

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICRON TECHNOLOGY, INC.,
Petitioner,

v.

INNOVATIVE MEMORY SYSTEMS, INC.,
Patent Owner.

Case IPR2016-00326
Patent 6,324,537 B1

Before KARL D. EASTHOM, JAMES B. ARPIN, and
KEVIN W. CHERRY, *Administrative Patent Judges*.

CHERRY, *Administrative Patent Judge*.

DECISION
Granting Patent Owner's Request for Rehearing
37 C.F.R. § 42.71(d)

Amended Institution of *Inter Partes* Review
35 U.S.C. § 314(a) and 37 C.F.R. § 42.108

On June 17, 2016, Patent Owner filed a Request for Rehearing (Paper 13, “Request” or “Reh’g Req.”) of our Decision to Institute (Paper 10, “Decision”) an *inter partes* review in this case. We have reviewed Patent Owner’s Request, and we agree that we overlooked the matters identified in the Request. *See* Reh’g Req. 2–4. Thus, for the reasons stated in the Request, we *grant* Patent Owner’s Request for Rehearing. On rehearing, we *withdraw* our previous Decision and *reconsider* our Decision in light of the full record, as Patent Owner requests. *Id.* at 4. Pursuant to this reconsideration, we issue the instant Amended Decision to Institute.

I. INTRODUCTION

Micron Technology, Inc. (“Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting an *inter partes* review of claims 1, 2, and 13 of U.S. Patent No. 6,324,537 B1 (“the ’537 patent,” Ex. 1001). Pet. 1. Innovative Memory Systems, Inc. (“Patent Owner”) filed a Preliminary Response (Paper 8, “Prelim. Resp.”). Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted “unless . . . the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.”

Upon consideration of the Petition and Preliminary Response, we determine that the information presented shows there is a reasonable likelihood that Petitioner would prevail in establishing the unpatentability of at least one of claims 1, 2, and 13 (“the challenged claims”) of the ’537 patent.

A. Related Matters

According to the parties, the '537 patent is at issue in a co-pending lawsuit: *Innovative Memory Sys., Inc. v. Micron Tech., Inc.*, 14-cv-1480 (D. Del. 2014). *See* Pet. 1, Paper 5, 1.

Petitioner filed a number of other petitions challenging the patentability of certain subsets of claims in the following patents owned by Patent Owner: (1) U.S. Patent No. 6,169,503 B1 (Case IPR2016-00320); (2) U.S. Patent No. 7,045,849 B2 (Case IPR2016-00322); (3) U.S. Patent No. 7,495,953 B2 (Case IPR2016-00323); (4) U.S. Patent No. 7,886,212 B2 (Case IPR2016-00324); (5) U.S. Patent No. 7,000,063 B2 (Case IPR2016-00325); (6) U.S. Patent No. 7,085,159 B2 (Case IPR2016-00327); and (7) U.S. Patent No. 6,901,498 B2 (Case IPR2016-00330). *See* Pet. 2–3.

B. The '537 Patent

The '537 patent is titled “Device, System, and Method for Data Access Control,” and issued November 27, 2001. Ex. 1001, at [54], [45]. The '537 patent generally relates to an access control device that controls all access to data stored in an electronic data storage device, according to various types of permissions. Ex. 1001, 2:30–36. The '537 patent explains that, although prior art software-based and operating system-based approaches implemented access controls, such approaches are subject to hacking by unauthorized users. *Id.* at 1:34–60. In addition, the '537 patent explains that such software-based and operating system-based systems have the disadvantage that, if the data storage device itself was stolen, the data typically becomes completely unprotected and subject to access by unauthorized users. *Id.* at 1:60–64. The '537 patent contends that the prior art systems cannot overcome these problems because those systems are

stored and implemented separately from the storage device. *Id.* at 1:64–67. The '537 patent proposes a solution to these problems that does not rely on separately stored programs to control access to data stored on the electronic storage device. *Id.* at 2:8–16.

The '537 patent describes enabling various types of permissions to be set for determining access to stored data, such that if an attempt is made to access particular data that does not have a suitable permission type, access is denied. *Id.* at 2:30–36. Figure 1 of the '537 patent is reproduced below.

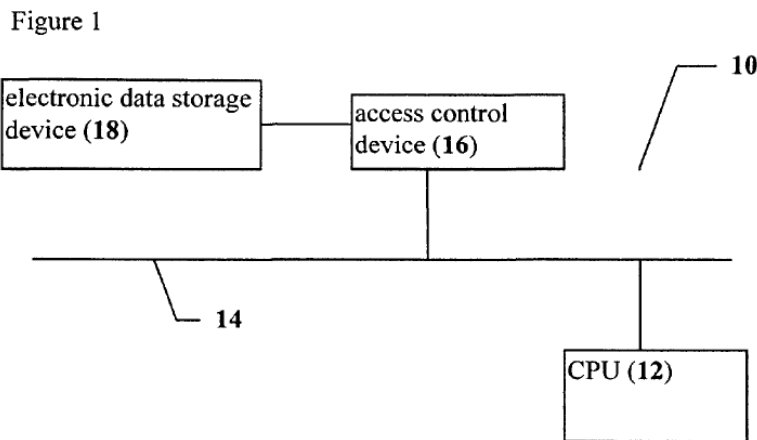


Figure 1 is a schematic block diagram showing an exemplary system according to the alleged invention for controlling data access. *Id.* at 5:23–25. Figure 1 shows system 10 featuring CPU 12 for executing instructions, such as, a request to read data. *Id.* at 5:25–27. CPU 12 is connected to bus 14. *Id.* at 5:27–28. Access control device 16 is connected to bus 14, such that access control device 16 is in communication with CPU 12 through bus 14. *Id.* at 5:28–31. Data storage device 18 is in communication with access control device 16, such that any attempts to access data in data storage device 18 must pass through access control device 16. *Id.* at 5:34–38.

The '537 patent explains that, “[r]egardless of the type of implementation of the device of the present invention,” an “important feature” of the alleged invention is that it allows a plurality of different types of access to be combined in a single storage device. *Id.* at 4:65–5:1. The '537 patent states that the prior art generally is “restricted to a single type of data access,” but the “present invention is flexible and is able to store data according to several different access types within a single device.” *Id.* at 5:1–6. According to the Specification, the “permission” can be stored in the electronic storage device or the access control device, among other places. *Id.* at 5:6–12, 6:43–48. For example, the type of data access could be appended to the data in the electronic storage device, so that the data access is defined according to a “soft,” data-based definition:

[T]he present invention may optionally determine the type of data access according to information which is appended to the stored data, such that the type of data access is defined according to a “soft”, databased definition, rather than according to a “hard” definition which is implemented only in the hardware itself.

Id. at 5:6–12.

The '537 patent further explains that:

[a]s an example, one type of permission could be a standard read and write permission, but with write protection, such that access control device 16 would permit data to be read from data storage device 18, but would block an attempt to write data to data storage device 18. If such a permission is to be stored in an abbreviated code, the code for this particular type of permission could be given as “R/W/WP”, for example. Such a code could optionally be stored in the non-volatile memory of access control device 16, for example. However, the permission is such that it could be changed to permit such write access, or a read and write permission with no write protection, with a code as follows: R/W/NP. These standard types of read and write permissions are

often used for hard disks, floppy diskettes and other storage media, for example.

Id. at 6:34–53.

C. Illustrative Claim

Of the challenged claims, claim 1 is independent. Claims 2 and 13 depend from claim 1. Illustrative claim 1 is reproduced below:

1. A system for controlling access to stored data, the stored data having at least one associated type of permission, the system comprising:
 - (a) an electronic data storage device for storing the stored data and information appended to the stored data, said appended information featuring said at least one associated type of permission for accessing the stored data; and
 - (b) an access control device for controlling access to said electronic data storage device, such that the stored data is only accessed through said access control device, and such that said access control device determines access to the stored data according to at least one said associated type of permission.

Ex. 1001, Certificate of Correction.

D. Evidence Relied Upon

Petitioner relies upon the following prior art references:

Anderl US 4,816,653 Mar. 28, 1989 Ex. 1005

M. HENDRY, SMART CARD SECURITY AND APPLICATIONS (1997) (Ex. 1006).

Petitioner also relies upon the Declaration of R. Jacob Baker, Ph.D., dated January 26, 2016 (“Baker Decl.”). Ex. 1003.

E. Asserted Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability:

Reference(s)	Basis	Challenged Claim(s)
Anderl	§ 102(b)	1 and 13
Anderl	§ 103(a)	1 and 13
Anderl and Hendry ¹	§ 103(a)	2

II. ANALYSIS

A. Claim Interpretation

In an *inter partes* review, the Board construes claims by applying the broadest reasonable interpretation in light of the specification. 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, No. 15-446, 2016 WL 3369425, at *10–14 (U.S. June 20, 2016). Under this standard, absent any special definitions, claim terms or phrases are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art, in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

“said appended information featuring said at least one associated type of permission for accessing the stored data”

Neither party proposes an explicit construction for this claim limitation. Patent Owner contends, however, that for “said appended information” to “feature[e]” an “associated type of permission” that information must “represent the types of actions that can actually be

¹ The Petition lists two grounds based on Anderl and Hendry. Although they use slightly different reasoning, we consider them as a single ground.

performed.” Prelim. Resp. 13. Patent Owner also asserts that merely because a “specific type of action may be *associated* with [information appended]” that is not sufficient to teach this limitation because such types of action are “not a prominent and conspicuous part of the [information appended], and therefore not ‘featured’ by the appended information.” *Id.* at 14. Petitioner’s implicit construction would not require that the appended information actually represent a permission or that the specific type of action be “a prominent and conspicuous part” of the data itself. *See* Pet. 23–24.

At this preliminary stage, there does not appear to be a dispute about what the “said appended information” is. Patent Owner contends there also does not appear to be a dispute as to what “type of permission” means. Prelim. Resp. 11. In particular, Patent Owner argues that the parties agree that “type of permission” is the type of action that can be performed with respect to the stored data, e.g., reading or writing. *Id.* at 11–12. Instead, Patent Owner focuses its claim construction arguments on what “featuring” requires. *Id.* at 13–15.

As an initial matter, despite the parties’ apparent agreement, we are not persuaded that “type of permission” is limited to only the type of action that can be performed, e.g., reading or writing, with respect to the data. Instead, the Specification repeatedly refers to the “*types* of permissions” as “for determining access to the stored data, such that if an attempt is made to access particular data which does not have a suitable permission type, access is denied.” *See, e.g.*, Ex. 1001, Abstract (“The device, method and system enable various types of permissions to be set for determining access to the stored data, such that if an attempt is made to access particular data which does not have a suitable permission type, access is denied.”); 2:32–36 (“The

present invention enables various types of permissions to be set for determining access to the stored data, such that if an attempt is made to access particular data which does not have a suitable permission type, access is denied.”); 3:4:26–30 (same). Given this broader usage in the Specification, for purposes of this decision, the “type of permission” is for determining access to the stored data, such that if an attempt is made to access particular data that does not have a suitable permission type, access is denied. The access, if not denied, may include reading from or writing to the stored data.

As for “featuring,” we are not persuaded that “featuring,” as used in claim 1 of the ’537 patent is synonymous with “represent,” as Patent Owner contends. A relevant meaning of “featuring” is “to be an important part or aspect of something.” *See* Ex. 3001. This meaning only requires that the thing that is featured be an important part or aspect, not that it correspond to or represent the thing. Patent Owner does not point us to any disclaimer or definition that would limit this meaning. *See* Prelim. Resp. 13–15. Instead, the Specification appears to use the related term “feature” in this ordinary sense. *See, e.g.,* Ex. 1001, 4:54–56 (“As another option, the device may feature a single chip with a microprocessor and firmware for operating the data access features”); 5:25–27 (“A system 10 features a CPU 12 for executing instructions....”); 8:15–19 (“For example, an access control code could be implemented with a combination of different types of data, each of which could again feature a separately selected and assigned data access permission, which optionally and preferably is different for each portion of the data.”). Moreover, the portion of Specification cited by Patent Owner (Prelim. Resp. 12–13 (citing Ex. 1001, 6:34–61)) makes clear that it only

refers to a preferred embodiment and the permissions do not need to be stored as a “code,” i.e., specific information or data representing the permission. *See id.* at 6:35–36 (“According to preferred embodiments...”), 6:43–47 (“*If* such a permission is to be stored in an abbreviated code, the code for this particular type of permission *could be given* as ‘R/W/WP’, *for example*. Such a code *could optionally* be stored in the non-volatile 16, *for example*.” (emphases added)). Such optional language is not sufficient to limit the claimed “appended information” to only something that “represents” the permission, such as a code. *See Prolitec Inc. v. Scentair Techs., Inc.*, 807 F.3d 1353, 1358 (Fed. Cir. 2015) (“[T]he use of ‘may’ signifies that the inventors did not intend to limit [the claim]. . . .”); *Ancora Techs., Inc. v. Apple, Inc.*, 744 F.3d 732, 735 (Fed. Cir. 2014) (noting that non-limiting examples are not sufficient to redefine a term).

We also have reviewed the prosecution history to determine if it sheds any further light on the meaning of “featuring.” *See Microsoft Corp. v. Proxyconn, Inc.*, 789 F.3d 1292, 1298 (Fed. Cir. 2015) (“The PTO should also consult the patent’s prosecution history in proceedings in which the patent has been brought back to the agency for a second review.”). The prosecution history does not persuade us that “featuring,” as recited in this limitation, is limited to data actually “representing” the permission. The only discussion we have located in the prosecution history of the “featuring” language was when application claim 26, which included this limitation, was added. Ex. 1002, 69. In adding this new claim, Applicants contended that this limitation was “clearly described” on page 5, lines 9–13, of the Specification, as filed. *Id.* This discussion is identical to the column 5, lines 6–12, of the Specification of the ’537 patent quoted above. This passage

merely states that the permissions are determined by the data stored, not defined only in the hardware itself. *See* Ex. 1001, 5:6–12 (“[S]uch that the type of data access is defined according to a ‘soft’, databased definition, rather than according to a ‘hard’ definition which is implemented only in the hardware itself.”). This statement does not support the narrow definition that Patent Owner proposes.

Thus, we determine, on the present record, that “said appended information featuring said at least one associated type of permission for accessing the stored data” requires that the appended information be an important part or aspect of the type of permission, where the “type of permission” is for determining access to the stored data, such that, if an attempt is made to access particular data that does not have a suitable permission type, access is denied.

Remaining Terms

On this record at this preliminary stage, we see no need to construe other claim terms expressly. *See, e.g., Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (only those claim terms or phrases that are in controversy need to be construed, and only to the extent necessary to resolve the controversy).

B. Alleged Anticipation of Claims 1 and 13 by Anderl

Petitioner contends that claims 1 and 13 are anticipated by Anderl. Pet. 18–30. To support its contentions, Petitioner provides explanations as to how the prior art discloses each claim limitation. *Id.* Petitioner also relies upon the Baker Declaration (Ex. 1003) to support its positions. At this stage of the proceeding, we are persuaded by the Petitioner’s explanations and supporting evidence.

1. Anderl (Ex. 1005)

Anderl is titled “Security File System for a Portable Data Carrier,” and generally relates to a system for securing data containing in portable data carriers having electrical memories for storing data. Ex. 1005, at [54], 1:7–11. Figure 1 of Anderl is reproduced below.

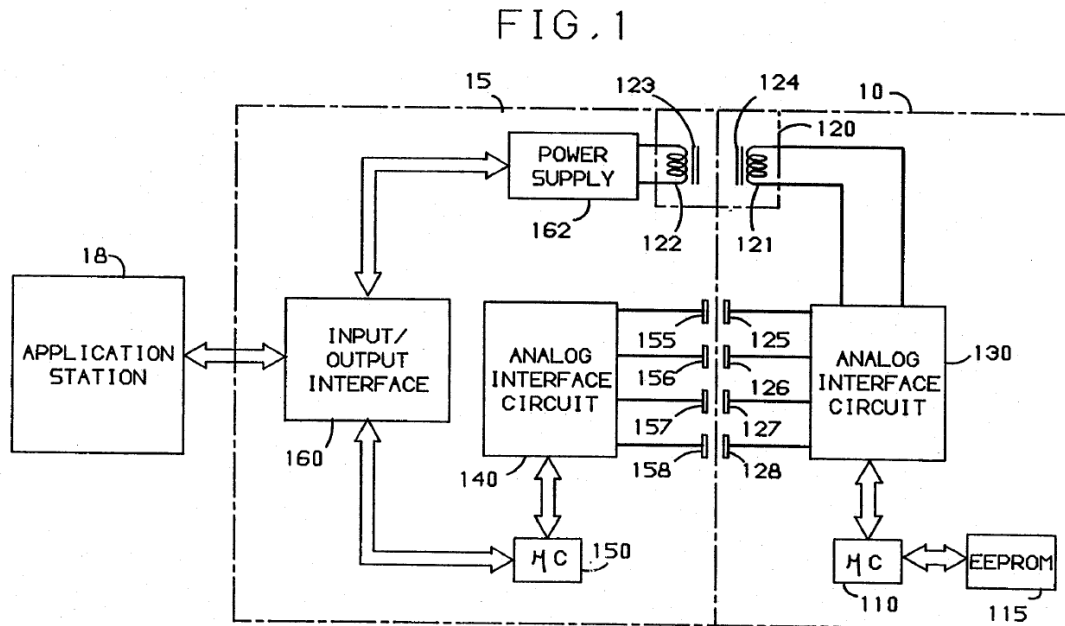


Figure 1 is a functional block representation of the major functional components of a portable data carrier system and their general interconnections with each other. *Id.* at 2:47–50. As shown in detail in Figure 1, Anderl describes a portable data carrier system consisting of three main subsystems: (1) portable data carrier or card 10, which contains a memory capable of storing and updating information for a user; (2) card reader/writer 15; and (3) station 18, which is linked to card 10 by card reader/writer 15. *Id.* at 3:19–26. Station 18 is a suitably configured application station that runs application software necessary for accessing the memory in the card. *Id.* at 3:26–30. The application software resides in the

station and enables the retrieval and modification of information stored in the memory of card 10. *Id.* at 3:30–32. Card 10 includes microcomputer 110, electrical erasable programmable read-only memory (EEPROM) 115, analog interface circuit 130, secondary winding 121 of transformer 120, and capacitive plates 125 through 128. *Id.* at 3:38–43. Microcomputer 110 includes a central processing unit and memory units in the form of random-access memory and read-only memory. *Id.* at 3:44–46. Anderl explains that by operating under firmware control provided by its internal read-only memory, microcomputer 110 formats data that is transferred directly to the EEPROM 115 and via the reader/writer 15 to the station 18. *Id.* at 3:49–53. Microcomputer 110 also interprets commands from station 18 received through reader/writer 15. *Id.* at 3:55–57. Anderl describes that the entire EEPROM or a portion of it may be an integral part of the microcomputer, or it may be a separate element. *Id.* at 3:53–55.

Anderl also describes how, by using six different security levels, Anderl's card system provides security protection for the card file system and the card commands. *Id.* at 5:18–21. Anderl explains that users do not need to fear the consequences of misappropriation of the card because the card requires a user to identify himself or herself by means of a password before allowing access to files, other than those at the public level. *Id.* at 6:9–19. Figure 2 of Anderl is shown below:

FIG. 2

SECURITY LEVEL	USER
6	DEVELOPER
5	SUPER USER (FACTORY)
4	MASTER ISSUER (OWNER)
3	SUB ISSUER
2	USER (CARD HOLDER)
1	PUBLIC (CARD OWNER INFO) (MEDICAL DATA)

Figure 2 of Anderl shows the six security levels available in Anderl. *Id.* at 5:29–6:8.

Figure 4 of Anderl is reproduced below.

FIG. 4

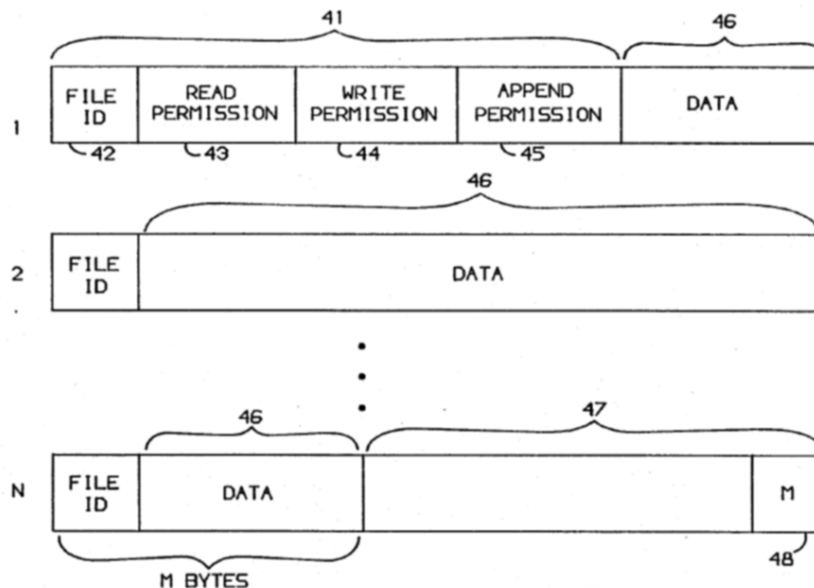


Figure 4 illustrates the three sections of each data file stored in the portable data carrier system. *Id.* at 2:56–58. Anderl explains that the file includes prefix section 41, which is located in the first record of each file and contains the file identification number 42 and protection bytes 43, 44, and

45. *Id.* at 6:55–60. Protection bytes 43 through 45 specify the file permissions. *Id.* at 6:65–66. First byte 43 represents read permission designating the minimal level at which the file may be read, and second byte 44 represents read/write permission designating the minimal level at which the file may be both read and written. *Id.* at 6:66–7:2. Thus, the read permission for a file is separable from read/write permission for a file. *Id.* at 7:3–4. Different security levels also may be specified for the read versus the read/write access. *Id.* at 7:4–6. Protection byte 45 may be set to implement an “append-only” mode that permits the user to only add data to a file, but not overwrite existing data. *Id.* at 7:38–41. Records reflecting the appropriate application file are created for accepting this data as it is entered. *Id.* at 7:41–43. Thus, a file may be designated for read/append permission as well as read/write permission. *Id.* at 7:43–45.

Also, information section 46 of a file contains the actual data located in each record of that file. *Id.* at 7:46–47. Suffix section 47 has number M in last byte 48 of last record N, which indicates the number of application data bytes in that last record. *Id.* at 7:47–50.

The executive operating system on the card is accessed by the normal security class levels through use of the commonly understood command primitives. *Id.* at 7:51–54. These command primitives control the security access for the card, file creation and access, and also administrative and testing activities. *Id.* at 7:54–56. Operation of these command primitives may be illustrated through a description of the operation of the “login” command. *Id.* at 7:59–61. In order to log into the card, the user is required to specify a login level and a password. *Id.* at 7:61–62. This password is “checked internally by the card algorithmically against the appropriate

password at the same login level in the card header.” *Id.* at 7:62–65. If a card user is attempting to gain access to a file with a login level lower than that required by the file, permission to open the file either for read or for read/write is denied. *Id.* at 7:65–67.

2. Analysis

As noted above, Petitioner asserts that Anderl anticipates claims 1 and 13. *See* Pet. 18–30. With respect to the preamble of claim 1, Petitioner asserts that Anderl discloses the recited “system for controlling access to stored data, the stored data having at least one associated type of permission.” Pet. 17–21 (citing Ex. 1005, Fig. 1 (showing data storage card and associated circuitry)), 3:38–43, 3:49–53, 3:58–62, Fig. 4 (showing permissions associated with stored data), 1:53–57, 6:39–7:10, 7:14–27, 7:38–52); Ex. 1003, 34–46. Petitioner relies on Anderl’s smart card that includes an EEPROM as disclosing the “electronic data storage device for storing the stored data,” as recited in claim 1. Pet. 21 (citing Ex. 1005, Fig. 1 (showing data storage card with EEPROM), 3:38–43, 3:49–53, 3:58–62); Ex. 1003, 47–49.

As for the requirement that there be “information appended to the stored data” of claim 1, Petitioner asserts that Anderl’s description that the EEPROM can store files that include data and protection bytes where the protection bytes are appended to the stored data accounts for this limitation. Pet. 22 (citing Ex. 1005, Fig. 4 (showing appended permissions for accessing the stored data and the stored data), 1:53–57, 6:39–7:10, 7:14–27, 7:38–52); Ex. 1003, 52–53.

Petitioner further submits that Anderl discloses that the appended information features at least one associated type of permission for accessing

the stored data, as recited in claim 1. *Id.* at 23–24. In particular, Petitioner submits that Anderl discloses that the protection bytes can specify different types of permissions, such as read, write, or append permissions, for accessing the stored data. *Id.* at 23 (citing Ex. 1005, 5:18–27, 6:65–7:10, 7:14–27, 7:38–45, Fig. 4). Petitioner also contends that the read permissions of Anderl can designate the minimum security level at which the file may be read. *Id.* (citing Ex. 1005, 6:66–68). Petitioner further asserts that the appended protection byte also could include a requirement for an optional password before access to the file is allowed. *Id.* at 23–24 (citing Ex. 1005, 7:15–18, 7:62–67). Petitioner explains that Anderl discloses that if a user attempts to access a file with a login level lower than that required by the file, access will be denied, but if a user attempts to access the file with a higher login level than required, access to the file will be granted. *Id.* at 24 (citing Ex. 1005, 6:9–19, 7:27–45, 7:59–68).

Petitioner relies on Anderl’s microcomputer 110 on card 10 in Figure 1, which runs an operating system that controls access to EEPROM 115 and is the only way to access EEPROM 115, to disclose “an access control device for controlling access to said electronic data storage device, such that the stored data is only accessed through said access control device,” as recited in claim 1. Pet. 24–26. In particular, Petitioner asserts that, as Figure 1 demonstrates, microcomputer 110 is the only way to access data on EEPROM 115. Pet. 24–25. Petitioner further asserts that microcomputer 110 runs an operating system stored on a Read Only Memory (ROM) on card 10. *Id.* at 25 (citing Ex. 1005, 1:68–2:10, 3:33–37, 3:44–57, 7:54–56; Ex. 1003 ¶ 53). Petitioner contends that operating system includes a set of command primitives that may be sent from the station,

microcomputer 110 interprets those operating system command primitives, and those command primitives control security access for the files on the EEPROM. *Id.* at 25–26 (citing 3:49–57, 7:54–56). Petitioner points to the example where a password is sent to the card via these command primitives, the microcomputer interprets these commands, and, based on the commands, the microcomputer will deny access to the stored data if the appropriate password required by the file is not entered. *Id.* at 26 (citing Ex. 1005, 1:68–2:12, 3:55–57, 5:24–27, 6:15–54, 6:65–7:10, 7:14–27, 7:38–45, 7:51–68, 8:17–19, 8:28–40).

As for the recitation in claim 1 that the access control device determines access to the stored data according to the associated type of permission, Petitioner relies on Anderl’s disclosure that the microcomputer running the operating system grants access to data based on both the login level and the protection bytes in the file. Pet. 26–29 (Ex. 1005, 2:20–22, 3:49–57, 7:51–56, 7:59–68). Petitioner notes that, as discussed above, the microcomputer running the operating system controls access to the stored data on the smart card. *Id.* at 27 (citing Ex. 1005, 7:54–55, 2:6–10, 3:33–43, 3:49–57, 7:59–68). Petitioner asserts that Anderl discloses that there can be six different security levels (login levels) on the card. *Id.* (Ex. 1005, 2:13–26, 5:18–27). Petitioner further asserts that the respective files on the cards have protection bytes indicating what security level can access the respective file for each type of permission. *Id.* (citing Ex. 1005, 6:65–7:10, 7:14–27, 7:38–45, Fig. 4). Petitioner argues that, if a user attempts to gain access to a file with a login level lower than that required by the file, permission to open that file is denied. *Id.* at 28 (citing 7:65–68). Petitioner further submits that each permission (e.g., read permission and write permission) can require a

different security level, and the microcomputer controls access separately for each type of permission. *Id.* (citing 7:3–10).

With respect to the limitations not disputed by Patent Owner and discussed below, we determine that Petitioner has shown sufficiently that Anderl discloses these limitations.

In its Preliminary Response, Patent Owner argues that Anderl fails to disclose “said appended information featuring said at least one associated type of permission for accessing the stored data,” as recited in independent claim 1. Prelim. Resp. 11–15. Patent Owner contends that the parties do not appear to dispute that “type of permission” should be construed as “the type of action that may be performed with respect to the stored data, e.g., read, write, append.” *Id.* at 11 (citing Pet. 20–21, 23). Patent Owner submits that this construction is consistent with the use of the term “permission” in the Specification of the ’537 patent. *Id.* at 11–13 (citing Ex. 1001, 6:34–61). Patent Owner argues that, under this construction, the protection bytes of Anderl do not feature the types of permissions, such as read, write, and append, as required by claim 1. *Id.* at 13. Patent Owner asserts that the appended protection bytes in Anderl only include values representing the levels of security that are required before those actions can be performed. *Id.* Thus, Patent Owner contends that the protection bytes of Anderl do not include values that represent the types of actions that can be performed. *Id.*

Patent Owner further argues that under this understanding of Anderl, the protection bytes of Anderl do not “feature” the type of permission, in the sense that the actual actions that may be performed, such as read, write, and append, are any part of the protection bytes. *Id.* at 14. Patent Owner submits that the specific type of action may be associated with the protection

bytes, but it is not “featured” by the appended information. *Id.* Patent Owner asserts that, in the ’537 patent, the appended information is not merely associated with the particular type of action that may be performed, as are the protection bytes in Anderl, but rather, the appended information actually *represents* the types of actions that may be performed. *Id.* at 14–15. Patent Owner contends that the advantage of the ’537 patent is the ability to freely manipulate and change the types of actions that may be performed with respect to the stored data. *Id.* at 15. Patent Owner argues that Anderl, by contrast, only allows the security levels necessary to perform certain predetermined actions, but not the actions themselves, to be changed. *Id.*

Patent Owner submits that the appended information in Anderl features only the user’s level of security required to perform a particular action with respect to the stored data. *Id.* Patent Owner argues that Anderl’s appended information is completely user dependent, while the ’537 patent is completely independent of the user. *Id.*

On this record and based on our preliminary construction of this claim limitation, we are persuaded that Petitioner has shown adequately that Anderl discloses “said appended information featuring said at least one associated type of permission for accessing the stored data,” as recited in claim 1. Patent Owner focuses narrowly on the value of the data included in protection bytes 43 to 45 of Anderl. *See* Prelim. Resp. 13–15. Yet the claim does not focus only on the data alone, but instead recites “appended information.” As the Petition explains, Anderl discloses that the information is appended based on location in file as the value at the particular location. *See* Pet. 23–24. In particular, Anderl discloses that each file includes prefix section 41 that is located in the first record of each file and contains file

identification number 42 and protection bytes 43, 44, and 45. Ex. 1005, 6:57–60. Anderl states that “[t]he protection bytes 43 through 45 *specify* the file permissions.” *Id.* at 6:65–66 (emphasis added). As Anderl discloses,

[t]he first byte 43 represents read permission designating the minimal level at which the file may be read, and the second byte 44 represents read/write permission designating the minimal level at which the file may be both read and written into. Thus read permission for a file is separable from read/write permission for a file. Different security levels may also be specified for the read verses the read/write access. For example, the read permission for a file may be at PUBLIC level allowing public access to public information, but the write permission could be specified at USER level which prohibits writing to the file without the user’s consent.

Ex. 1005, 6:66–7:10.

On this record, Petitioner has shown sufficiently that the “information” in Anderl, comprised of the position and the value stored at that position, can be set to one of six values (shown in Figure 2 of Anderl), which is an important part or aspect, of determining access to the stored data, such that if an attempt is made to access particular data that does not have a suitable permission type, access is denied. For example, if a user makes an attempt to read certain data that is above his or her security level found in the corresponding protection byte for reading, access then is denied. Accordingly, on this record, this showing is sufficient to demonstrate a reasonable likelihood that that Anderl discloses this limitation, as we have construed it.

Patent Owner also makes certain arguments that the appended information must be “user independent.” Prelim. Resp. 15. We do not discern any such limitation in the claim or the requirement of “user

independence” in the Specification. Thus, we do not find these arguments persuasive because they are not commensurate with the scope of the claim.

Based on the current record, Petitioner has demonstrated a reasonable likelihood that it would prevail in showing that independent claim 1 is anticipated by Anderl.

Dependent claim 13 depends from claim 1 and additionally recites “said access control device is integrated with said electronic data storage device.” Petitioner relies on Anderl’s disclosure that the microcomputer that controls access to the data is on the same smart card as the EEPROM. Pet. 29 (citing Ex. 1005, 1:53–66, 3:38–43, Fig. 1). Petitioner also notes that Anderl discloses that the EEPROM can be an “integral part of the microcomputer.” *Id.* at 30 (quoting Ex. 1005, 3:53–54). For the remainder of the limitations, Petitioner relies the disclosures that were discussed above with respect to claim 1. *Id.* at 29. Patent Owner does not raise any separate argument regarding the remaining limitations at this time, apart from those considered above with respect to claim 1. Prelim. Resp. 16.

Petitioner’s showing at this stage is sufficient. Based on the record before us, Petitioner has demonstrated a reasonable likelihood that it would prevail in showing that claim 13 is anticipated by Anderl.

Accordingly, based on the present record, we are persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing in showing that claims 1 and 13 are anticipated by Anderl.

C. Alleged Obviousness of Claims 1 and 13 over Anderl

Petitioner contends that claims 1 and 13 are unpatentable as obvious over Anderl. Pet. 30–35. To support its contentions, Petitioner provides explanations as to how the prior art teaches or suggests each claim

limitation. *Id.* Petitioner also relies upon the Baker Declaration (Ex. 1003) to support its positions. At this preliminary stage, we are persuaded by the Petitioner's explanations and supporting evidence.

With respect to Petitioner's contentions that claim 1 would have been obvious over Anderl, Petitioner relies on its citations and analysis from its anticipation analysis for all of the limitations of claim 1, except for the requirement for "an access control device for controlling access to said electronic data storage device, such that the stored data is only accessed through said access control device." *See* Pet. 30–34. For that limitation, Petitioner argues that Anderl renders obvious such an access control device. *Id.* at 32. In particular, Petitioner submits that, if we do not find that Anderl expressly discloses that the EEPROM is accessed only through the microcomputer, it would have been obvious to have the microcomputer of Anderl control access to the EEPROM, such that the stored data is only accessed through the microcomputer. *Id.* Petitioner submits that Anderl explicitly discloses that the operating system command primitives, which the microcomputer interprets, control security access and manipulate the files. *Id.* at 33 (citing Ex. 1005, 2:6–10, 3:33–37, 7:51–56, 7:59–68). Moreover, Petitioner notes that Figure 1 does not show any other path to the data stored on the EEPROM, except through the microcomputer. *Id.* Petitioner argues that making the microprocessor the sole access point to the EEPROM would have allowed security regardless of where the card was used, which is consistent with Anderl's goal of securing data. *Id.*

Finally, Petitioner also argues that, given Anderl's disclosure that the EEPROM could be "an integral part of the microcomputer," a person of ordinary skill would understand that the EEPROM could be on the same

chip as the microcomputer. *Id.* at 34 (citing Ex. 1003, App. A).

Petitioner submits that, in such a case, there would be no other interface to the EEPROM, except through the microcomputer as a practical matter, and, thus, it would be common sense that the only access to the EEPROM should occur through the microcomputer. *Id.*

Patent Owner does not raise any separate arguments challenging this ground, apart from those considered above with respect to the anticipation of claim 1. Prelim. Resp. 16.

Petitioner's showing at this preliminary stage is sufficient. Based on the current record, we are persuaded that Petitioner has demonstrated a reasonable likelihood that it would prevail in showing that independent claim 1 is obvious over Anderl.

With respect to dependent claim 13, Petitioner relies on the same disclosure discussed above with respect to the anticipation ground. Pet. 35. For the remainder of the limitations, Petitioner relies the disclosures that were discussed above with respect to claim 1 for the obviousness ground. *Id.* at 35.

Patent Owner does not raise any separate arguments challenging this ground, apart from those considered above with respect to the anticipation of claim 1. Prelim. Resp. 16.

Petitioner's showing at this stage is sufficient. Based on the current record, we are persuaded that Petitioner has demonstrated a reasonable likelihood that it would prevail in showing that claim 13 would have been obvious over Anderl.

D. Alleged Obviousness of Claim 2 over Anderl and Hendry

Petitioner contends that claim 2 is unpatentable as obvious over

Anderl and Hendry.² Pet. 35–40. To support its contentions, Petitioner provides explanations as to how the prior art discloses each claim limitation. *Id.* Petitioner also relies upon the Baker Declaration (Ex. 1003) to support its positions. At this preliminary stage, we are persuaded by the Petitioner’s explanations and supporting evidence.

Hendry

Hendry is a textbook titled *Smart Card Security Applications*. Ex. 1006, 1. Hendry describes the background and evolution of smart phone technology. Hendry notes that “[t]he most important aspect of the smart card . . . was the control of access to the card’s memory through the use of passwords and other internal mechanisms.” *Id.* at 47. Hendry explains that for “maximum security and true portability of data,” the smart card “must incorporate a microprocessor.” *Id.* at 54. Hendry states that, “[w]ith a microprocessor card, the data are never directly available to the external application”; instead “[t]hey must always pass through the microprocessor, which can carry on a dialogue with the application.” *Id.* at 54–55. Hendry notes that several IC manufacturers at that time produced single chips that included both the microprocessor and the memory. *Id.*

Analysis

Claim 2 depends from claim 1 and recites that “said electronic data storage device and said access control device are implemented on a single chip.” Petitioner argues that Anderl and Hendry render this limitation

² As noted above, Petitioner identifies this as the second obviousness ground with respect to claim 2, depending on whether Petitioner relies on its analysis that Anderl anticipates independent claim 1 or its analysis that Anderl renders independent claim 1 obvious.

obvious. Pet. 35–39. Petitioner contends that Anderl discloses that the smart card could be an “integral part of the microcomputer” (*id.* at 35 (citing Ex. 1005, 3:53–55)), and Hendry supplements that disclosure and teaches that many manufacturers produced such integrated cards (*id.* at 35–36 (citing Ex. 1006, 54–55)). Petitioner submits that a person of ordinary skill would have combined these disclosures because they address similar problems of providing security for data on smart cards, and that these were known methods that could have improved related devices with predictable results. Pet. 36–37 (citing Ex. 1005, 1:47–49, 1:53–57, Ex. 1006, 16, 54–55; Ex. 1003 ¶¶ 62, 63). Petitioner argues that a person of ordinary skill in the art would have been motivated to place the microcomputer and the EEPROM on the same chip as microprocessor and memory size decreased, and this would have provided an easier to use, more integrated solution. *Id.* at 37 (citing Ex. 1003 ¶ 64).

Petitioner relies in the alternative on its anticipation and obviousness analysis for independent claim 1 to account for the remaining limitations. *Id.* at 37, 39.

Patent Owner does not raise any separate arguments challenging this ground, apart from those considered above with respect to the anticipation of claim 1. Prelim. Resp. 17.

We have reviewed Petitioner’s citations and Petitioner’s showing at this stage is sufficient. Based on the current record, we are persuaded that Petitioner has demonstrated a reasonable likelihood that it would prevail in showing that claim 2 is unpatentable as obvious over Anderl and Hendry.

III. CONCLUSION

We determine that the information presented in the Petition demonstrates that there is a reasonable likelihood that Petitioner would prevail in challenging claims 1, 2, and 13 of the '537 patent are unpatentable. At this preliminary stage, we have not made a final determination with respect to the patentability or claim construction of these challenged claims.

IV. ORDER

Accordingly, it is

ORDERED that Patent Owner's Request for Rehearing is *granted*;

FURTHER ORDERED that our prior Decision to Institute is *withdrawn* and this Amended Decision to Institute is *substituted* in its place;

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(a) and 37 C.F.R. § 42.4, an *inter partes* review is hereby instituted on the grounds:

A. Claims 1 and 13 of the '537 patent are unpatentable under

35 U.S.C. § 102(b) as anticipated by Anderl;

B. Claims 1 and 13 of the '537 patent are unpatentable under

35 U.S.C. § 103(a) as obvious over Anderl; and

C. Claim 2 of the '537 patent is unpatentable under 35 U.S.C.

§ 103(a) as obvious over Anderl and Hendry;

FURTHER ORDERED that no other grounds are authorized for this *inter partes* review other than those specifically identified above; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial; the trial will commence on the entry date of this decision.

IPR2016-00326
Patent 6,324,537 B1

For PETITIONER:

Douglas W. McClellan
Jeremy Jason Lang
Weil, Gotshal & Manges LLP
doug.mcclellan@weil.com
jason.lang@weil.com

For PATENT OWNER:

Robert W. Morris
Philip E. Levy
Eckert Seamans Cherin & Mellott, LLC
rwmorris@eckertseamans.com
plevy@eckertseamans.com