UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

UNIFIED PATENTS INC.,
Petitioner

v.

SECUREWAVE STORAGE SOLUTIONS INC.,
Patent Owner

_____

Case No. IPR2019-00501
Patent No. 7,036,020

_____

PATENT OWNER'S NOTICE OF APPEAL

Pursuant to 35 U.S.C. §§ 141(c) and 319, the patent owner, SecureWave Storage Solutions Inc. ("SecureWave") hereby gives notice that it appeals to the United States Court of Appeals for the Federal Circuit from the Final Written Decision entered by the Patent Trial and Appeal Board on July 7, 2020 (Paper 31) and from all underlying orders, decisions, rulings and opinions. A copy of the Final Written Decision is attached to this notice of appeal.

This notice of appeal is timely filed within 63 days of that final written decision. *See* 37 C.F.R. § 90.3(a)(1).

In accordance with 37 C.F.R. § 90.2(a)(3)(ii), SecureWave indicates that the issues on appeal include the Board's determinations of unpatentability of claims 1–5 of U.S. Patent No. 7,036,020, including, for example, one or more of the following:

(1) The Board's determinations that claims 1–5 are unpatentable under 35 U.S.C. § 103 as obvious over Robb (U.S. Patent No. 6,931,503, Ex. 1007) in view of Jones (U.S. Patent No. 5,623,637, Ex. 1008) and further in view of Grawrock (U.S. Patent No. 6,081,893, Ex. 1009);

(2) the Board's explicit and implicit constructions of the language of claims 1–5, including, for example, "one or more authority records," "master authority record," "firmware for reading data from and writing data to the storage medium," "wherein only the firmware is permitted to access the

secure data and the one or more authority records," "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," "secure data partition contains a master authority record" and "wherein each of the one or more authority records contains one public-private key pair for authenticating data that originates from the security partition";

(3) the Board's findings that Robb, Jones, and/or Grawrock disclose or suggest the limitations of claims 1–5, including, for example, "one or more authority records," "master authority record," "firmware for reading data from and writing data to the storage medium," "wherein only the firmware is permitted to access the secure data and the one or more authority records," "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," "secure data partition contains a master authority record" and "wherein each of the one or more authority records contains one public-private key pair for authenticating data that originates from the security partition";

(4) the Board's finding that one of ordinary skill in the art would have combined the teachings of Robb, Jones, and Grawrock to arrive at the claimed invention; and

(5) the Board's failure to consider the testimony of Jay Jawadi, an expert witness who testified on behalf of SecureWave during the IPR trial.

SecureWave notes that the issues on appeal may also include (6) the Board's failure to address arguments made by SecureWave; (7) the Board's mischaracterization of SecureWave's arguments; (8) the Board's failure to explain adequately the basis for its decision; (9) the Board's improper assignment of the burden of proof on SecureWave; (10) the Board's failure to afford SecureWave its full due-process and other procedural rights guaranteed by the U.S. Constitution and/or the Administrative Procedure Act, including, for example, providing adequate notice, opportunity to be heard, and opportunity to present rebuttal evidence; and (11) unconstitutionality of the appointments of the Board judges who decided this case.

SecureWave also appeals from any and all finding, determination, statutory interpretations, regulatory interpretations, and/or procedures supporting or relating to the aforementioned issues, as well as all other issues decided adversely to SecureWave in any written or verbal orders, decisions, rulings, and opinions.

Respectfully Submitted,

Date: September 8, 2020

Cabrach Connor
Registration No. 53,837
Lead Counsel for Patent Owner
CONNOR KUDLAC LEE PLLC

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing **PATENT OWNER'S NOTICE OF APPEAL** and all documents filed with it were served via electronic mail upon the following counsel for the Petitioner on September 8, 2020:

Ashraf Fawzy (Lead Counsel) afawzy@unifiedpatents.com
Jung S. Hahm (First Back-up Counsel) jung@unifiedpatents.com
Andrew R. Sommer (Back-up Counsel) sommera@gtlaw.com
Jonathan R. Bowser (Back-up Counsel) jbowser@unifiedpatents.com
Jonathan Stroud (Back-up Counsel) jonathan@unifiedpatents.com
Ming Hung Hung (Back-up Counsel) mhung@winston.com

I further certify that on September 8, 2020, the foregoing **PATENT OWNER'S NOTICE OF APPEAL** and a copy of the Final Written Decision (Paper 31) that was filed with is being sent by USPS Priority Mail to the Director of the United States Patent and Trademark Office, at the following address:

Office of Solicitor
United States Patent & Trademark Office
Mail Stop 8, P.O. Box 1450
Alexandria, VA 22313-1450

I further certify that on September 8, 2020, the foregoing **PATENT OWNER'S NOTICE OF APPEAL** and a copy of the Final Written Decision (Paper 31) and the required fee is being filed with the United States Court of Appeals for the Federal Circuit via its CM/ECF electronic filing system.

Date: September 8, 2020

/Cabrach Connor/
Cabrach Connor
Registration No. 53,837
Lead Counsel for Patent Owner
CONNOR KUDLAC LEE PLLC

Trials@uspto.gov
571-272-7882

Paper 31
Date: July 7, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS INC.,
Petitioner,

v.

SECUREWAVE STORAGE SOLUTIONS, INC.,
Patent Owner.

IPR2019-00501
Patent 7,036,020

Before JONI Y. CHANG, ANNETTE R. REIMERS, and GARTH D. BAER, *Administrative Patent Judges*.

BAER, *Administrative Patent Judge*.

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

I. INTRODUCTION

Unified Patents Inc., ("Petitioner") filed a Petition (Paper 2, "Pet."), requesting an *inter partes* review of claims 1–5 (the "challenged claims") of U.S. Patent No. 7,036,020 (Ex. 1001, "the '020 patent"). Petitioner also filed the supporting Declaration of Dr. Martin Kaliski. Ex. 1002. SecureWave Storage Solutions, Inc. ("Patent Owner") filed a Preliminary Response to the Petition (Paper 6, "Prelim. Resp."). Upon consideration of the Petition and Preliminary Response, we instituted *inter partes* review of all challenged claims on all grounds raised. Paper 7 ("Dec. Inst.").

Patent Owner filed a Response to the Petition (Paper 12, "PO Resp."), Petitioner filed a Reply (Paper 17, "Pet. Reply"). Petitioner also filed the supporting Reply Declaration of Dr. Martin Kaliski. Ex. 1015. Patent Owner filed a Sur-Reply (Paper 22, "PO Sur-Reply"). An oral hearing was held on April 9, 2020, and the hearing transcript is included in the record. *See* Paper 30 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6(b). This is a Final Written Decision under 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons set forth below, we find Petitioner has shown by a preponderance of evidence that claims 1–5 of the '020 patent are unpatentable.

A. RELATED PROCEEDINGS

The parties identify *SecureWave Storage Solutions, Inc. v. Kingston Tech. Co., Inc.*, Case No. 8:18-cv-01425 (C.D. Cal.) and *SecureWave Storage Solutions, Inc. v. Micron Tech., Inc.*, Case No. 18-cv-01398-MN (D. Del.) as related matters. Paper 4, 2–3. The parties also note that the '020 patent is at issue in IPR2019-00494. *Id.* at 2. IPR2019-000494 was filed by Kingston Technology Company, Inc. and was denied institution. *See*

Kingston Tech. Co., Inc. v. SecureWave Storage Solutions, Inc., IPR2019-00494, Paper 8 (PTAB July 11, 2019).

B. THE '020 PATENT

The '020 patent is directed to a storage device in a computer system. Ex. 1001, (code 57). The storage device includes a security partition with restricted access. *Id.* The storage device further includes at least one authority record and associated data. *Id.* The methods and systems in the '020 patent promote security in the computer system. *Id.*

C. ILLUSTRATIVE CLAIM

Petitioner challenges claims 1–5 of the '020 patent. Claim 1 is the only independent challenged claim and is reproduced below:

> 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 two 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 and Asserted Grounds

Petitioner asserts the following grounds of unpatentability. Pet. 9.

Claim(s) Challenged	35 U.S.C. §[1]	Reference(s)/Basis
1–5	§ 103	Guthery,[2] Dethloff[3]
1–5	§ 103	Guthery, Dethloff, Moran[4]
1–5	§ 103	Robb[5], Jones[6], Grawrock[7]

II. ANALYSIS

A. Level of Skill in the Art

Petitioner asserts that a skilled artisan "would have had (1) a bachelor's in computer science, electrical engineering, computer engineering, or similar field, and (2) at least one year of experience with secure computer architectures, computer security software, and data security." Pet. 9–10. In addition, according to Petitioner, "[m]ore experience could accommodate for less education and vice versa." *Id.* at 10. Patent Owner's formulation for a skilled artisan is not meaningfully different from Petitioner's. *See* PO Resp. 15. We agree with and adopt Petitioner's proposal because it is consistent with the '020 patent, as well as the problems and solutions in the prior art of record. *See Daiichi Sankyo Co. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007). We note, however, that

[1] The Leahy-Smith America Invents Act ("AIA") amended 35 U.S.C. § 103. *See* Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011). As the application that issued as the '020 patent was filed before the effective date of the relevant amendments, the pre-AIA version of § 103 applies.
[2] U.S. Patent No. 6,567,915 B1 (May 20, 2003) (Ex. 1004).
[3] U.S. Patent No. 4,837,422 (June 6, 1989) (Ex. 1005).
[4] U.S. Patent No. 6,324,537 B1 (Nov. 27, 2001) (Ex. 1006).
[5] U.S. Patent No. 6,931,503 B1 (Aug. 16, 2005) (Ex. 1007).
[6] U.S. Patent No. 5,623,637 (Apr. 22, 1997) (Ex. 1008).
[7] U.S. Patent No. 6,081,893 (June 27, 2000) (Ex. 1009).

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 *inter partes* review proceedings based on petitions filed on or after November 13, 2018,[8] such as this one, we construe claims using the same claim construction standard that would be used in a civil action under 35 U.S.C. § 282(b), as articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc), and its progeny. *See* 37 C.F.R. § 42.100(b) (2019).

1. "authority record"

According to Petitioner, "the phrase '**one or more authority records**' means '*at least one record that defines who or what has access to the secure partition and secure data.*'" Pet. 10. Patent Owner asserts that there is no need to further construe "authority record" (*see* PO Resp. 18), but if the Board does construe the term, we should "add the word 'permissions' after the word 'access' and add the word 'data' between 'secure' and 'partition,' to track more precisely with the express teachings and language of the patent." *Id*. at 19. The parties' constructions are not materially different.[9]

[8] On October 11, 2018, the USPTO revised its rules to harmonize the Board's claim construction standard with that used in civil actions under 35 U.S.C. § 282(b) in federal district courts. Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340, 51,358 (Oct. 11, 2018) (amending 37 C.F.R. § 42.100(b) effective November 13, 2018) (now codified at 37 C.F.R. § 42.100(b) (2019)). This rule change applies to petitions filed on or after November 13, 2018.

[9] Petitioner relies on Jones for teaching an authority record. *See* Pet. 49. Patent Owner does not contest that Jones teaches an authority record under its construction or Petitioner's. *See* PO Resp. 46–57. Our conclusion *infra*

Nonetheless, we agree with Patent Owner that its construction follows the claims' language more closely. Thus, we construe "authority record" as "at least one record that defines who or what has access permissions to the secure data partition and the secure data."

2. "master authority record"

According to Petitioner, "[t]he phrase '**master authority record**' means '*an authority record that provides access permissions for a user to create or delete other authority records*.'" Pet. 10. Patent Owner asserts that there is no need to explicitly construe "master authority record" (*see* PO Resp. 19), and again offers a construction that differs only slightly from Petitioner's. Specifically, according to Patent Owner, "[t]he master authority record does not *provide* access permissions, as Petitioner agues, but rather it *enables* the creation and deletion of authority records *according to* access permissions it maintains. In other words, the master authority record 'governs' the authority records." *Id*. at 20. Here again, the parties' constructions are not materially different.[10] Nonetheless, we agree with Patent Owner that its construction follows the claims' language more closely. Specifically, according to the '020 patent, "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. Thus, we adopt Patent Owner's construction: a master authority record is a record that "enables the creation and deletion of authority records according to access permissions it maintains."

---

that the Jones teaches authority records would not change based on the parties' different constructions.

[10] Petitioner relies on Grawrock for teaching a master authority record. *See* Pet. 53. Our conclusion *infra* that Grawrock teaches a master authority record would not change based on the parties' different constructions.

C. ASSERTED PRIOR ART

1. Robb (Ex. 1007)

Robb discloses a storage device including a storage medium for storing information, and a ROM for storing firmware for controlling operation of the storage device. Ex. 1007, code (57). The firmware stored in ROM includes a supervisor that protects information stored on the storage medium. *Id.* Figure 1 is reproduced below.

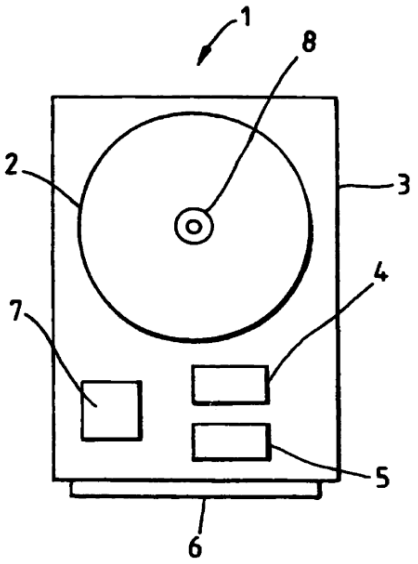

Fig. 1

Figure 1 above illustrates a hard disk drive embodiment. *Id.* at 7:9–10.

2. Jones (Ex. 1008)

Jones discloses:

> [a] detachable [Personal Memory Card Industry Association ("PCMCIA")] memory card incorporating a smart-card integrated circuit for storing a password value and logic circuitry for preventing access to information stored on the memory card unless the user of the host computer to which the memory card is connected can supply a password matching the stored password.

Ex. 1008, code (57). Figure 1 is reproduced below.

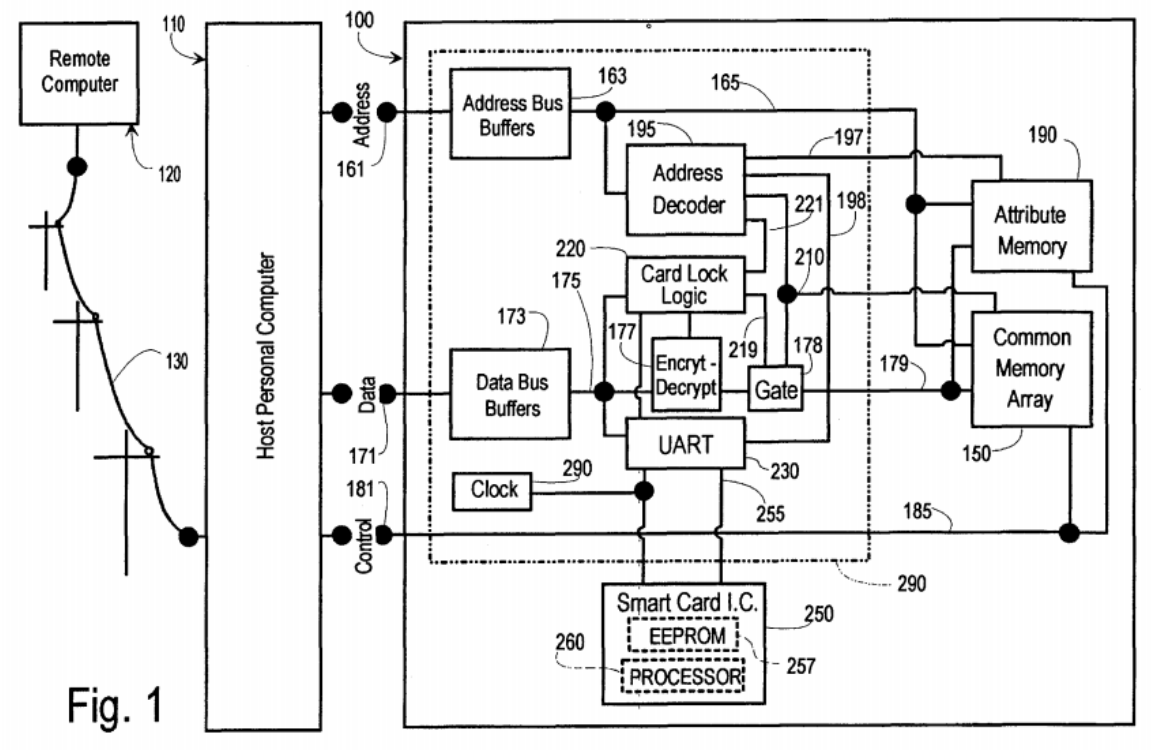

Fig. 1

Figure 1 above illustrates a block diagram of the secure memory card. *Id.* at 2:66–67. This card includes common memory array 150 that stores data, *id.* at 3:50–55, non-volatile attribute memory 190 that establishes an interface with the host computer, *id.* at 4:23–30, and smartcard IC 250 that stores and controls access for secret keys, *id.* at 5:1–7.

3. Grawrock (Ex. 1009)

Grawrock discloses a password-based system for controlling access to secure files in a workstation. Ex. 1009, code (57). A system administrator is authorized to create their own password and default log-in records for further authorized users, who in turn provide their own new passwords. *Id.* at 15:43–61.

D. Obviousness Analysis

1. Obviousness of Claims 1–5 based on Robb, Jones, and Grawrock

Petitioner asserts that independent claims 1–5 would have been obvious over a combination of Robb, Jones, and Grawrock. Pet. 42. Based

on Petitioner's analysis and as explained below, we find Petitioner has shown by a preponderance of evidence that claims 1–5 would have been obvious over Robb, Jones, and Grawrock.

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

Claim 1 requires "firmware for reading data from and writing data to the storage medium." Petitioner relies on Robb for this limitation. Pet. 47–48. Specifically, Petitioner asserts Robb's "Supervisor" firmware "'controls the transfer of information to and from the storage medium via the interface to the computer system,' and can 'allow/restrict/prohibit, read/write operations upon the storage medium.'" *Id*. 47–48 (quoting Ex. 1007, 2:38–42, 4:4–11). Patent Owner distinguishes Robb's firmware that is merely "used to control read/write operations," from the claim, which, according to Patent Owner, requires firmware that "*itself* reads data from and writes data to the storage medium." PO Resp. 46.

We agree with Petitioner that Robb discloses the disputed firmware limitation. The claim requires "firmware for reading data from and writing data to the storage medium." Nothing in the claim's plain language requires that read 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. Although, as Patent Owner notes, the '020 patent describes "[t]he storage device 12 contains firmware 14 that reads and writes data from a data storage portion 16 of the storage device 12," (PO Resp. 47 (emphasis omitted) (quoting Ex. 1001, 4:46–48)), that disclosure, like the disputed claim language, does not necessitate that the firmware *alone* must perform all aspects of reading and writing.

Robb's supervisor firmware "controls the transfer of information to and from the storage medium" and "allow[s]/restrict[s]/prohibit[s], read/write operations upon the storage medium." Ex. 1007, 2:36–42, 4:4–11. Robb further characterizes its supervisor firmware as "integrat[ed] . . . into the existing control firmware of the hard disk drive, ensuring that no interface request is serviced before the Supervisor firmware has checked and validated the request." *Id*. at 10:24–27. Thus, we agree with Dr. Kaliski's characterization of Robb's firmware as "intercept[ing] read/write requests from a host computer system to the storage medium for validation and then once it determines that they are valid, Robb's firmware *causes* the read/write operations to be performed on the storage medium." Ex. 1015 ¶ 23 (emphasis added). In light of Robb's disclosures and Dr. Kaliski's testimony, we find Robb discloses firmware for reading data from and writing data to the storage medium, as claim 1 requires. *See* Ex. 1007, 2:36–42, 4:4–11, 10:24–27; Ex. 1002 ¶ 122; Ex. 1015 ¶¶ 19–25.

b. "the secure data partition for storing secure data and one or more authority records"

Claim 1 requires a "secure data partition for storing secure data and one or more authority records." Petitioner relies on the combined teachings of Robb and Jones for this limitation. Pet. 48–51. Specifically, Petitioner asserts "Robb's 'dedicated area' or 'special partition' is the claimed *secure data partition* that stores *secure data*" and "Jones's password stored in [Card Information Structure ("CIS")] . . . or 'passwords, key values, access codes and the like' . . . constitute the claimed authority records" Pet. Reply 6 (quoting Ex. 1008, 7:65–66). Petitioner further explains, with support from its expert, Dr. Kaliski, that one skilled in the art would have been motivated to apply Jones's authority-record-access teaching to Robb's secure partition

as a known way of "protect[ing] the partitions from unauthorized use." Pet. 56 (citing Ex. 1002 ¶ 142; *see id*. at 57 (explaining that "Jones's per-partition security scheme would have proven to be a useful feature to provide the security suggested by Robb"). Petitioner also explains that a skilled artisan would have been motivated to store Jones's authority records in Robb's special partition as "a cost-effective and secure solution for storing Jones's authority records." *Id*. at 58.

Patent Owner asserts that Petitioner's challenge fails because in Jones, neither the password stored in CIS nor the passwords, key values, and access codes stored (i.e., the claimed authority records) are stored in a secure data partition. PO Resp. 48–52. Patent Owner also contends that "Petitioner's conclusory arguments about reasons to combine Jones with Robb do not withstand scrutiny," because "Jones teaches away from the solutions proposed by Robb." *Id*. at 54. According to Patent Owner, placing Jones's authority records into Robb's dedicated area "would render the invention inoperable, because the authority records would be cleared after every system reset." *Id*.

We agree with Petitioner's analysis. Patent Owner does not dispute that Robb discloses a secure partition for storing secure data, or that Jones discloses authority records under Patent Owner's construction for the term. *See* PO Resp. 48–55. Thus, Petitioner has shown that its proffered *combination* of Robb and Jones teaches "the secure data partition for storing . . . one or more authority records." *See* Pet. 42–63. Patent Owner's argument—that Jones's authority records are not stored in a secure partition—attacks the references individually rather than in combination, as Petitioner asserts. *See* Pet. 51. It does not matter whether Jones teaches

storing data in a secure data partition because Petitioner relies on Robb, not Jones, for teaching that feature. *See id*.

In addition, we find Petitioner has articulated sufficient reasoning with some rational underpinning to support the legal conclusion that its proffered combination would have been obvious to one skilled in the art. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007). We disagree with Patent Owner's argument that Jones teaches away from placing authentication records in Robb's secure partition because Patent Owner has not identified any teaching in Jones or Robb that "criticize[s], discredit[s], or otherwise discourage[s] investigation into" doing so. *Meiresonne v. Google, Inc.*, 849 F.3d 1379, 1382 (Fed. Cir. 2017); *see* PO Resp. 54. We also disagree with Patent Owner that combining Jones's authority records with Robb would render the invention inoperable given Robb's optional information clearing after system reset. We disagree first because the information clearing feature is optional, and second because Patent Owner's argument improperly relies on bodily incorporating the references. *See Hewlett-Packard Co. v. Mustek Sys., Inc.*, 340 F.3d 1314, 1326 (Fed. Cir. 2003) ("[A] prior art product that sometimes, but not always, embodies a claimed method nonetheless teaches that aspect of the invention."); *In re Keller*, 642 F.2d 413, 425 (CCPA 1981) ("The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference."). Thus, we agree with Petitioner that the combination of Robb and Jones teaches "the secure data partition for storing secure data and one or more authority records." *See* Pet. 48–51

c. "the secure data partition contains a master authority record"

Claim 1 recites "the secure data partition contains a master authority record." Petitioner asserts Grawrock discloses the claimed master authority

record because Grawrock's administrator record "allows for the creation and deletion of records for other users" and "provides access permissions for a user to create or delete authority records." Pet. 53 (citing Ex. 1002 ¶ 137; Ex. 1009, 15:43–55, 15:46–50, 15:58–61, 21:26–28). Further, according to Petitioner, one skilled in the art would have had a reason to combine Grawrock's master authority record with Robb's secure-partition system because doing so would have "allowed the creation of a system where different users could gain access to different partitions based on whether they were assigned access by a system administrator." *Id.* at 58, 59. Petitioner goes on to explain, with support from Dr. Kaliski, that Grawrock's master authority record feature "would have been viewed as being an important feature when implementing Robb in, for example, a corporate or other multi-user environment in which many users may be accessing the same host and memory, but where it is desirable to limit certain people to accessing certain data." *Id.* at 59 (citing Ex. 1002 ¶ 144). Further, according to Petitioner, a skilled artisan would be motivated to place Grawrock's master authority record in Robb's dedicated area or special partition to better secure the data. *See id.*

Patent Owner asserts that Petitioner's challenge fails because Grawrock's administrator record (i.e., the claimed master authority record) is not stored in a secure, private partition, PO Resp. 57, and because "Robb's system already has the ability to control which users can activate which partitions in protected mode," *id.* at 58.

We agree with Petitioner's analysis. As Petitioner explains, *see* Pet. 53, Grawrock teaches that the first time a user or administrator logs into a workstation, "a default log-in report is held within the workstation for the system administrator." Ex. 1009, 15:43–55. The administrator is then

prompted to provide a new password and "[a] new record is originated for the system administrator." *Id.* at 15:46–50. "The system administrator is thereafter allowed to log in-under his/her new password and to create additional temporary, default log-in records for subsequently authorized users." *Id.* at 15:58–61. The administrator can also delete user records. *Id.* at 21:26–28. In light of those disclosures, we agree with Petitioner that Grawrock's administrator record is a master authority record. *See* Pet. 53.

In addition, we find Petitioner has articulated sufficient reasoning with some rational underpinning to support the legal conclusion that its proffered combination would have been obvious to one skilled in the art. *See KSR*, 550 U.S. at 418. As Petitioner explains, a skilled artisan would be motivated to employ Grawrock's master authority record in Robb's system to facilitate limiting access to certain data in a multi-user environment. Pet. 59. Further, a skilled artisan would have placed Grawrock's master authority record in Robb's secure partition to better secure the data. *See id.* Patent Owner's argument—that Grawrock's administrator record is not stored in a secure partition—again attacks the references individually rather than in combination, as Petitioner asserts. *See id.* It does not matter whether Grawrock teaches storing its master authority record in a secure data partition because Petitioner relies on Robb, not Grawrock, for teaching that feature. *See id.* Further, even assuming Patent Owner is correct that Robb's system "already has the ability to control which users can activate which partitions in protected mode," PO Resp. 58, that does not undermine Petitioner's assertion that it would have been obvious to combine Grawrock's alternative method of doing so. *See In re Fulton*, 391 F.3d 1195, 1200 (Fed. Cir. 2004) ("[O]ur case law does not require that a particular combination must be the preferred, or the most desirable,

combination described in the prior art in order to provide motivation for the current invention."); *see also KSR*, 550 U.S. at 417 ("If a person of ordinary skill in the art can implement a predictable variation, and would see the benefit of doing so, § 103 likely bars its patentability."). Thus, we agree with Petitioner that the combination of Robb and Grawrock teaches "the secure data partition contains a master authority record."

d. Undisputed Elements of Claim 1

Claim 1 recites "[a] storage device for promoting security in a computer system." Petitioner asserts that Robb teaches this limitation because "Robb teaches 'a storage device (1) for a host computer system,' and the storage device 'incorporates a Supervisor function for controlling access to information stored in a storage medium (2) of the device.'" Pet. 47 (quoting Ex. 1007, code (57)). We agree with Petitioner's analysis and Patent Owner does not dispute Petitioner's assertions in this regard.

Claim 1 further recites "a storage medium for storing data." Petitioner asserts that Robb teaches this limitation because "Robb's Figure 1 'shows a storage device in the form of a hard disk drive 1.'" Pet. 47 (quoting Ex. 1007, 7:17–19). We agree with Petitioner's analysis and Patent Owner does not dispute Petitioner's assertions in this regard.

Claim 1 further recites "a partition defined on the storage medium for dividing the storage medium into a data partition and a secure data partition." Petitioner asserts Robb teaches this limitation because Robb's "boot partition or other active partitions like the read only partition, are data partitions," whereas Robb's "dedicated area" or "special partition," accessible only to the supervisor firmware, "is the claimed 'secure data partition.'" Pet. 49 (citing Ex. 1007, 8:40–60, 9:16–26). We agree with

Petitioner's analysis and Patent Owner does not dispute Petitioner's assertions in this regard.

Claim 1 further recites "wherein the one or more authority records define access permissions relating to the secure data partition and the secure data." Petitioner asserts that Jones teaches this limitation. Pet. 52. In particular, according to Petitioner, "each of Jones's authority records provide access permissions related to the secure data partition and the secure data because the passwords indicate the user that has access to a particular secure partition" and "the access code indicates the remote user and host that has access to the secure partition to engage in encrypted data communications with a remote station." *Id*. (citing Ex. 1008, 2:38–43, 8:35–41, 8:52–54, 9:1–25). Further, as outlined above, Petitioner explains that one skilled in the art would have been motivated to combine Jones's authority records with Robb's secure partition as a known way of protecting Robb's partitions from unauthorized use. *See supra.* We agree with Petitioner's analysis and Patent Owner does not dispute Petitioner's assertions in this regard.

Claim 1 further recites "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." Petitioner asserts Grawrock discloses this limitation because "Grawrock's master authority records provide access permissions for the creation and deletion of authority records." Pet. 54 (citing Ex. 1009, 15:52–55 ("The System administrator is thereafter allowed to log-in under his/her new password and to create additional temporary, default log-in records for subsequently authorized users."), 21:26–28 (an administrator can "erase the . . . log-in record . . . of a given user at will.")). Further, as outlined above, Petitioner explains that one skilled in the art would have been motivated to combine Grawrock's

master authority record feature with Robb's secure partition to facilitate a system in which different users can access different assigned partitions based on whether a system administrator assigns access. *See supra* § II.D.1.c. We agree with Petitioner's analysis and Patent Owner does not dispute Petitioner's assertions in this regard.

Claim 1 further requires "wherein only the firmware is permitted to access the secure data and the one or more authority records." Petitioner asserts that the combination of Robb and Jones teaches this limitation because Robb's dedicated area/special partition is "accessible only to, and is protected by the [firmware] Supervisor." Pet. 55 (quoting Ex. 1007, 9:16–18). In addition, Petitioner explains, "[i]t would have been obvious to store [Jones's] authority records in Robb's 'special partition,' since that is a location that provides enhanced data security . . . and was known to store secure data like passwords." *Id*. We agree with Petitioner's analysis. In addition, as explained above, we agree with Petitioner that it would have been obvious for one skilled in the art to apply Jones's authority-record-access teaching to Robb's secure partition and to store Jones's authority records in Robb's special partition. Thus, we agree with Petitioner that the combination of Robb and Jones teaches "wherein only the firmware is permitted to access the secure data and the one or more authority records." Given our findings and conclusions above, we find Petitioner has proved by a preponderance of the evidence that claim 1 would have been obvious over Robb, Jones, and Grawrock.

e. Claim 2

Claim 2 depends from claim 1 and additionally requires "wherein the storage device is in communication with a computer system having an operating system." Petitioner asserts Robb discloses this limitation because

in Robb's storage device is "a hard disk drive 1 for incorporating in a host computer system." Pet. 59 (quoting Ex. 1007, 7:17–19). Further, Petitioner notes, because Robb refers to "initiating 'the operating system boot,'" Robb's computer system has an operating system. *Id*. at 59–60 (quoting Ex. 1007, 6:35–40). We agree with Petitioner's analysis and Patent Owner does not dispute Petitioner's assertions in this regard.

f. Claim 3

Claim 3 depends from claim 2 and additionally requires "wherein secure data stored in the secure data partition is invisible to the operating system." Petitioner asserts Robb discloses this limitation because Robb's dedicated area/special partition, which contains the secure data, is accessible only to the firmware Supervisor and is thus "effectively 'hidden' from the host system." Pet. 60 (quoting Ex. 1007, 9:18–22). We agree with Petitioner's analysis and Patent Owner does not dispute Petitioner's assertions in this regard.

g. Claim 4

Claim 4 depends from claim 1 and additionally requires "wherein each of the one or more authority records contains one public-private key pair for authenticating data that originates from the security partition." Petitioner asserts Jones discloses this limitation because "Jones discloses that 'public and private key values' are 'used to encrypt and decrypt data stored on the card.'" Pet. 61 (quoting Ex. 1008, code (57)). According to Petitioner,

> A [Person of Ordinary Skill in the Art ("POSA")] would have been motivated to include Jones's encryption keys as part of the authority records stored in the special partition because such an arrangement would allow for secure, encrypted communications to the host processor, thus giving further security to the system

> and preventing unauthorized interception of the data from the secure partition.

Id. (citing Ex. 1002 ¶ 158).

Patent Owner argues that Jones does not disclose the additional limitation in claim 4 because "Petitioner conflates 'protecting' data with 'authenticating' data." PO Sur-Reply 19. According to Patent Owner "Jones discloses encryption of data but does not disclose authentication of data." *Id*. at 20.

We agree with Petitioner's analysis. As Petitioner notes, Jones teaches that "[t]he smartcard integrated circuit may also be used to store public and private key values used to encrypt and decrypt data stored on the card or elsewhere on the host computer or exchanged with a remote computer." Ex. 1008, code (57). Patent Owner's argument suggests Jones's disclosure is limited to only encryption using a public key and decryption using a private key. *See* PO Sur-Reply 19. We disagree because Jones discloses using both public and private keys both for encryption and decryption—i.e., "public and private key values used to encrypt and decrypt data." Ex. 1008, code (57).[11] Thus, Jones discloses a public-private key pair for authenticating data even under Patent Owner's more narrow construction. *See* Ex. 1002 ¶¶ 153–158.

h. Claim 5

Claim 5 depends from claim 1 and additionally requires "wherein the storage device further comprises: cryptographic operations embedded in the

[11] Patent Owner's argument also fails because Patent Owner raised it for the first time in its Sur-Reply. *See* 37 C.F.R. § 42.23(b) ("A reply may only respond to arguments raised in the corresponding . . . patent owner response.").

firmware of the storage device." Petitioner asserts Jones discloses this limitation because "[Jones's] private key, or a key-pair having a private key, is for executing a cryptographic operation." Pet. 62 (citing Ex. 1002 ¶ 161). Further, according to Petitioner, a skilled artisan would have had reason to combine Jones's private key cryptographic operations because "[a] POSA would have understood that there are advantages to encrypting data stored Robb's special partitions such as those disclosed by Robb when that data is sensitive and access to that data should be restricted." *Id*. at 63 (citing Ex. 1002 ¶ 162). We agree with Petitioner's analysis and Patent Owner does not dispute Petitioner's assertions in this regard.

2. Other Asserted Grounds

Petitioner asserts that claims 1–5 are obvious over Guthery and Dethloff or, alternatively, that claims 1–5 are obvious over a combination of Guthery, Dethloff, and Moran. Pet. 9. Because we find that Petitioner has demonstrated claims 1–5 would have been obvious over Robb, Jones, and Grawrock, it is unnecessary for us to reach the remaining grounds of unpatentability proposed by Petitioner. *See Beloit Corp. v. Valmet Oy*, 742 F.2d 1421, 1423 (Fed. Cir. 1984) (holding that once a dispositive issue is decided, there is no need to decide other potentially dispositive issues); *Formlabs Inc. v. Envisiontec, Inc.*, IPR2017-01258, Paper 41 at 17 (PTAB Oct. 5, 2018).

III. CONCLUSION[12]

We have reviewed the Petition, Patent Owner Response, Petitioner Reply, and Patent Owner Sur-Reply. We have considered all of the evidence and arguments presented by Petitioner and Patent Owner, and have weighed and assessed the entirety of the evidence as a whole.

We determine, on this record, that Petitioner has demonstrated by a preponderance of evidence that claims 1–5 of the '020 patent are unpatentable over Robb, Jones, and Grawrock.

Claims	35 U.S.C. §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–5	103	Robb, Jones, Grawrock	1–5	

IV. ORDER

It is hereby:

ORDERED that claims 1–5 of the '020 patent are unpatentable under 35 U.S.C. § 103(a) as obvious over Robb, Jones, and Grawrock; and

[12] 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).

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

For PETITIONER:

Ashraf Fawzy
Jung S. Hahm
Jonathan Stroud
Ming Hung
Jonathan R. Bowser
UNIFIED PATENTS INC.
afawzy@unifiedpatents.com
jung@unifiedpatents.com
jonathan@unifiedpatents.com
mhung@winston.com
jbowser@unifiedpatents.com

Ming Hung Hung
WINSTON & STRAWN LLP
mhung@winston.com

Andrew R. Sommer
sommera@gtlaw.com

For PATENT OWNER:

Cabrach Connor
CONNOR KUDLAC LEE PLLC
cab@connorkudlaclee.com

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