Trials@uspto.gov
571-272-7882

Paper No. 8
Entered: July 11, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KINGSTON TECHNOLOGY COMPANY, INC.,
Petitioner,

v.

SECUREWAVE STORAGE SOLUTIONS, INC.,
Patent Owner.

Case IPR2019-00494
Patent 7,036,020 B2

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

BAER, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

Kingston Technology Company ("Petitioner") filed a Petition (Paper 2, "Pet."), 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"). SecureWave Storage Solutions, Inc. ("Patent Owner") filed a Preliminary Response to the Petition (Paper 7, "Prelim. Resp."). For the reasons discussed below, we deny the Petition and do not institute *inter partes* review.

A. RELATED PROCEEDINGS

The parties identify *SecureWave Storage Solutions, Inc. v. Kingston Tech. Co., Inc.*, Case No. 8:18-cv-10425 (C.D. Cal.) and *SecureWave Storage Solutions, Inc. v. Micron Tech., Inc.*, Case No. 18-cv-01398-MN (D. Del.) as related matters. Pet. 2, Prelim. Resp. 15–16. The parties also note that the '020 patent is at issue in IPR2019-00501. Paper 4, 2.

B. THE '020 PATENT

The '020 patent is directed to a storage device in a computer system. Ex. 1001, Abstract. 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 1–14 of the '020 patent. Independent claim 12 is illustrative of the challenged claims and is reproduced below:

> 12. A storage device comprising: a storage medium having 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, wherein the mechanism comprises a processor disposed within the storage device adapted to limit access to the security partition by an operating system of a computer system, and firmware disposed within the storage device adapted to limit access to the security partition by an operating system of a computer system.

Ex. 1001, 14:14–26.

D. Asserted Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability. Pet. 3–4.

References	Basis	Challenged Claim(s)
Silvester[1] and Hamlin[2]	§ 103	1–4 and 12–14
Silvester, Hamlin, and X.509[3]	§ 103	4
Silvester, Hamlin, and Kadooka[4]	§ 103	5
Silvester, Hamlin, Kadooka, and Dancs[5]	§ 103	6
Silvester, Hamlin, Dancs	§ 103	7–10
Silvester, Hamlin, Dancs, and Kadooka	§ 103	7–10
Silvester, Hamlin, and Monsen[6]	§ 103	11

[1] U.S. Patent No. 7,155,615 B1 (filed June 30, 2000) (Ex. 1005).
[2] U.S. Patent No. 7,155,616 B1 (filed July 31, 2000) (Ex. 1006).
[3] ITU-T Standard No. X.509, "Information technology – Open Systems Interconnection – The Directory: Authentication framework" (published August 1997) (Ex. 1010).
[4] U.S. Patent No. 5,428,685 A (issued June 27, 1995) (Ex. 1007).
[5] U.S. Patent No. 6,141,752 A (issued October 31, 2000) (Ex. 1008).
[6] U.S. Patent No. 6,606,628 B1 (filed February 14, 2000) (Ex. 1009).

II. ANALYSIS

A. CLAIM CONSTRUCTION

Petitioner proposes that we construe the term "authority record" to be "a record that includes information about user authorizations to access the secure partition of the storage device," and that we construe the term "root assurance" to mean "root authority." Pet. 8, 10. Patent Owner does not propose alternative constructions, but asserts that these two terms should have their plain and ordinary meaning. Prelim. Resp. 24–26. We decline to construe these terms because no express claim construction is necessary for our determination of whether to institute *inter partes* review. *See Vivid-Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) ("[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.").

B. ASSERTED PRIOR ART

1. Silvester (Ex. 1005)

Silvester discloses a "secure-private partition on a storage device of a computer system," that "is normally invisible to an operating system unless the partition is unlocked." Ex. 1005, Abstract. Figure 4 is reproduced below.

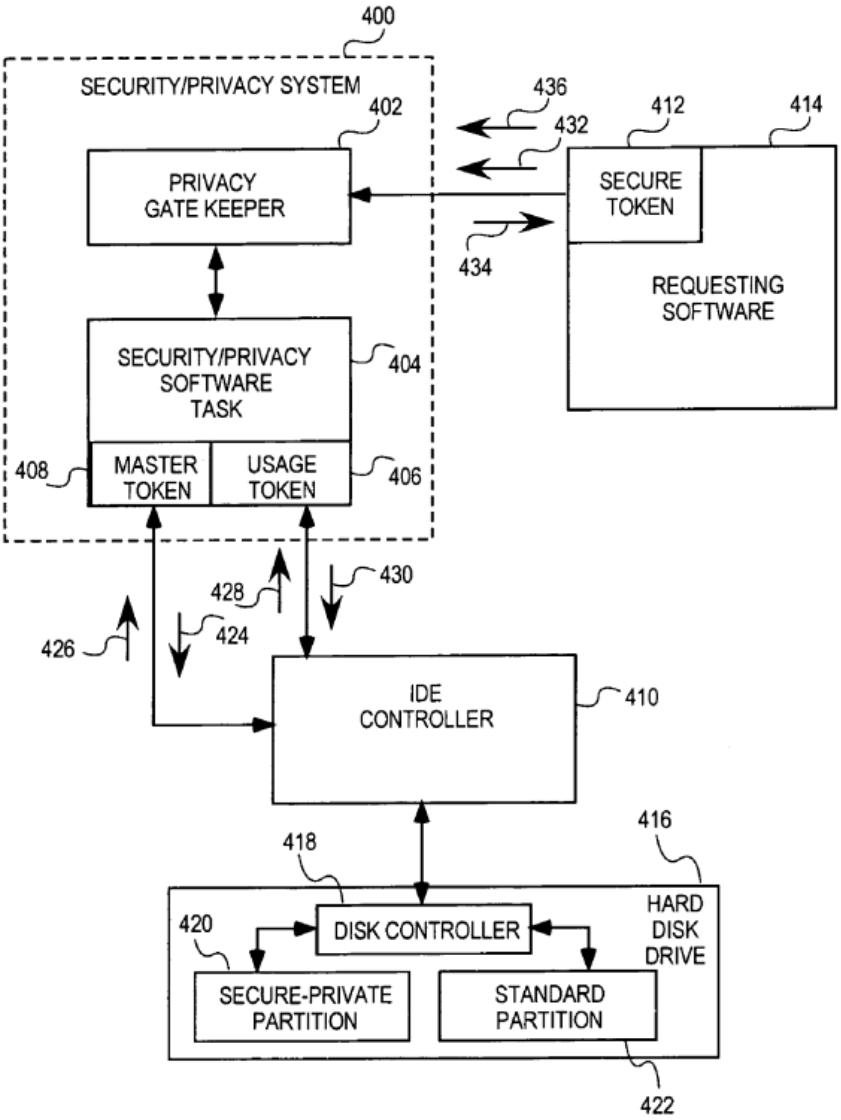

FIG. 4

Figure 4 illustrates "a block diagram of a security/privacy system according to one embodiment." *Id*. at 1:56–57.

2. Hamlin (Ex. 1006)

Hamlin discloses:

> an authentication server computer operated by a system administrator, and a disk drive connected to the authentication server computer. The disk drive comprises an interface for receiving the personal information data and user access data from the system administrator, a disk for storing data, and a disk

> controller for controlling access to the disk. An authenticator within the disk drive, responsive to the personal authentication data, enables the disk controller, and cryptographic circuitry encrypts the user access data received from the system administrator into encrypted data stored on the disk.

Ex. 1006, Abstract. Hamlin's Figure 3 is reproduced below.

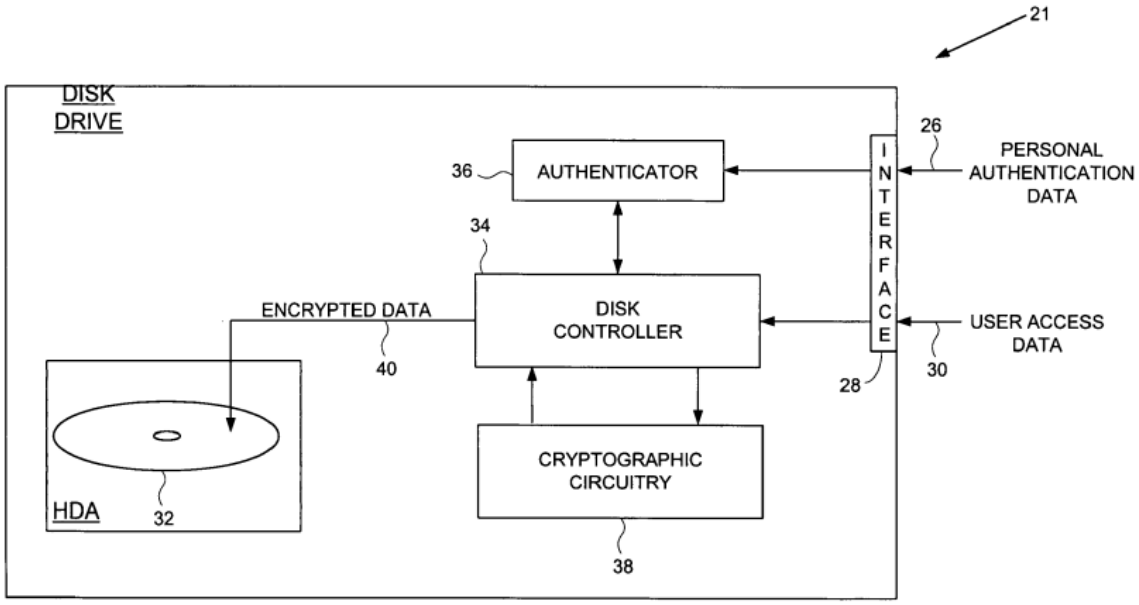

FIG. 3

Figure 3 illustrates one embodiment of the disk drive. *Id*. at 4:13–18.

3. X.509 (Ex. 1010)

X.509 discloses a standard method for authentication services. It teaches using a password for "simple authentication" and using cryptography for "strong authentication." Ex. 1010, Abstract. The strong authentication implements a public key cryptosystem with a user private key and a user public key. *Id.* at 9–10.

4. Kadooka (Ex. 1007)

Kadooka discloses a system for protecting data on a memory card. Ex. 1007, Abstract. In one embodiment, a memory card includes encryption firmware for "encrypting data written in the IC memory card" and

deciphering firmware "for deciphering data, which has been read from the IC memory card." *Id.* at 8:63–9:3.

5. *Dancs (Ex. 1008)*

Dancs discloses that it

> is in the field of network computer client devices (NCs) which rely upon a network connection to supply all necessary program files and data files and which accept individual users' smart cards containing account information with various internet service providers (ISPs). Specifically, the present invention addresses the need for authentication of the ISP to the NC and authentication of the smart card contents to the ISP.

Ex. 1008, 1:32–39. Figure 2 is reproduced below.

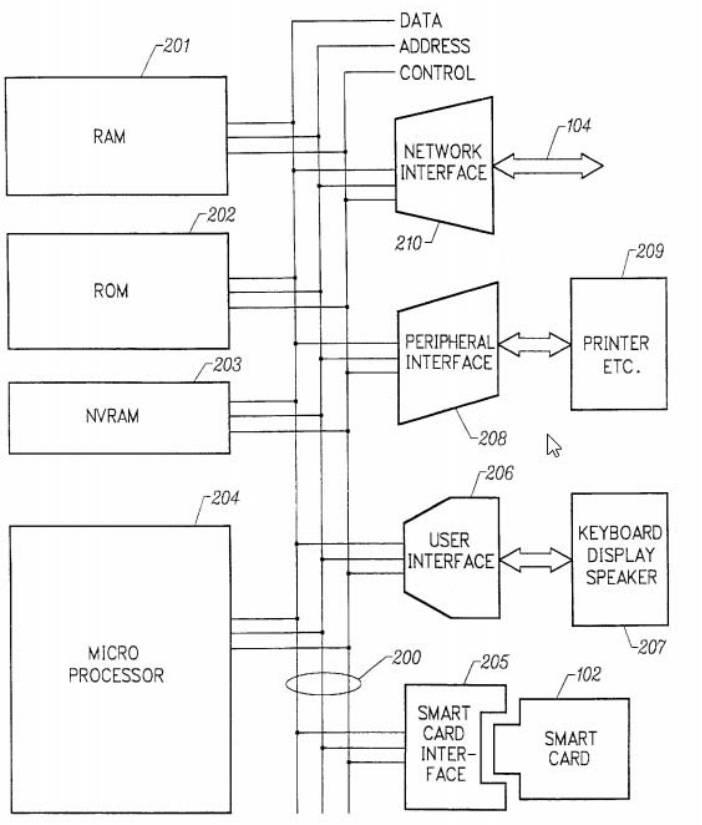

FIG. 2

Figure 2 is a block diagram illustrating an NC. *Id.* at 3:9–11. Dancs teaches that ROM 202 in the NC stores a "root authority" or "root public key" used for authentication with the ISP. *Id.* at 8:19–35, 52–63.

6. Monsen (Ex. 1009)

Monsen discloses a "file system for nonvolatile memory media." Ex. 1009, Abstract. This file system includes a software "common set of software functions," or "file system manager" to perform various functions, including opening, reading from, writing to, closing, and removing files. *Id.* at 6:1–17.

C. OBVIOUSNESS ANALYSIS

1. Claims 1–6, 11, and 13

Petitioner asserts that claims 1–6, 11, and 13 are obvious over Silvester and Hamlin either alone or in combination with other references. Pet. 3–4. For the reasons explained below, we find, on the current record, Petitioner has not shown a reasonable likelihood that it would prevail in its challenge to claims 1–6, 11, or 13.

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

Claim 1 (and by dependence claims 2–6 and 11) requires that "the secure data partition contains a master authority record" and that "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. According to Petitioner, Hamlin discloses the claimed master authority record by disclosing an administrator, who would necessarily have the claimed abilities and access permissions. Pet. 22–23. Petitioner asserts that the administrator's password is a specific example of the claimed master authority record. *Id.* at 23. According to Petitioner, it would have been obvious to include Hamlin's administrator capabilities

because "the inability to add or delete users to the system severely hampered [an administrator's] abilities to administer the system (allowing security threats to retain access or prevent access by cleared individuals)." Pet. 23. We disagree with Petitioner's argument for two reasons.

First, a password, by itself, does not disclose "access permissions according to the master authority record" because, while a password is information used to authenticate a user, a password does not have information about what access an authenticated user has. Further, we agree with Patent Owner that "Hamlin does not disclose that the master authority record is stored in a security partition on the storage device, as required in the '020 Patent." Prelim. Resp. 34. The cited portions of Hamlin recite a disk drive, not a secure partition. Pet. 23 (citing Ex. 1006, 5:2–7). Although Petitioner's proffered rationale for combining Hamlin—i.e., the need to add and delete users—explains why one skilled in the art would want Hamlin's administrator capabilities, it does not explain why it would be obvious to place Hamlin's administrator password within the secure data partition, as claim 1 requires. Given this deficiency, we find that Petitioner has not produced the required "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007).

Claims 2–6 and 11 depend ultimately from claim 1. Petitioner's analysis for these claims does not remedy the deficiencies explained above for claim 1. Similar to claim 1, claim 13 recites "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." Ex. 1001, 14:27–30. Petitioner's analysis of this limitation does not overcome the deficiencies noted above with respect to the authority record

limitation. *See* Pet. 36. Therefore, on this record and for purposes of this Decision, Petitioner has not shown a reasonable likelihood that it would prevail in establishing claims 1–6, 11, or 13 would have been obvious over the asserted prior art.

2. Claims 7–10

Petitioner asserts that independent claim 7 would have been obvious over a combination of Silvester, Hamlin, and Dancs (Pet. 46), or alternatively, over a combination of Silvester, Hamlin, Dancs, and Kadooka (*id.* at 53). For the reasons explained below, we find, on the current record, Petitioner has not shown a reasonable likelihood that it would prevail in its challenge to claim 7 or claims 8–10, which depend from claim 7.

b. "root assurance in the storage device"

Petitioner asserts that a combination of Silvester and Dancs renders obvious claim 7's limitation requiring "a root assurance in the storage device." *Id.* at 50; *see* Ex. 1001, 13:35–36. We disagree. The substance of Petitioner's argument is presented in more detail with Petitioner's claim 6 analysis. *See* Pet. 44–45. Claim 6 recites "a root assurance in the firmware of the device." Ex. 1001, 13:18–19. Claim 6 is dependent on claim 5, which specifies the firmware is "firmware of the storage device," *id.* at 13:15–16, and is dependent on claim 1, which lists firmware as a component of a "storage device," *id.* at 11:52–56. Thus, both claims 6 and 7 require the root assurance to be placed within the storage device. Petitioner maps the claimed "root assurance" to Dancs' "root public key." Pet. 45. However, in the cited portions of Dancs, the root public key is stored in ROM 202. Ex. 1008, 8:19–35. Dancs' Figure 2 illustrates ROM 202 as external to Dancs' analogous storage device, smart card 102. Petitioner does not propose a combination or modification to Dancs that would place Dancs' root public

key in the smart card storage device as claim 7 requires. The existence of the root public key, and even the desirability of a root public key in ROM, is not sufficient to render obvious the claimed root assurance *in the storage device*. In addition, Petitioner's proffered rationale for combining Dancs' root public key with Silvester—"to improve the security of Silvester's storage device by ensuring the authenticity of the encrypted data that is stored in the storage device," Pet. 45—does not explain sufficiently why one skilled in the art would place Dancs' root public key in Silvester's storage device, as opposed to externally as in Dancs.

Petitioner's alternative inclusion of Kadooka in its prior art combination does not remedy this deficiency related to a root assurance in the storage device. *See* Pet. 53. Claims 8–10 depend ultimately from claim 7. Petitioner's analysis for these claims does not remedy the deficiency explained above for Petitioner's claim 7 challenge. Therefore, on this record and for the purposes of this Decision, Petitioner has not shown a reasonable likelihood that it would prevail in establishing claims 7–10 would have been obvious over the asserted prior art.

3. Claims 12 and 14

Because claims 12 and 14 recite neither a "master authority record" nor a "root assurance in the storage device," Ex. 1001, 14:14–26, 31–34, the Petition's deficiencies addressed above do not impact Petitioner's analysis for these two claims. Based on Petitioner's analysis, *see* Pet. 32–38, we find Petitioner has demonstrated a reasonable likelihood of prevailing on claims 12 and 14.

Under 35 U.S.C § 314, however, the Board is required to make "a binary choice—either institute review or don't." *SAS Institute Inc. v. Iancu*, 138 S. Ct. 1348, 1355 (2018). Thus, "if the PTAB institutes a trial, the

PTAB will institute on all challenges raised in the petition." USPTO "Guidance on the Impact of *SAS* on AIA Trial Proceedings" (April 26, 2018); *see also BioDelivery Scis. Int'1, Inc. v. Aquestive Therapeutics, Inc.*, 898 F.3d 1205, 1209 (Fed. Cir. 2018) (holding that *SAS* "requires institution on all challenged claims and all challenged grounds"). In exercising this discretion whether to institute review, we consider the number of claims and grounds that meet the reasonable likelihood standard. *Chevron Oronite Co. LLC v. Infineum USA L.P.*, Case IPR2018-00923, slip op. at 10–11 (PTAB Nov. 7, 2008) (Paper 9) (informative) ("*Chevron*"); *Deeper, UAB v. Vexilar, Inc.*, Case IPR2018-01310, slip op. at 41–43 (PTAB Jan. 24, 2019) (Paper 7) (informative) ("*Deeper*").

Here, Petitioner demonstrates a reasonable likelihood of prevailing on only two claims, or one partial ground, of its challenge to fourteen claims on seven total grounds. On this record, and based on the particular facts of this case, we find that instituting a trial with respect to all fourteen claims on all seven grounds, based on sufficient evidence and arguments directed to only two claims and a portion of one ground, would neither be conducive to "the efficient administration of the Office [and] the ability of the Office to timely complete proceedings," 35 U.S.C. § 316(b), nor would it "secure the just, speedy, and inexpensive resolution of every proceeding," 37 C.F.R. § 42.1(b). *See Chevron* at 11 (denial based on likelihood of prevailing on two out of twenty challenged claims); *Deeper* at 42–43 (denial of likelihood of prevailing on two claims under one ground out of twenty-three challenged claims under four grounds).

III. CONCLUSION

For the foregoing reasons, we find, on the current record, Petitioner has not set forth a reasonable likelihood on succeeding on any of the seven asserted grounds of unpatentability for claims 1–11 and 13. We further determine that because Petitioner has set forth a reasonable likelihood of succeeding on only two of fourteen challenged claims and on only a portion of one of seven asserted grounds, instituting a trial with respect to all fourteen claims and seven grounds is not an efficient use of the Board's time and resources.

Thus, we do not institute an *inter partes* review.

IV. ORDER

Accordingly, pursuant to 35 U.S.C. § 314, it is:

ORDERED that the Petition is denied as to the challenged claims of the '020 patent; and

FURTHER ORDERED that no *inter partes* review is instituted.

For PETITIONER:

David Hoffman
FISH & RICHARDSON P.C.
hoffman@fr.com

Martha Hopkins
LAW OFFICE OF S.J. CHRISTINE YANG
mhopkins@sjclawpc.com

For PATENT OWNER:

Cabrach Connor
CONNOR KUDLAC LEE PLLC
cab@connorleepllc.com

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