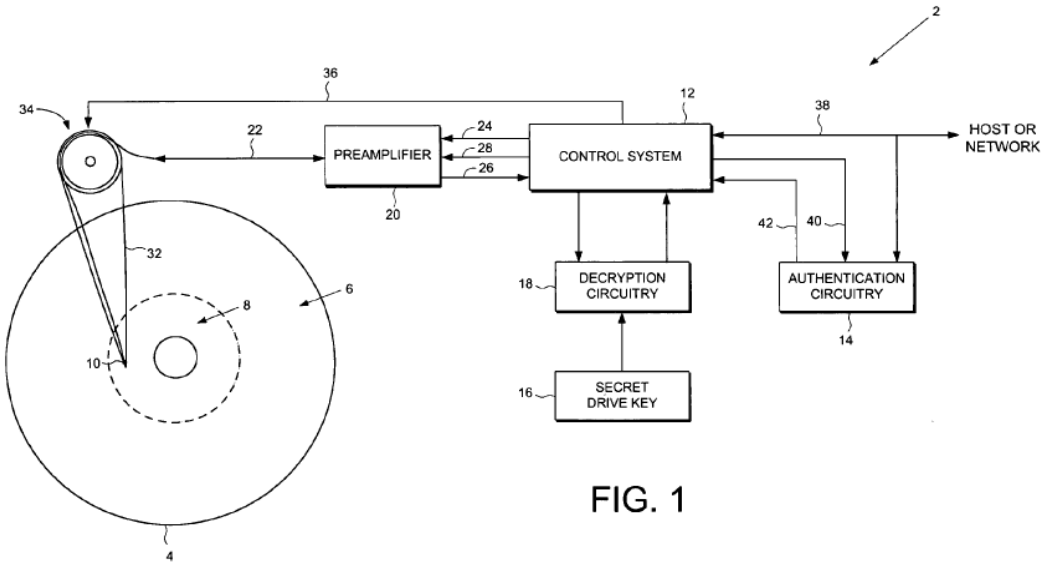

FIG. 1

Figure 1 of Hamlin illustrates disk drive 2 comprising disk 4 having public area 6 for storing plain text data and pristine area 8 for storing encrypted data. Ex. 1004, 3:52−59, 4:3−27. As shown, only control system 12 is directly connected (whether through the preamplifier or not) to disk 4.

Hamlin expressly discloses "control system 12 for *controlling access to the pristine area 8 of the disk 4*." *Id.* at 4:18−19 (emphasis added). Decryption circuitry 18 and the external entities (e.g., the host or network) must access the secure data or authority records stored in pristine area 8 *via control system 12*. *Id.* at 5:45−49 ("*The encrypted data is read from the disk 4 by the control system 12*, decrypted by the decryption circuitry 18." (emphasis added)), 5:8−10 ("the control system 12 *receives via line 38 a request from an external entity* to access the pristine area 8 (read or write)" (emphasis added)). Hamlin makes clear that control system 12 (not the host, network, or decryption circuitry) performs the actual access (read or write). *Id.* at 3:19−21 ("The disk comprises a plurality of physical blocks *accessed*

by the control system through physical block addresses." (emphasis added)), 4:28−34 ("[D]uring a write operation . . . preamplifier 20 *receives digital write data 24 from the control system 12* which is to be written to the disk 4." (emphasis added)), 4:38−44 ("During a read operation . . . preamplified analog read signal 26 is *supplied to the control system 12* where it is demodulated into an estimated data sequence representing the originally recorded data." (emphasis added)), 4:47−50 ("The *control system 12 sends control sequences* to the preamplifier 20 over line 28 in order to configure it for write or read operations." (emphasis added)).

Therefore, we are not convinced by Patent Owner's argument that Hamlin does not teach "*only the firmware* is permitted to access the secure data and the one or more authority records" because Hamlin's decryption circuitry and the operating system of a host computer also have access to the secure data. Sur-reply 10−17.

For the foregoing reasons, we determine that Petitioner has shown sufficiently that Hamlin, in view of Fisherman and the knowledge of an ordinarily skilled artisan, teaches "wherein only the firmware is permitted to access the secure data and the one or more authority records," as recited in claim 1, and "firmware disposed within the storage device adapted to limit access to the security partition by an operating system of a computer system," as recited in claim 12.

c. "one or more authority records"

Claim 1 recites "the secure data partition for storing secure data and one or more authority records, wherein the one or more authority records

define access permissions relating to the secure data partition and the secure data." Ex. 1001, 12:59−62. Claim 12 recites "a security partition containing one or more authority records and at least one data set associated with each of the one or more authority records" and "a mechanism within the storage device adapted to limit access to the security partition based on the one or more authority records." *Id*. at 14:15−20.

As discussed above in our claim construction Section II.B.4, we determine that "authority records" should be given its plain and ordinary meaning, and "access permissions" is "related to the secure data partition and the secure data." However, we decline to adopt Patent Owner's implicit claim construction. We clarify that "authority records" does not exclude information that is used for both authentication and authorization. And, the claim language "one or more authority records define access permissions relating to the secure data partition and the secure data" encompasses both: (1) a single authority record that includes multiple access permissions, and (2) multiple authority records that include multiple access permissions—e.g., each record includes at least one permission.

Petitioner asserts that Hamlin alone, or in view of Fisherman, discloses the aforementioned "authority records" limitations. Pet. 27−30, 37−40. Upon consideration of the entire trial record, we determine that Petitioner has shown sufficiently that Hamlin alone teaches the "authority records" limitations under the proper claim construction. Although we decline to adopt Patent Owner's claim construction, we determine that

Petitioner has shown sufficiently that Hamlin in view of Fisherman teaches the "authority records" limitations, even under Patent Owner's construction.

In its Petition, Petitioner asserts that Hamlin's pristine area (the secure data partition) stores sensitive information (secure data), such as "a password, credit card number, etc.," as well as user/device authentication information (authority records). Pet. 27 (citing Ex. 1004, 4:65−5:1, 5:50−63, 6:4−8, 7:55−60, 8:12−15). Petitioner explains that Hamlin's authentication information discloses "one or more authority records" because the authentication information defines an entity's access permissions to the pristine area and Hamlin's authentication circuitry uses it to *authorize or deny access* to the data or information stored in the pristine area. *Id*. at 28 (citing Ex. 1004, 4:61−5:7, 5:58−6:12, 7:38−43, 7:50−59).

Dr. Levy testifies that a person of ordinary skill in the art would have understood that Hamlin's authentication information (the authority records) includes the entity ID, "password, finger print, voice print, spectral signature, etc." and information sufficient to identify the data set for which access is protected and the associated area in the pristine area storing the sensitive information (e.g., a credit card number). Ex. 1003 ¶¶ 125, 126 (citing Ex. 1004, 4:61−5:7, 5:50−63, 7:38−43, 7:50−59). Dr. Levy also testifies that the authentication information is an "authority record" because "the authentication information is used to control access to the pristine area 8 and to the data within that partition." *Id.* ¶ 126.

Alternatively, Petitioner asserts that "[t]o the extent authority records are required to define flexible access rights or be associated with a specific

data set, Fisherman discloses this." Pet. 28−29; Ex. 1003 ¶¶ 128. Petitioner avers that Fisherman discloses "one or more authority records" because Fisherman's ACCESS_FIELD has two subfields, each of which can have a value of 0 or 1, representing read and write rights. Ex. 1005, 8:46−60. For example, ACCESS_FIELD = (1, 1) means that the cluster is accessible for both reading and writing; and ACCESS_FIELD = (1, 0) means that the cluster is accessible for reading, but not writing. *Id.* at 8:46−60, 22:46−47.

Petitioner argues that one of ordinary skill in the art would have been motivated to include Fisherman's flexible access rights in Hamlin's authentication information and store such records in Hamlin's pristine area so that the entities in Hamlin can have different types of rights to access the data in the pristine area. Pet. 45−47. Petitioner explains that "an additional field may be added to Hamlin's 'user/device authentication information' to denote what kind of access right the user has, as Fisherman teaches." *Id.*

Dr. Levy testifies that Fisherman "discloses more detailed user access permissions, which would also improve the security and utility of the Hamlin invention" because "such protection methods are known to 'prevent mischievous, intentional violation of an access restriction by a user.'" Ex. 1003 ¶¶ 223, 226 (quoting Ex. 1016 (Abraham Silberschatz & Peter Baer Galvin, *Operating System Concepts*, 598 (Lynne Doran Cote ed., 5th ed. 1998))). Dr. Levy also testifies that "Fisherman's flexible access rights would allow the Hamlin invention to establish tiers of trust and enforce different access policies depending on the user's trust tier." *Id.* ¶ 227.

Based on the evidence in the entire trial record, we determine that Petitioner has demonstrated sufficiently, either relying on Hamlin alone or alternatively Hamlin in view of Fisherman, that the combination of Hamlin, Fisherman, and the knowledge of an ordinary skilled artisan teaches the aforementioned "authority records" limitations recited in claims 1 and 12.

Patent Owner opposes, advancing several arguments.

First, Patent Owner argues that Petitioner conflates authentication with authorization and that Hamlin discloses authentication but not authorization, suggesting that authentication and authorization cannot be performed using the same information. PO Resp. 32−36 (citing Ex. 2008 ¶¶ 112−120); Sur-reply 23−24.

As discussed above in our claim construction Section II.B.4, however, we decline to adopt Patent Owner's implicit claim construction that improperly imports a negative limitation into the claims. Rather, we determine that the term "authority records" does not exclude information that is used for both authentication and authorization.

As Dr. Levy testifies, Hamlin's authentication information "is used to *both authenticate* the external entity, *i.e.*, confirm the identity of the external entity, *and authorize* the external entity, *i.e.*, grant the external entity access to the user's area in the pristine area." Ex. 1021 ¶ 66 (emphases added). In particular, Hamlin's authentication information defines access permissions (e.g., read or write) to the pristine area and the secure data stored in the pristine area. Ex. 1004, 4:61−5:7, 5:50−6:12, 7:38−43, 7:50−60, 8:12−15. For example, Hamlin discloses that "[w]hen an external entity sends *a*

request to access to the pristine area 8, . . . [t]he authentication circuitry 14 uses the entity ID to read the associated password from the pristine area 8, and the request is authenticated if it matches the entity password received in the request," and that "*[o]therwise*, the request is not authenticated and *access is denied*." *Id*. at 4:61−5:7 (emphases added). Hence, Hamlin's authentication information is used for both authentication and authorization to authorize or deny access to the secure data stored in the pristine area. Ex. 1003 ¶ 126.

Applying the proper claim construction, we determine that Petitioner has established sufficiently that Hamlin teaches the aforementioned "authority records" limitations recited in claims 1 and 12. Patent Owner's argument that Petitioner conflates authentication with authorization and that Hamlin discloses authentication but not authorization is unavailing.

Second, Patent Owner argues that the construction of "authority records" requires multiple access permissions in that "a single authority record defines access permission***s*** (plural), such as R/W Access Rights, WriteOnce, Write Over, WriteAny, ReadCur, ReadAny, and Hidden Read." PO Resp. 25; Sur-reply 24−27; Ex. 2008 ¶¶ 121−136.

To the extent that Patent Owner argues that Hamlin does not disclose each authority record includes multiple access permissions, that argument is unavailing. As discussed above in our claim construction Section II.B.4, the claim language encompasses both: (1) a single authority record that includes multiple access permissions, and (2) multiple authority records that include multiple access permissions (e.g., each record includes at least one

permission). Moreover, Patent Owner concedes that "[b]y the plain and customary reading of the phrase 'wherein the one or more authority records defines access permissions,' it is clear that one authority record can define multiple access permissions, *or alternatively, multiple authority records can define multiple access permissions*." Sur-reply 25 (emphasis added).

Applying the proper claim construction, we find that Petitioner has established sufficiently that Hamlin teaches the aforementioned "authority records" limitations because Hamlin teaches multiple authority records that collectively include multiple access permissions. As Petitioner points out (Pet. 27−28; Reply 13; 1003 ¶¶ 125−127), Hamlin discloses that multiple external entities can request access to the pristine area, and each entity has an entity ID, password, and associated area to access in the pristine area. Ex. 1004, 4:61−5:7 ("disk drive 2 receives requests from external entities (e.g., a host or client computer) to access the pristine area"), 5:50−6:12, 7:38−43, 7:50−60, 8:12−15. For example, an external entity may send a request to disk drive 2 *to store* a credit card number in the pristine area in encrypted form, and a subsequent request may be sent to disk drive 2 *to read* the encrypted message stored in the pristine area. *Id.* at 7:38−49. Therefore, Hamlin discloses multiple authority records that collectively include multiple permissions—each record having at least one access permission (read or write) to the pristine area. Ex. 1021 ¶¶ 69−72. Accordingly, Patent Owner's argument that Hamlin does not discloses each authority record includes multiple access permissions is unavailing.

In addition, even if we were to apply Patent Owner's implicit claim construction that requires each authority record to include multiple access permissions, we find that Petitioner has shown sufficiently that Hamlin, in combination with Fisherman and the knowledge of an ordinarily skilled artisan, teaches such authority records. Pet. 15−17, 27−30, 44−47; Ex. 1003 ¶¶ 128−129.

As discussed above, Petitioner alternatively relies upon Hamlin in view of Fisherman to disclose "one or more authority records" because Fisherman discloses an authority record that includes flexible access permissions by having an access field that includes two subfields, each of which can have a value of 0 or 1, representing read and write rights. Pet. 28−29, 45−47; Ex. 1003 ¶ 128; Ex. 1005, 8:46−60; Reply 15−16; Ex. 1021 ¶¶ 74−83. Petitioner explains that "an additional field may be added to Hamlin's 'user/device authentication information' to denote what kind of access right the user has, as Fisherman teaches." Pet. 46−47; Ex. 1003 ¶ 230. Petitioner avers that a person of ordinary skill in the art would have been motivated to include the additional field in Hamlin's authentication information and store the records in Hamlin's pristine area so that the external entities in Hamlin can have different types of rights to access the data in the pristine area. Pet. 45−47; Reply 15−16; Ex. 1003 ¶¶ 223−232; Ex. 1021 ¶¶ 74−75. Dr. Levy testifies that Fisherman "discloses more detailed user access permissions, which would also improve the security and utility of the Hamlin invention" because "such protection methods are known to 'prevent mischievous, intentional violation of an

access restriction by a user.'" Ex. 1003 ¶¶ 223, 226 (quoting Ex. 1016). Dr. Levy also testifies that "Fisherman's flexible access rights would allow the Hamlin invention to establish tiers of trust and enforce different access policies depending on the user's trust tier." *Id.* ¶ 227.

Based on the evidence in this entire trial record, we determine that Petitioner has established adequately that Hamlin, in view of Fisherman and the knowledge of an ordinarily skilled artisan, teaches the aforementioned "authority records" limitations even under Patent Owner's implicit construction that requires multiple permissions in each record.

Third, Patent Owner argues that Fisherman does not disclose device-based authority records, a disk-level partition, and a security partition, and that Fisherman's implementation involves reducing available disk space which is contrary to the teachings of the '020 patent. PO Resp. 36−42.

However, attacking Fisherman individually does not undermine Petitioner's obviousness showing that is based on a combination of Hamlin, Fisherman, and the knowledge of an ordinarily skilled artisan. *See In re Keller* 642 F.2d 413, 426 (CCPA 1981) (nonobviousness cannot be established by attacking prior art teachings individually where the ground of unpatentability is based upon a combination of the prior art teachings). The relevant issue here is whether the prior art combination, taken as a whole, would have suggested the patentees' claimed invention to a person having ordinary skill in the art. *See Merck*, 800 F.2d at 1097.

Significantly, as discussed above, Hamlin teaches using authentication information (an authority record) stored in the pristine area (security partition) of a storage device for granting or denying access to the pristine area. The combination of Hamlin, Fisherman, and the knowledge of an ordinarily skilled artisan would have taught an authority record having multiple access permissions stored in the pristine area of a storage device.

In addition, Patent Owner narrowly focuses on the physical differences between the systems disclosed in the references and requires bodily incorporating Fisherman's system into Hamlin's disk drive. "It is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements." *In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. June 26, 2012); *In re Etter*, 756 F.2d 852, 859 (Fed. Cir. 1985) (en banc); *Keller* 642 F.2d at 425 (Obviousness does not require that all of the features of the secondary reference be bodily incorporated into the primary reference.).

Accordingly, Patent Owner's argument that Fisherman does not disclose a device-based authority records, disk-level partition, and security partition, and that Fisherman's implementation involves reducing available disk space which is contrary to the teachings of the '020 patent, is unavailing. PO Resp. 36−42. To the extent that Patent Owner argues that there is no motivation to combine Hamlin with Fisherman, we address those arguments below in Section II.E.1.e (the discussion on the reasons to combine Hamlin with Fisherman).

Fourth, Patent Owner argues that "Hamlin discloses storing passwords but not records" because Hamlin discloses only a single field (a password) is read from the pristine area, citing a portion of Hamlin for support. PO Resp. 34−36 (citing Ex. 1004, 5:51−64, 6:4−5); Ex. 2008 ¶¶ 126−136.

However, Patent Owner implicitly construes "authority records" to require multiple fields in each authority record. As discussed in our claim construction Section II.B.4, we decline to adopt this construction because it improperly imports a limitation into the claims. Even if we apply Patent Owner's implicit construction, we find that Petitioner has shown sufficiently that the asserted combination teaches the aforementioned "authority records" limitations recited in claims 1 and 12 for the reasons discussed below.

Notably, Patent Owner narrowly focuses on a portion of Hamlin and fails to consider Hamlin as a whole. The two sentences immediately before the portion of Hamlin relied upon by Patent Owner, in the very same paragraph, state:

> User/device authentication may be implemented, for example, by associating selected information (e.g., a password, finger print, voice print, spectral signature, etc.) with a trusted entity. In one embodiment, user/device authentication information (e.g., a password) is stored in the pristine area 8 of the disk 4.

Ex. 1004, 5:58−63. These two sentences make clear that Hamlin's authentication information includes "a password, finger print, voice print, spectral signature, etc.," which is more than a single field for a password. *Id.* The sentences also make clear that the authentication information is stored in the pristine area. *Id.* Patent Owner's reading of Hamlin is unduly narrow, limiting the authentication information to only a single field.

In addition, the portion of Hamlin relied upon by Patent Owner does not support Patent Owner's argument that "Hamlin discloses storing only passwords but not records." PO Resp. 35−36. That portion of Hamlin makes clear that "authentication circuitry 14 *uses the entity ID to read the associated password* from the pristine area 8." Ex. 1004, 5:65−67 (emphasis added). Both Patent Owner and Mr. Jawadi ignore that the password is *associated* with the entity ID. PO Resp. 34−36; Ex. 2008 ¶¶ 126−136. The prior sentences (reproduced above) also make clear that the authentication information is *associated with a trusted entity*. Ex. 1004, 5:58−63.

As Dr. Levy testifies, one of ordinarily skill in the art would have understood that Hamlin's authentication information includes at least: (1) one field for identifying the user ("entity ID"), and (2) another field for containing the authentication information itself that is associated with the entity ID. Ex. 1003 ¶ 126. Dr. Levy also testifies that "the authority record would include the entity ID, entity password, and information sufficient to identify the area of the pristine area to which the external entity has the right to access." Ex. 1021 ¶ 67. Dr. Levy explains that "in order to allow the access, the authentication circuitry must first authenticate the external entity by determining whether the entity ID and password match the authentication information stored in the pristine area." *Id*. We credit Dr. Levy's testimony (Ex. 1003 ¶ 126; Ex. 1021 ¶ 67), as it is consistent with the teachings of Hamlin (Ex. 1004, 5:50−6:3) that the authentication information (authority records) for each entity includes more than one field.

Accordingly, Patent Owner's argument that "Hamlin discloses storing passwords but not records" is unavailing. Moreover, Patent Owner does not dispute that Hamlin in view of Fisherman discloses an authority record with multiple fields, including an access field that provides flexible access permissions (Ex. 1005, 8:46−60). *See generally* PO Resp.; Sur-reply.

Finally, Patent Owner argues that Hamlin's authentication information is not organized, structured, or stored as records, as required by the claims. PO Resp. 35. However, the claims do not recite any specific organization or structure. It is well established that limitations not appearing in the claims cannot be relied upon for patentability. *In re Self*, 671 f.2d 1344, 1348 (CCPA 1982).

For the foregoing reasons, we determine that Petitioner has shown sufficiently that Hamlin, in view of Fisherman and the knowledge of an ordinarily skilled artisan, teaches the aforementioned "authority records" limitations.

d. "a master authority record"

Claim 1 recites "the secure data partition contains a master authority record," and "wherein the one or more authority records can be created and deleted as required by a user having access permissions according to the *master authority record*." Ex. 1001, 12:63−67 (emphasis added). Claim 13 depends from claim 12 and further recites that "the one or more authority records comprises *a master authority record* including instructions for governing the one or more authority records in said storage device." *Id*. at 14:27−30 (emphasis added).

Petitioner asserts that Hamlin, in combination with Fisherman and the knowledge of an ordinarily skilled artisan, teaches the aforementioned "master authority record" limitations. Pet. 30−31, 40−41, 44−47. Petitioner explains that Fisherman discloses a "supervisor" user who performs privileged operations. *Id*. at 30 (citing Ex. 1005, 1:60−61 ("file-access criteria [are] established by the supervisor"), 10:19−20 ("system 20 should be installed by the supervisor")). Petitioner contends that the supervisor's name and password discloses a "master authority record." *Id*. According to Petitioner, Fisherman's supervisor can create and delete user's associated data (authority records), executing a command that "pertains to the registration of a new user, the deletion of a user, or a change in file status." *Id.* at 31, 41 (citing Ex. 1005, 14:37−57 ("the new user registration command"), 14:66−15:11 ("a delete user command"), 15:20−24).

Petitioner asserts that it would have been obvious to include Fisherman's supervisor features in Hamlin by including a master authority record in Hamlin's pristine area to create and delete authority records. *Id.* at 27−31, 45−47. Dr. Levy testifies that one of ordinary skill in the art would have understood that a master authority record, when implemented in Hamlin, would have been implemented in the pristine area (the secure data partition) because the authentication information (authority record) is already disclosed in Hamlin as being stored in the pristine area. Ex. 1003 ¶¶ 132−133 (citing Ex. 1004, 5:61−62). Dr. Levy also testifies that such an artisan would have been motivated to store the master authority record in the

pristine area because the purpose of the pristine area is to keep the data secure. *Id.* (citing Ex. 1004, 1:27−30).

Dr. Levy also testifies that adding a master authority record for a system administrator/supervisor in Hamlin's pristine area "would provide the benefits of allowing easy configuration and customization of the drive—enabling the administrator (supervisor) of the computer system to ensure that information about users and devices authorized to access Hamlin's pristine area are up-to-date." *Id.* ¶ 225. The combination would allow "only authorized employees or members [to] have access to critical or sensitive information," and as "employees and members join, leave, or become more or less trusted, the administrator must update the list of users and their credentials accordingly." *Id.*

Based on the evidence in the entire trial record, we determine that Petitioner has demonstrated sufficiently that the combination of Hamlin, Fisherman, and the knowledge of an ordinary skilled artisan teaches the aforementioned "master authority record" limitations.

Patent Owner opposes, advancing several arguments. PO Resp. 42−45. First, Patent Owner argues Hamlin does not disclose a master authority record because Hamlin does not disclose authority records or creating and deleting authority records, relying on the same arguments for the "authority records" limitations. *Id.* at 42−43; Sur-reply 23−27.

However, as discussed above, Hamlin alone, or in view of Fisherman, discloses the "authority records" limitations. We have addressed those

arguments in our analysis and find them unavailing here for the reasons stated above.

In addition, attacking Hamlin individually does not undermine Petitioner's obviousness showing that is based on Hamlin, Fisherman, and the knowledge of an ordinarily skilled artisan. *See Keller*, 642 F.2d at 426. As discussed above, Fisherman discloses a master authority record (the supervisor's name and password), and the supervisor governs (e.g., adds and deletes) other user records. Ex. 1005, 14:37−57, 14:66−15:11, 15:20−24. Therefore, Patent Owner's argument that Hamlin does not disclose a master authority record is misplaced.

Second, Patent Owner argues that Petitioner improperly mixes the prior art invention described in Fisherman's background section, with Fisherman's invention, and that Fisherman "criticizes the prior art." PO Resp. 43−45 (citing Ex. 1005, 2:5−15).

We disagree, however. Petitioner merely shows that the features of a system administrator (supervisor) in a multi-user environment were known in the art at the time of the invention, as evidenced by Fisherman's background section and Fisherman's invention. *See* Pet. 30, 45; Reply 17; Ex. 1003 ¶ 86. Patent Owner does not dispute that such features of a system administrator (supervisor) were known in the art at the time of the invention. *See generally* PO Resp.; Sur-reply. "A reference must be considered for everything that it teaches, not simply the described invention or a preferred embodiment." *In re Applied Materials, Inc.*, 692 F.3d 1289, 1298 (Fed. Cir.

2012) (citing *EWP Corp. v. Reliance Universal Inc.*, 755 F.2d 898, 907 (Fed. Cir. 1985)).

We understand Patent Owner's "criticizes the prior art" argument to be a teaching away argument. Fisherman's invention does not teach away from these system administrator/supervisor features. *See generally* Ex. 1005. The portion of Fisherman cited by Patent Owner is not directly related to the supervisor, but instead addresses the prior art "subsystem" that Fisherman's invention sought to improve. Ex. 1005, 2:4−15 ("An obvious disadvantage of the above-described *subsystem* is . . . ." (emphasis added)). Additionally, the existence of better alternatives "does not mean that an inferior combination is inapt for obviousness purposes." *Mouttet*, 686 F.3d at 1334 (citing *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994)). Therefore, Patent Owner's argument that Petitioner improperly mixes different inventions and that Fisherman "criticizes the prior art" is misplaced.

Third, Patent Owner argues that Fisherman is a host-based system, not a storage device-based system. PO Resp. 43. However, Patent Owner fails to consider the combination as a whole, attacking Fisherman individually. *See Merck*, 800 F.2d at 1097; *Keller*, 642 F.2d at 426. Significantly, Hamlin is a device-based system, and the combination of adding Fisherman's supervisor features to Hamlin would be a device-based system. Pet. 44−47; Ex. 1003 ¶ 93; Reply 17. Thus, Patent Owner's argument that Fisherman is a host-based system is inapposite.

Fourth, Patent Owner argues that Fisherman does not disclose storing master authority records in a secure partition and creating and deleting authority records. PO Resp. 43−44.

Again, Patent Owner fails to consider the combination as a whole, attacking Fisherman's teachings individually. *See Merck*, 800 F.2d at 1097; *Keller*, 642 F.2d at 426. As Dr. Levy testifies, the supervisor's name and password in Fisherman discloses a master authority record because "[t]he supervisor name and password are placed in the first element of the USER_LIST," and the supervisor governs other user records by adding and deleting users or by altering file parameters related to a user's access permissions. Ex. 1003 ¶¶ 88, 132−136 (citing Ex. 1005, 10:19−24, 14:37−57).

Dr. Levy also testifies that one of ordinary skill in the art "would have understood that a master authority record, when implemented in Hamlin, would be implemented in the secure data partition" because Hamlin's user/device authentication information (authority records) is already stored in the pristine area (the secure data partition) of the disk. *Id*. ¶ 133 (citing Ex. 1004, 5:61−62). Dr. Levy further testifies that such an artisan would have been motivated to put the master authority record in the pristine area for keeping the data secure. *Id*. (citing Ex. 1004, 1:27−30). According to Dr. Levy, "[i]t is even more important to keep the master authority record secure because it may authorize the creating and deleting of other authority records." *Id*. Dr. Levy explains that "when implementing a Fisherman-style supervisor user name and password record in Hamlin, the supervisor

authority record would be implemented in Hamlin's existing dataset of authentication information, which resides in Hamlin's pristine area (the secure partition)." *Id*. ¶¶ 125−127, 133.

Based on the evidence of record, we determine that Petitioner has shown sufficiently that Hamlin in view of Fisherman teaches the aforementioned "master authority record" limitations. Patent Owner's argument that Fisherman does not disclose storing master authority records in a security partition, and creating and deleting authority records, is unavailing.

Finally, Patent Owner argues that the Board has held that Hamlin III does not disclose storing the master authority record in a security partition in IPR2019-00494. PO Resp. 44 (citing IPR2019-00494, Paper 8, 9 (Decision Denying Institution)).

Patent Owner's argument is inapposite. The asserted grounds and evidentiary record in the instant proceeding are different than those in IPR2019-00494. Notably, in the instant proceeding, Petitioner relies upon Hamlin and Fisherman, not Hamlin III, to teach the "master authority record" limitations. Pet. 30−31, 40−41, 44−47. Neither Hamlin nor Fisherman was asserted in IPR2019-00494. IPR2019-00494, Paper 8 at 3. More importantly, as discussed above, we determine that Petitioner has shown sufficiently that Hamlin in view of Fisherman teaches the "master authority record" limitations. Therefore, Patent Owner's argument that the Board has held that Hamlin III does not disclose storing the mater authority record in a security partition in IPR2019-00494 is inapposite.

For the foregoing reasons, we conclude that Petitioner has shown sufficiently that Hamlin in view of Fisherman teaches the aforementioned "master authority record" limitations recited in claims 1 and 13.

e. Reasons to combine Hamlin with Fisherman

Petitioner's arguments

Petitioner asserts that a person of ordinary skill in the art would have been motivated to implement Fisherman's flexible access permissions and supervisor features in Hamlin's pristine area because the combination would have achieved known benefits, such as increased security and more flexible security policies in Hamlin's multi-user environment. Pet. 45−47. In addition, Petitioner avers that such an artisan would have had a reasonable expectation of success to implement those features in Hamlin's disk drive because the combination merely involves adding an access field and a master authority record in Hamlin's preexisting data structure with routine modification to Hamlin's firmware. *Id.*; Ex. 1003 ¶¶ 223−232.

In support of Petitioner's arguments, Dr. Levy testifies that adding an access field in Hamlin's authentication information (authority records) "allow[s] the Hamlin invention to establish tiers of trust and enforce different access policies depending on the user's trust tier." Ex. 1003 ¶ 227. As Dr. Levy explains, "highly trusted users may be allowed to read and write to the pristine area, whereas a less-trusted user may be given only read access to ensure no data is tampered with, and entirely untrusted users could be barred access." *Id.* Dr. Levy also testifies that adding a master authority record for a system administrator/supervisor in Hamlin's pristine area

"would provide the benefits of allowing easy configuration and customization of the drive—enabling the administrator (supervisor) of the computer system to ensure that information about users and devices authorized to access Hamlin's pristine area are up-to-date." *Id.* ¶ 225. The combination would allow "only authorized employees or members have access to critical or sensitive information," and as "employees and members join, leave, or become more or less trusted, the administrator must update the list of users and their credentials accordingly." *Id.*

Dr. Levy also testifies that one of ordinary skill in the art "would have understood that a master authority record, when implemented in Hamlin, would be implemented in the secure data partition" because Hamlin's user/device authentication information (authority records) is already stored in the pristine area (the secure data partition) of the disk. *Id*. ¶ 133 (citing Ex. 1004, 5:61−62). Dr. Levy further testifies that such an artisan would have been motivated to put the master authority record in the pristine area for keeping the data secure. *Id*. (citing Ex. 1004, 1:27−30). According to Dr. Levy, "[i]t is even more important to keep the master authority record secure because it may authorize the creating and deleting of other authority records." *Id*. Dr. Levy explains that "when implementing a Fisherman-style supervisor user name and password record in Hamlin, the supervisor authority record would be implemented in Hamlin's existing dataset of authentication information, which resides in Hamlin's pristine area (the secure partition)." *Id*. ¶¶ 125−127, 133.

Based on the evidence in the entire trial record, we determine that Petitioner has articulated sufficient reasons to combine Fisherman's flexible access permissions and supervisory features in Hamlin's disk drive.

Patent Owner's incompatibility arguments

Patent Owner opposes, advancing several arguments. We address below each of Patent Owner's arguments in turn.

First, Patent Owner argues that a person of ordinary skill in the art would not have been motivated to combine Hamlin with Fisherman because Fisherman's host-based implementation is incompatible with Hamlin's device-based implementation and "Fisherman's operating system and file system dependent software is different from and incompatible with Hamlin's operating system independence and file system independence," citing Mr. Jawadi's testimony for support. PO Resp. 37−40, 47−61; Sur-reply 21−23; Ex. 2008 ¶¶ 185−187.

However, Patent Owner's argument and Mr. Jawadi's testimony incorrectly rest on the premise that the combination "would have required porting host-based hardware and host-based software to the disk drive." PO Resp. 48; Ex. 2008 ¶ 186. Again, Patent Owner and Mr. Jawadi narrowly focus on the physical differences between the storage systems disclosed in the references and require bodily incorporating Fisherman's system into Hamlin's disk drive. "It is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements." *Mouttet*, 686 F.3d at 1332.

Notably, the combination does not rely on incorporating Fisherman's hardware or software into Hamlin's disk drive. Rather, the combination merely implements an access field in Hamlin's authentication information (authority record) and adds a master authority record for a supervisor user. Pet. 45−47; Ex. 1003 ¶¶ 223−232; Ex. 1021 ¶¶ 92−96.

Petitioner makes clear that the combination maintains Hamlin's pre-existing data structures and firmware. Pet. 45−47; Ex. 1003 ¶ 232; Reply 21; Ex. 1021 ¶ 94. Dr. Levy testifies that "[i]n implementing the supervisor user and the flexible access permissions, no alternations to Hamlin's structure or general organization would be required by these changes" because "the organization of the 'user/device authentication information' already present in Hamlin." Ex. 1003 ¶ 232. Indeed, Hamlin's authentication information (authority records) is already stored in the pristine area (the secure data partition) of the disk. Ex. 1004, 5:61−62.

In addition, Dr. Levy testifies that "the ACCESS_FIELD and supervisor features in Fisherman are not specific to a host-based system, nor are they operating system dependent." Ex. 1021 ¶¶ 92−95; *see also* Ex. 1003 ¶¶ 224−230. Dr. Levy also testifies that "[a]dding an ACCESS_FIELD element (binary numbers) to the user/device authentication information in Hamlin does not transform Hamlin into a host-based system, and does not require Hamlin to be operating system dependent." Ex. 1021 ¶¶ 92−94.

More significantly, "if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would

improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill." *KSR*, 550 U.S. at 417. Here, as evidenced by Fisherman, the flexible access permissions and supervisor features were known in the art at the time of the invention (Ex. 1005, 1:7−11, 8:46−60, 10:19−24, 14:37−57, 14:66−15:11), and Patent Owner does not dispute that. *See generally* PO Resp.; Sur-reply. The evidence of record also shows that adding an access field and a master authority record for a supervisor in the pristine area of Hamlin's storage device is not beyond the skill of a pertinent artisan.

Notably, Dr. Levy testifies that Fisherman's access field "feature would have been easily implemented in Hamlin because a POSITA merely needed to add an additional field, which is two bits in size, to the user/device authentication information in Hamlin." Ex. 1021 ¶ 74; Ex. 1003 ¶ 230. Indeed, Mr. Jawadi admits that Fisherman's access field is two binary numbers and that "a bit in a *device-based* system could be used to determine whether a block is readable or not" and "*that's a very basic construct in computing* in general." Ex. 1022, 64:16−18, 79:10−14, 80:7−10 (emphases added). As Dr. Levy also explains, "read/write access rights, such as implemented in ACCESS_FIELD, had already been used in storage-device based systems" before the filing date of the '020 patent. Ex. 1021 ¶ 94. For example, Moran (U.S. Patent No. 6,324,537 B1, filed on September 30, 1999) discloses access control features that are "integrated with the hardware of the storage device," incorporating multiple read/write access rights. *Id.* (citing Ex. 1039, 2:1−16, 6:12−15, 6:55−59).

In addition, Dr. Levy testifies that implementing the supervisor features "would be straightforward because a POSITA would only need to designate the user that has the lowest 'entity ID' value as the supervisor and give the supervisor permission to add and delete other entities." Ex. 1003 ¶¶ 224−225, 229; Ex. 1021 ¶ 93. Dr. Levy explains that "adding a supervisor user in Hamlin's device does not change Hamlin's storage system structure (it only adds another Hamlin authority record for the supervisor user who has permission to create and delete other authority records), and does not transform Hamlin into a host-based system." Ex. 1021 ¶¶ 93−95. We credit Dr. Levy's testimony (e.g., Ex. 1003 ¶¶ 223−232; Ex. 1021 ¶¶ 92−96) because it is consistent with the prior art disclosures and other evidence of record (e.g., Exs. 1004, 1005, 1039).

Furthermore, as Petitioner explains, implementing an access field and a master authority record for a supervisor would achieve known benefits, such as increased security and more flexible security policies in Hamlin's multi-user environment in that it would allow multi-tiers of trust to enforce difference access policies and allow a system administrator to maintain an up-to-date list of authorized users and access permissions. Pet. 45−47. Dr. Levy testifies that adding an access field in Hamlin's authentication information (authority records) "allow[s] the Hamlin invention to establish tiers of trust and enforce different access policies depending on the user's trust tier." Ex. 1003 ¶ 227. For example, as Dr. Levy explains, "highly trusted users may be allowed to read and write to the pristine area, whereas a

less-trusted user may be given only read access to ensure no data is tampered with, and entirely untrusted users could be barred access." *Id.*

Dr. Levy also testifies that adding a master authority record for the administrator/supervisor in Hamlin's pristine area "would provide the benefits of allowing easy configuration and customization of the drive—enabling the administrator (supervisor) of the computer system to ensure that information about users and devices authorized to access Hamlin's pristine area are up-to-date." *Id.* ¶ 225. The combination would allow "only authorized employees or members have access to critical or sensitive information," as "employees and members join, leave, or become more or less trusted, the administrator must update the list of users and their credentials accordingly." *Id.*

As the Supreme Court has held, "when a patent 'simply arranges old elements with each performing the same function it had been known to perform' and yields no more than one would expect from such an arrangement, the combination is obvious." *KSR*, 550 U.S. at 418 (*quoting Sakraida v. Ag Pro, Inc.*, 425 U.S. 273, 282 (1976)).

For the foregoing reasons, we determine that Petitioner has articulated sufficient reasons to combine Hamlin with Fisherman. We are not convinced by Patent Owner's arguments and Mr. Jawadi's testimony that Fisherman's host-based implementation is incompatible with Hamlin's device-based implementation and "Fisherman's operating system and file system dependent software is different from and incompatible with Hamlin's

operating system independence and file system independence." PO Resp. 37−40, 47−61; Sur-reply 21−23; Ex. 2008 ¶¶ 185−187.

To the extent that Patent Owner is arguing that one of ordinary skill in the art would not have considered combining Hamlin with Fisherman because Fisherman and Hamlin are not analogous art, we do not agree.

Prior art is analogous and can be applied in an obviousness combination if it either (1) "is from the same field of endeavor, regardless of the problem addressed" or (2) "is reasonably pertinent to the particular problem with which the inventor is involved." *In re Clay*, 966 F.2d 656, 658−59 (Fed. Cir. 1992). A reference is analogous if either of these two tests is met. *Scientific Plastic Prods., Inc. v. Biotage AB*, 766 F.3d 1355, 1359 (Fed. Cir. 2014). The U.S. Court of Appeals for the Federal Circuit has indicated that the scope of analogous art should be construed broadly. *Wyers v. Master Lock Co.*, 616 F.3d 1231, 1238 (Fed. Cir. 2010) ("The Supreme Court's decision in *KSR* . . . directs us to construe the scope of analogous art broadly . . . .").

Here, the '020 patent broadly defines its "Field of the Invention," stating that "[t]he present invention generally relates to methods and systems for *securing computer systems*" and "more particularly relates to methods and devices for *securing information in a computer system* wherein the computer system may be connected to a networked environment." Ex. 1001, 1:7−14 (emphases added). The field of endeavor of the '020 patent is not limited to device-based implementation or file system independence, as Patent Owner suggests. PO Resp. 36−42, 47−61; Ex. 2008 ¶¶ 185−229;

Sur-reply 17−23. As our reviewing court has held, "[t]he field of endeavor of a patent is not limited to the specific point of novelty, the narrowest possible conception of the field, or the particular focus within a given field." *Unwired Planet, LLC v. Google Inc.*, 841 F.3d 995, 1001 (Fed. Cir. 2016). Hence, the field of endeavor of the '020 patent encompasses "methods and devices for securing information in a computer system." Ex. 1001, 1:7−14.

Significantly, both Hamlin and Fisherman disclose methods and systems for securing information in a computer system. Ex. 1004, code 54, 1:26−30 (disclosing a "[d]isk drive employing a disk with a pristine area for storing encrypted data accessible only by trusted devices") 2:49−3:49; Ex. 1005, code 57, 1:7−11, 2:30−44 (disclosing that the "objects of the instant invention are achieved by providing a hard disk protection system for protecting data stored on a hard disk of a personal computer"); Ex. 1003 ¶¶ 220−222. As such, Hamlin, Fisherman, and the '020 patent are within the same field of endeavor that encompasses "methods and devices for securing information in a computer system." Ex. 1001, 1:7−14. Accordingly, Hamlin and Fisherman are analogous prior art to the '020 patent.

<u>Patent Owner's argument regarding Petitioner's reliance on host based and file system dependent features</u>

Second, Patent Owner argues that Petitioner relies on features in Fisherman that are "host based and file system dependent." PO Resp. 60−61 (citing Ex. 2008 ¶¶ 225−229; Ex. 1005, 5:63−64, 5:64−6:9, 8:20−9:22). According to Patent Owner, Fisherman's service data are in the host computer and are dependent on the operating file, and Fisherman's

description of the service area shows that the fields are specific to the file system, files, directories, and clusters. *Id.*

However, as discussed above, Petitioner makes clear that the combination would store the authority records, including the access field and the master authority record, in the pristine area of Hamlin's disk (not in a host system), and use the authority records to apply permissions to the blocks in Hamlin's disk, not clusters. Pet. 46−47; Ex. 1003 ¶¶ 125−129, 133, 232; Reply 21−22; Ex. 1021 ¶¶ 78−79. Petitioner explains that "Fisherman simply implements these features within its architecture, and these features are equally applicable and useful in Hamlin's device." Reply 22; Ex. 1021 ¶ 94.

Indeed, Dr. Levy testifies that "[i]n implementing the supervisor user and the flexible access permissions, no alternations to Hamlin's structure or general organization would be required by these changes," and Fisherman's access field and supervisor features are equally applicable and useful in device-based systems. Ex. 1003 ¶¶ 133, 232; Ex. 1021 ¶ 94. Dr. Levy also testifies that an ordinarily skilled artisan "merely needed to add an additional field, which is two bits in size, to the user/device authentication information in Hamlin." Ex. 1021 ¶ 74; Ex. 1003 ¶ 230. Moreover, Mr. Jawadi admits that Fisherman's access field is two binary numbers and that "a bit in a *device-based* system could be used to determine whether a block is readable or not" and "*that's a very basic construct in computing* in general." Ex. 1022, 64:16−18, 79:10−14, 80:7−10 (emphases added).

Dr. Levy further testifies that "adding a supervisor user in Hamlin's device does not change Hamlin's storage system structure (it only adds another Hamlin authority record for the supervisor user who has permission to create and delete other authority records), and does not transform Hamlin into a host-based system." Ex. 1021 ¶¶ 93−95.

Based on the evidence in this entire trial record, we are not convinced by Patent Owner's argument that Petitioner relies on features that are "host based and file system dependent." PO Resp. 60−61.

Patent Owner's teaching away arguments

Third, Patent Owner argues that "a POSITA would not be motivated to combine Hamlin and Fisherman to arrive at the '020 Patent because all three teach away from such combination." Sur-reply 21−23; *see also* PO Resp. 47−54. To support its argument, Patent Owner avers that Hamlin and the '020 patent teach away from Fisherman and from any potential combination of a host-based system with a device-based system. Sur-reply 22 (citing Ex. 1004, 1:42−52, 2:16−21; Ex. 1001, 1:35−54, 10:67−11:3).

"A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant." *Gurley*, 27 F.3d at 553. Thus, the "mere disclosure of alternative designs does not teach away." *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004). Furthermore, just because better alternatives exist in the prior art does not mean that an inferior combination is inapt for obviousness purposes. *Gurley*, 27 F.3d at 553.

Patent Owner's theory of teaching away is misplaced. Again, Patent Owner's arguments and Mr. Jawadi's testimony incorrectly rest on the premise that the combination "would have required porting host-based hardware and host-based software to the disk drive." PO Resp. 48; Ex. 2008 ¶ 186. As discussed above, Petitioner makes clear that the combination maintains Hamlin's pre-existing data structures and firmware. Pet. 45−47; Ex. 1003 ¶¶ 125−129, 133, 232; Reply 21; Ex. 1021 ¶ 94.

For data security, Hamlin stores the authentication information (authority records) in the pristine area (the secure data partition) of a disk. Ex. 1004, 1:26−30, 4:65−5:1, 5:50−63, 6:4−8, 7:55−60, 8:12−15. Hamlin's authentication circuitry uses the authentication information to authorize or deny access (read/write permissions) to the secure data or information stored in the pristine area. *Id*. at 4:61−5:12, 5:58−6:12, 7:38−43, 7:50−59.

To prevent unauthorized access to data stored on a disk, Fisherman discloses a way to implement: (1) flexible access permissions by adding an access field, and (2) features for a supervisor user to have access permissions to create and delete authority records. Ex. 1005, 1:7−11, 8:46−60, 10:19−24, 14:37−57, 14:66−15:11. As Dr. Levy testifies, "the ACCESS_FIELD and supervisor features in Fisherman are not specific to a host-based system, nor are they operating system dependent." Ex. 1021 ¶¶ 92−95; *see also* Ex. 1003 ¶¶ 224−230. Dr. Levy also testifies that "[a]dding an ACCESS_FIELD element (binary numbers) to the user/device authentication information in Hamlin does not transform Hamlin into a host-based system, and does not require Hamlin to be operating system

dependent." Ex. 1021 ¶¶ 92−94. Neither Hamlin nor the '020 patent discourages an ordinarily skilled artisan from implementing flexible access permissions or supervisor features in a device-based system, or to lead such an artisan in a direction divergent from the path taken by Applicant. Ex. 1001; Ex. 1004.

In short, Patent Owner's argument that Hamlin, Fisherman, and the '020 patent teach away from the combination of Hamlin, Fisherman, and the knowledge of an ordinarily skilled artisan is unavailing.

Patent Owner's arguments regarding Dr. Levy's Testimony

Lastly, Patent Owner argues that "Dr. Levy's discussion completely omits any reference to *the time of the invention* and utterly fails to explain why a POSITA at that particular point in time would have been motivated to make such a combination." PO Resp. 46−47; Sur-reply 17−19. Patent Owner also argues that Dr. Levy "does not discuss any consumer demand for such an invention at *the time of the invention*," "the state of the industry or the state of that particular market *at the time of the invention*," or "why a POSITA with knowledge of Hamlin would have been motivated to combine Fisherman *at the time of the invention*." PO Resp. 46.

Patent Owner's arguments are misplaced. There is no requirement that an expert has to repeat the phrase "at the time of the invention" in each sentence. Dr. Levy's Declarations, as a whole, show that his opinions and analysis are from the perspective of a person of ordinary skill in the art at the time of the invention.

Significantly, Dr. Levy states repeatedly that his analysis was done from the perspective of a person of ordinary skill in the art at the time of the invention. *See, e.g.*, Ex. 1003 ¶¶ 21, 22, 24, 28, 51, 116, 112. Indeed, Dr. Levy expressly testifies that his "opinions and analysis set forth in [his] Opening Declaration are from the perspective of a POSITA *at the time of the alleged invention*, which [he] understood to be no earlier than July 25, 2001, including [his] analysis of the patent claims, prior art references, motivations to combine the prior art references, and reasonable expectation of success in combining the references." Ex. 1021 ¶ 5 (emphasis). Dr. Levy also testifies in his Opening Declaration that "[his] opinions are given from the perspective of a POSITA *at the time of the July 25, 2001*, filing of the application that became the '020 Patent," and that "[his] analysis and conclusions herein are from the perspective of a POSITA *as of July 25, 2001*." Ex. 1003 ¶¶ 22, 24 (emphases added).

Dr. Levy further testifies that "[i]n providing [his] opinions in this declaration, [he] was asked to consider the patent claims and the prior art standing in the shoes of a person of ordinary skill in the art ("POSITA") *at the time of the alleged invention*" and that "[he] understand[s] that common factors considered in determining the ordinary level of skill in a field of art include the level of education and experience of persons working in the field, the types of problems encountered in the field, and the sophistication of the technology *at the time of the invention*." *Id.* ¶ 21 (emphases added).

More importantly, Dr. Levy also cites to supporting evidence that is contemporaneous with, or predates, the '020 patent. Notably, Dr. Levy

testifies that "[i]n forming [his] opinions and reaching the conclusion given in this declaration, [he] relied on the documents and materials cited in this declaration as well as those identified in Appendix A" of his Declaration. *Id.* ¶ 19. Apart from Exhibit 1001 that contains a copy of the '020 patent, the documents and materials cited in Dr. Levy's Declarations and those identified in Appendix A predate the filing of the '020 patent. *See generally* Ex. 1003; Ex. 1021; Ex. 1003 at 168−169 (Appendix A).

Moreover, as discussed in our analysis above, we credit Dr. Levy's testimony because it is supported by the Specification, prior art, and other evidence of record (e.g., Exs. 1001, 1004−1013, 1016, 1017, 1038, 1039). It is within the Board's discretion to assign appropriate weight to evidence. *See e.g.*, *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1368 (Fed. Cir. 2004); *Velander v. Garner*, 348 F.3d 1359, 1371 (Fed. Cir. 2003) ("It is within the discretion of the trier of fact to give each item of evidence such weight as it feels appropriate.").

Upon consideration of the evidence of record, we are not convinced by Patent Owner's argument that Dr. Levy's discussion fails to offer a perspective of a person of ordinary skill in the art at the time of the invention and fails to explain why such an artisan at that particular point in time would have been motivated to make such a combination.

f. Conclusion on claims 1, 12, and 13

In sum, Petitioner has demonstrated adequately that the combination of Hamlin, Fisherman, and the knowledge of an ordinarily skill artisan teaches all of the limitations recited in claims 1,

12, and 13, and has articulated sufficient reasons to combine the prior art teachings. We determine that Petitioner has established by a preponderance of the evidence that claims 1, 12, and 13 are unpatentable under § 103(a) as obvious over Hamlin, in combination with Fisherman and the knowledge of an ordinarily skill artisan.

2. Claims 2, 3, 5, and 14

Claims 2, 3, and 5 depend from claim 1, and claim 14 depends from claim 12. Petitioner has accounted for the limitations recited in each of these dependent claims. Pet. 33−36, 42−47. For these claims, Patent Owner relies upon the same arguments presented for claim 1, and does not make any additional arguments. PO Resp. 23−61. We already addressed those arguments in our analysis above, and we find those arguments unavailing here for the reasons stated above.

Upon consideration of the evidence in this entire record, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 2, 3, 5, and 14 are unpatentable under § 103(a) as obvious over Hamlin, in combination with Fisherman and the knowledge of an ordinarily skill artisan.

For example, as to claim 2, which recites "wherein the storage device is in communication with a computer system having an operating system," Petitioner asserts that Hamlin discloses that its invention is to "improve security . . . with respect to probing attacks and virus attacks on computer operating systems." Pet. 33−34 (citing Ex. 1004, 2:43−45, 7:39−42, Figs. 1−3). Petitioner points out that Hamlin's disk drive is in

communication with and "receives requests from . . . a host or client computer," which would run such an operating system. *Id.* (citing Ex. 1004, 4:61−63, 7:39−42, Figs. 1−3). Petitioner further contends that Hamlin claims a "disk drive comprising: . . . a control system for interfacing with a host computer." *Id.* (citing Ex. 1004, 8:56−64, 9:1−3, 9:55−61, 10:55−63, 11:1−4, 12:1−6). Based on the evidence before us, we determine that Petitioner has shown sufficiently that claim 2 is obvious over Hamlin in view of Fisherman and the knowledge of an ordinarily skill artisan.

For claim 3, which recites "wherein secure data stored in the secure data partition is invisible to the operating system," Petitioner asserts that Hamlin's "pristine area 8 comprises at least one physical block" that is "not externally accessible through a logical block address during normal operation of the disk drive 2," and such blocks are "not mapped from logical block addresses." Pet. 34−35 (citing Ex. 1004, 7:67−8:4, 8:19−25). Dr. Levy testifies that this disclosure indicates that at least one block of the pristine area is invisible to the operating system. Ex. 1003 ¶¶ 143−144.

Alternatively, Petitioner asserts that Fisherman discloses that each of its logical drives is broken into several zones, including a HiddenZone where "the disk space occupied by this zone is excluded from the disk space accessible to the operating system." Pet. 34−35 (citing Ex. 1005, 5:7−11, 5:38−45). Dr. Levy testifies that making the HiddenZone inaccessible to the operating system renders it invisible. Ex. 1003 ¶ 145.

Petitioner asserts that a person of ordinary skill in the art would have been motivated to implement Fisherman's invisible partition teaching in

Hamlin's pristine area of the disk because "Fisherman's teaching of a partition that is invisible to the operating system would further improve the security of Hamlin's invention" as "it is much harder for a compromised operating system to access it." Pet. 47; Ex. 1003 ¶¶ 233−237. Dr. Levy testifies that such an artisan "would have had a reasonable expectation of success in making this combination" because "implementation of this feature in Hamlin requires no large changes to Hamlin, and indeed only requires updates to Hamlin's firmware that would have been well understood by a POSITA." Ex. 1003 ¶ 237. Dr. Levy also testifies that "the implementation would have provided the predictable result of rendering the pristine area of Hamlin invisible to the operating system." *Id.*

Based on the evidence of record, we determine that Petitioner has shown sufficiently that claim 3 is obvious over Hamlin in view of Fisherman and the knowledge of an ordinarily skill artisan.

As to claim 5, which recites "wherein the storage device further comprises: cryptographic operations embedded in the firmware of the storage device," Petitioner asserts that Hamlin discloses that information "may be encrypted by the disk drive 2 before it is written to the pristine area 8" and authentication circuitry 14 performs cryptographic operations, such as generating a message authentication code using a hashing function. Pet. 35−36 (citing Ex. 1004, 7:10−27, 7:42−44; Ex. 1003 ¶¶ 152−154). Petitioner contends that Hamlin discloses using firmware on a processor to implement the control system and authentication circuitry of the disk drive

(as discussed above in its analysis for claim 1), and therefore firmware includes these cryptographic operations. *Id.*; Ex. 1003 ¶¶ 152−154.

Based on the evidence of record, we determine that Petitioner has shown sufficiently that claim 5 is obvious over Hamlin in view of Fisherman and the knowledge of an ordinarily skill artisan.

Claim 14 requires each authority records to include a plurality of fields and "a first field of the plurality of fields contains access rights governing access to the at least one data set." As discussed above, Petitioner has shown sufficiently that Hamlin in view of Fisherman teaches a plurality of fields in each authority record, including Fisherman's access field that has two subfields to represent read and write rights. Ex. 1005, 8:46−60. Dr. Levy testifies that it is clear from Fisherman's disclosure that the access field is a first field of the plurality of fields and it contains access rights. Ex. 1003 ¶ 217 (citing Ex. 1005, 8:20−26, 8:46−60, 9:7−17).

Based on the evidence of record, we determine that Petitioner has shown sufficiently that claim 14 is obvious over Hamlin in view of Fisherman and the knowledge of an ordinarily skill artisan.

For the foregoing reasons, we determine that Petitioner has established by a preponderance of the evidence that claims 2, 3, 5, and 14 are unpatentable under § 103(a) as obvious over Hamlin, in combination with Fisherman and the knowledge of an ordinarily skill artisan.

3. Conclusion on Ground 1

In short, we determine that Petitioner has established by a preponderance of the evidence that claims 1−3, 5, and 12−14 are unpatentable under § 103(a) as obvious over Hamlin, in combination with Fisherman and the knowledge of an ordinarily skill artisan.

F. Ground 2: Hamlin, Fisherman, Silvester, and the knowledge of an ordinarily skilled artisan

Petitioner asserts that claims 3 and 11 are unpatentable under § 103(a) as obvious over Hamlin, in combination with Fisherman, Silvester, and the knowledge of an ordinarily skilled artisan, citing Dr. Levy's Declaration for support. Pet. 48–54; Ex. 1003.

Patent Owner relies upon its arguments in connection with claim 1. PO Resp. 45−46. We already addressed those arguments in our analysis above, and find those arguments unavailing here for the same reasons stated above. In addition, as discussed above, we also determine that Petitioner has shown by a preponderance of the evidence that claim 3 is unpatentable under § 103(a) as obvious over Hamlin in view of Fisherman and the knowledge of an ordinarily skill artisan.

As to dependent claim 11, which depends on claim 1 and further recites "wherein the secure data is accessed by the firmware using a security partition open call internal to the storage device and hidden from a user," Petitioner asserts that Silvester discloses that "operations . . . relating to opening, accessing and closing of the [secure-private partition] 420 are carried out in part by the IDE controller 410 which works in harmony with

the disk controller 418 on the hard drive 416." Pet. 49 (citing Ex. 1006, 3:3−7, 4:44−46, Fig. 4). Petitioner explains that "[t]he open operation would be carried out internal to the storage device because the disk controller (in harmony with the IDE controller) is internal to the hard disk drive." *Id*. at 50 (citing Ex. 1006, 2:61−64, 3:3−7, Fig. 4).

Petitioner contends that a person of ordinary skill in the art "integrating the open call from Silvester into Hamlin would have necessarily implemented it internal to Hamlin's drive." Pet. 51, 53−54. Petitioner articulates that such an artisan "would have been further motivated to combine Silvester with Hamlin and Fisherman because integrating Silvester's disclosures of opening (unlocking) and closing (locking) a partition into Hamlin would have increased the efficiency and security of Hamlin." *Id*.; Ex. 1003 ¶¶ 251−555.

Based on the evidence of record, we determine that Petitioner has shown sufficiently that Hamlin, in combination with Fisherman, Silvester, and the knowledge of an ordinarily skilled artisan, teaches the limitation recited in claim 11, and Petitioner has articulated an adequate reason to combine the prior art teachings.

For the reasons stated above, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 3 and 11 are unpatentable under § 103(a) as obvious over Hamlin, in combination with Fisherman, Silvester, and the knowledge of an ordinarily skill artisan.

G. Ground 3: Hamlin, Fisherman, Carter, and the knowledge of an ordinarily skilled artisan

Petitioner asserts that claim 4 is unpatentable under § 103(a) as obvious over Hamlin, in combination with Fisherman, Carter, and the knowledge of an ordinarily skilled artisan, citing Dr. Levy's Declaration for support. Pet. 55–60; Ex. 1003.

Patent Owner relies upon its arguments in connection with claim 1. PO Resp. 23. We already addressed those arguments in our analysis above, and find those arguments unavailing here for the same reasons stated above.

Claim 4 recites "wherein each of the one or more authority records contains one public-private key pair for authenticating data that originates from the security partition." Ex. 1001, 13:9−12. For this limitation, Petitioner asserts that each of Carter's user records in a soft-token store contains a certificate with a public key, a private key(s), and a digital signature created with the private key. Pet. 55 (citing Ex. 1007, 9:9−13, 9:59−62, Figs. 5−6 (reproduced above) (showing that the user record contains old certificate set 602, certificate with public key 604, digital signature 606, and private key set 608)).

Dr. Levy testifies that Carter discloses that the public-private key pair in the user record is used to authenticate data within the soft-token store because Carter provides a way to securely perform a transaction (updating confidential user data in the soft-token store) by authenticating the transaction with the public key in the certificate and the corresponding private key in the digital signature. Ex. 1003 ¶¶ 150, 259−264 (citing

Ex. 1007, 2:6−9, 19−23, 5:60−65, 6:16−35, 7:12−17, 9:9−67, 10:15−26, 13:9−13, 13:22−24). Dr. Levy further testifies that an ordinarily skilled artisan would have been motivated to combine Carter with Hamlin and Fisherman because Carter's teaching regarding key pairs would have provided a further layer of security to authenticate data in the pristine area in Hamlin. *Id.* ¶¶ 259−264.

Based on the evidence of record, we determine that Petitioner has shown sufficiently that Hamlin, in combination with Fisherman, Carter, and the knowledge of an ordinarily skilled artisan, teaches the limitation recited in claim 4, and articulated reasons to combine the prior art teachings.

For the reasons stated above, we determine that Petitioner has demonstrated by a preponderance of the evidence that claim 4 is unpatentable under § 103(a) as obvious over Hamlin, in combination with Fisherman, Carter, and the knowledge of an ordinarily skill artisan.

H. Ground 4: Hamlin, Fisherman, Mirov, and the knowledge of an ordinarily skilled artisan

Petitioner asserts that claims 6−10 are obvious over Hamlin, in combination with Fisherman, Mirov, and the knowledge of an ordinarily skilled artisan, citing Dr. Levy's Declaration for support. Pet. 60–75; Ex. 1003. Claim 6 depends from claim 5, which depends from claim 1. Claims 8−10 depend from claim 7.

For this ground, Patent Owner relies upon its arguments in connection with claim 1. PO Resp. 23. We already addressed those arguments in our

analysis above, and find those arguments unavailing here for the same reasons stated above.

In addition, Petitioner has accounted for the limitations recited in claims 6−10. Pet. 60−75. In its analysis regarding claims 6 and 7, Petitioner explains Hamlin's secure data is encrypted. *Id*. at 65 (citing Ex. 1004, 4:13−19). Petitioner also notes that Mirov's authentication of firmware is based on cryptography, and Mirov's authentication section 45 includes secured micro-code 51 (firmware), comparator 52, hash generator 53, decryptor 54, and public key 56. *Id*. at 60−61 (citing Ex. 1008, 2:4−20, 3:56−4:7). Petitioner further points out that secured micro-code 51 of authentication section 45 in Mirov performs cryptographic operations as part of authenticating programmable section 55. *Id*. (citing Ex. 1008, 4:8−25). Significantly, Petitioner explains that, once unsecured micro-code 58 in programmable section 55 is verified and raised to a level of trusted, other boot data can be similarly authenticated using trusted micro-code 58. *Id*. at 61 (citing Ex. 1008, 5:24−30). Petitioner further explains that Mirov's cryptographic code in micro-code 58 (firmware) is authenticated by the root assurance (secure micro-code 51) which forms a part of Mirov's firmware. Pet. 61; Ex. 1003 ¶ 158.

Dr. Levy testifies that a person of ordinary skill in the art would have been motivated to combine Mirov with Hamlin, Fisherman, and the knowledge of an ordinarily skilled artisan, because Mirov's mechanism to authenticate cryptographic code with a root authority would keep the critical firmware in Hamlin safe from corruption or malicious users and thus would

have improved the security of Hamlin. Ex. 1003 ¶ 268. Therefore, Hamlin's control system and authentication circuitry *in the disk drive*, as modified in view of Fisherman, Mirov, and the knowledge of an ordinarily skilled artisan, would include the features for authenticating cryptographic code with a root assurance.

Based on the evidence of record, we determine that Petitioner has shown sufficiently that Hamlin, in combination with Fisherman, Mirov, and the knowledge of an ordinarily skilled artisan, teaches the limitations recited in claims 6 and 7, and Petitioner has articulated an adequate reason to combine the prior art teachings.

As to claim 8, which recites "prohibiting access to the secure data partition by the operating system of the computer system," Petitioner asserts that, as explained in its analysis for claim 3, Hamlin discloses that at least one physical block of data in pristine area 8 is not externally accessible, and therefore, access by a computer operating system (external) to this data in pristine area 8 is prohibited. Pet. 66. Alternatively, Petitioner also asserts that Fisherman's invisible partition implemented in Hamlin's pristine area, as discussed in its analysis for claim 3, is inaccessible to the operating system. *Id.* at 66–67. Based on the evidence of record, we determine that Petitioner has shown sufficiently that claim 8 is obvious over Hamlin, in combination with Fisherman, Mirov, and the knowledge of an ordinarily skilled artisan.

With respect to claim 9, which recites "a portion of the firmware is non-writable," Petitioner asserts that, as evidence by Mirov, it was

well-known at the time of the invention that firmware can be non-writable. Pet. 67 (citing Ex. 1008, 3:55−4:7, Fig. 2). Petitioner argues that a person of ordinary skill in the art would have been motivated to combine Mirov's read-only firmware with Hamlin's pristine area to improve Hamlin's security by ensuring Hamlin's firmware safety. *Id.* at 74. Dr. Levy testifies that a disk drive may be "less susceptible to virus attacks" when the "firmware implemented by the disk controller" is "essentially static." Ex. 1003 ¶ 273 (citing Ex. 1010, 5:18−21). Based on the evidence of record, we determine that Petitioner has shown sufficiently that claim 9 is obvious over Hamlin, in combination with Fisherman, Mirov, and the knowledge of an ordinarily skilled artisan.

As to claim 10, which recites "writing data to the secure data partition by executing of a portion of the firmware of the storage device," Petitioner asserts that, as discussed in its analysis for claim 1, Hamlin's control system is implemented in firmware on a processor and the firmware writes data to the secure data partition. Pet. 68. Petitioner points out that Hamlin discloses that "during a write operation . . . preamplifier 20 receives digital write data 24 from the control system 12 which is to be written to the disk 4" and that "control system 12 'will access the pristine area'" for "a write or read operation." *Id.* (citing Ex. 1004, 4:28−38, 4:58−60; Ex. 1003 ¶¶ 186−188).

Based on the evidence of record, we determine that Petitioner has shown sufficiently that claim 10 is obvious over Hamlin, in combination with Fisherman, Mirov, and the knowledge of an ordinarily skilled artisan.

For the foregoing reasons, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 6−10 are unpatentable under § 103(a) as obvious over Hamlin, in combination with Fisherman, Mirov and the knowledge of an ordinarily skill artisan.

I. Ground 5: Hamlin, Fisherman, Mirov, Silvester, and the knowledge of an ordinarily skilled artisan

Petitioner asserts that claims 7−10 are obvious over Hamlin, in combination with Fisherman, Mirov, Silvester, and the knowledge of an ordinarily skilled artisan, citing Dr. Levy's Declaration for support. Pet. 75–77; Ex. 1003.

For this ground, Patent Owner relies upon its arguments in connection with claim 1. PO Resp. 23. We already addressed those arguments in our analysis above, and find those arguments unavailing here for the same reasons stated above. In addition, as discussed above, we also determine that Petitioner has shown by a preponderance of the evidence that claims 7−10 are unpatentable under § 103(a) as obvious over Hamlin in view of Fisherman, Mirov, and the knowledge of an ordinarily skill artisan.

Upon consideration of Petitioner's contentions and supporting evidence, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 7−10 are unpatentable under § 103(a) as obvious over Hamlin, in combination with Fisherman, Mirov, Silvester, and the knowledge of an ordinarily skill artisan.

III. CONCLUSION

For the foregoing reasons, we conclude that Petitioner has established by a preponderance of the evidence that claims 1−14 of the ’020 patent are unpatentable.

IV. ORDER[6]

For the foregoing reasons, it is

ORDERED that claims 1−14 of the ’020 patent have been shown to be 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.

In summary:

---

[6] 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).

Claim(s)	35 U.S.C. §	References	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1−3, 5, 12−14	103(a)	Hamlin, Fisherman, and the knowledge of an ordinarily skilled artisan	1−3, 5, 12−14	
3, 11	103(a)	Hamlin, Fisherman, Silvester, and the knowledge of an ordinarily skilled artisan	3, 11	
4	103(a)	Hamlin, Fisherman, Carter, and the knowledge of an ordinarily skilled artisan	4	
6−10	103(a)	Hamlin, Fisherman, Mirov, and the knowledge of an ordinarily skilled artisan	6−10	
7−10	103(a)	Hamlin, Fisherman, Mirov, Silvester, and the knowledge of an ordinarily skilled artisan	7−10	
Overall Outcome			1−14	

For PETITIONER:

Jeremy Jason Lang
ORRICK, HERRINGTON & SUTCLIFFE LLP
ptabdocketjjl2@orrick.com

Robert Perez
robert.perez@pillsburylaw.com

For PATENT OWNER:

Cabrach Connor
CONNOR KUDLAC LEE PLLC
cab@connorkudlaclee.com

Enrique Sanchez, Jr.,
WHITAKER CHALK SWINDLE & SCHWARTZ PLLC
rsanchez@whitakerchalk.com