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 IPR. No. **Unassigned**
U.S. Patent No. 6,324,537
Title: DEVICE, SYSTEM AND METHOD
FOR DATA ACCESS CONTROL

Petition For *Inter Partes* Review of U.S. Patent No. 6,324,537 Under 35 U.S.C. §§ 311-319 and 37 C.F.R. §§ 42.1-.80, 42.100-.123

***Mail Stop* "PATENT BOARD"**
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

Page

Exhibit List

Micron Exhibit #	Description
MICRON-1001	U.S. Patent No. 6,324,537 ("537 Patent")
MICRON-1002	File History for U.S. Patent No. 6,324,537
MICRON-1003	Declaration of Dr. R. Jacob Baker ("Baker Decl.")
MICRON-1004	*Curriculum Vitae* of Dr. R. Jacob Baker
MICRON-1005	U.S. Patent No. 4,816,653 ("Anderl")
MICRON-1006	M. Hendry, *Smart Card Security and Applications* (1997) ("Hendry")
MICRON-1007	J. M. Kaplan, *Smart Cards, The Global Information Passport* ("Kaplan")
MICRON-1008	M. Devargas, *Smart Cards & Memory Cards* ("Devargas")
MICRON-1009	U.S. Patent No. 4,105,156 ("Dethloff")
MICRON-1010	United States Copyright Office public record search result for M. Hendry, *Smart Card Security and Applications* (1997)
MICRON-1011	Declaration of Lisa Rowlison de Ortiz regarding M. Hendry, *Smart Card Security and Applications* (1997)

1. INTRODUCTION

Pursuant to 35 U.S.C. §§ 311-319 and 37 C.F.R. § 42.100, Micron Technology, Inc. ("Petitioner") hereby petitions the Patent Trial and Appeal Board to institute an *inter partes* review of claims 1, 2 and 13 of U.S. Patent No. 6,324,537, titled "Device, System and Method for Data Access Control" (MICRON-1001, the "537 Patent"), and cancel those claims as unpatentable.

2. REQUIREMENTS FOR PETITION FOR *INTER PARTES* REVIEW

2.1. Grounds for Standing (37 C.F.R. § 42.104(a))

Petitioner certifies that the 537 Patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting *inter partes* review of the challenged claims of the 537 Patent on the grounds identified herein.

2.2. Notice of Lead and Backup Counsel and Service Information

Pursuant to 37 C.F.R. §§ 42.8(b)(3), 42.8(b)(4), and 42.10(a), Petitioner provides the following designation of Lead and Back-Up counsel.

Lead Counsel	**Back-Up Counsel**
Douglas W. McClellan Registration No. 41,183 (doug.mcclellan@weil.com) Postal & Hand-Delivery Address: Weil, Gotshal & Manges LLP 700 Louisiana, Suite 1700 Houston, TX 77002 T: 713-546-5313; F: 713-224-9511	Jeremy Jason Lang Registration No. 73,604 (jason.lang@weil.com) Postal & Hand-Delivery Address: Weil, Gotshal & Manges LLP 201 Redwood Shores Parkway Redwood Shores, CA 94065 T: 650-802-3237; F: 650-802-3100

Pursuant to 37 C.F.R. § 42.10(b), a Power of Attorney for Petitioner is attached.

2.3. Notice of Real-Parties-in-Interest (37 C.F.R. § 42.8(b)(1))

Petitioner, Micron Technology, Inc., is the real-party-in-interest. No other parties exercised or could have exercised control over this petition; no other parties funded or directed this petition. *See* Office Patent Trial Practice Guide, 77 Fed. Reg. 48759-60.

2.4. Notice of Related Matters (37 C.F.R. § 42.8(b)(2))

Innovative Memory Systems has asserted the 537 Patent and U.S. Patent Nos. 6,169,503 (the "503 Patent"), 6,901,498 (the "498 Patent"), 7,000,063 (the "063 Patent"), 7,045,849 (the "849 Patent"), 7,085,159 (the "159 Patent"), 7,495,953 (the "953 Patent") and 7,886,212 (the "212 Patent") (collectively, "the asserted patents") against Micron in a co-pending litigation, *Innovative Memory Systems, Inc., v. Micron Tech., Inc.*, 14-cv-1480 (D. Del.) ("Co-Pending Litigation").

In addition to this Petition, Petitioner is filing petitions for *inter partes* review of each asserted patent in the Co-Pending Litigation: Petition for *Inter Partes* Review of U.S. Patent No. 6,169,503, IPR2016-Unassigned; Petition for *Inter Partes* Review of U.S. Patent No. 6,901,498, IPR2016-Unassigned; Petition for *Inter Partes* Review of U.S. Patent No. 7,000,063, IPR2016-Unassigned;

Petition for *Inter Partes* Review of U.S. Patent No. 7,045,849, IPR2016-Unassigned; Petition for *Inter Partes* Review of U.S. Patent No. 7,085,159, IPR2016-Unassigned; Petition for *Inter Partes* Review of U.S. Patent No. 7,495,953, IPR2016-Unassigned; and Petition for *Inter Partes* Review of U.S. Patent No. 7,886,212, IPR2016-Unassigned.[1]

The 537 Patent does not claim priority to any foreign or U.S. patent application. U.S. Patent No. 6,539,380 and PCT Application No. US00/26206 both are continuations of the application leading to the 537 Patent.

2.5. Fee for *Inter Partes* Review

The Director is authorized to charge the fee specified by 37 C.F.R. § 42.15(a), and any other required fees, to Deposit Account No. 506499.

2.6. Proof of Service

Proof of service of this petition on the patent owner at the correspondence address of record for the 537 Patent is attached.

3. IDENTIFICATION OF CLAIMS BEING CHALLENGED (§ 42.104(B))

Ground #1: Claims 1 and 13 of the 537 Patent are invalid under (pre-AIA) 35 U.S.C. § 102(b) on the ground that they are anticipated by U.S. Patent No. 4,816,653, to Anderl, et al. ("Anderl"), entitled "Security File System For A

[1] These petitions will be filed concurrently or within a few days.

Portable Data Carrier," issued on March 28, 1989. Anderl is attached as MICRON-1005. This ground is explained below and is supported by the Declaration of Dr. R. Jacob Baker (MICRON-1003, "Baker Decl.").

Ground #2: Claims 1 and 13 of the 537 Patent are invalid under (pre-AIA) 35 U.S.C. § 103(a) on the ground that they are obvious over Anderl. This ground is explained below and is supported by the Baker Declaration.

Ground #3: Claim 2 of the 537 Patent is invalid under (pre-AIA) 35 U.S.C. U.S.C. § 103(a) on the ground that it is obvious over Anderl (as anticipatory in Ground #1) in view of Mike Hendry, *Smart Card Security and Applications* (1997) ("Hendry"). The excerpts produced at MICRON-1006 are from a copy of the Hendry book that was published in 1997.[2] This ground is explained below and is supported by the Baker Declaration.

[2] Hendry has an imprint with a copyright date of 1997. The United States Copyright Office discloses a publication date of August 31, 1997 in the official registration of copyright. *See* MICRON-1010 (Retrieved Dec. 8, 2015 from the United States Copyright Office public record search). In addition to the copyright and publication date of the reference, *see* MICRON-1011 (Rowlison de Ortiz Declaration) which provides additional evidence of its availability to the public.

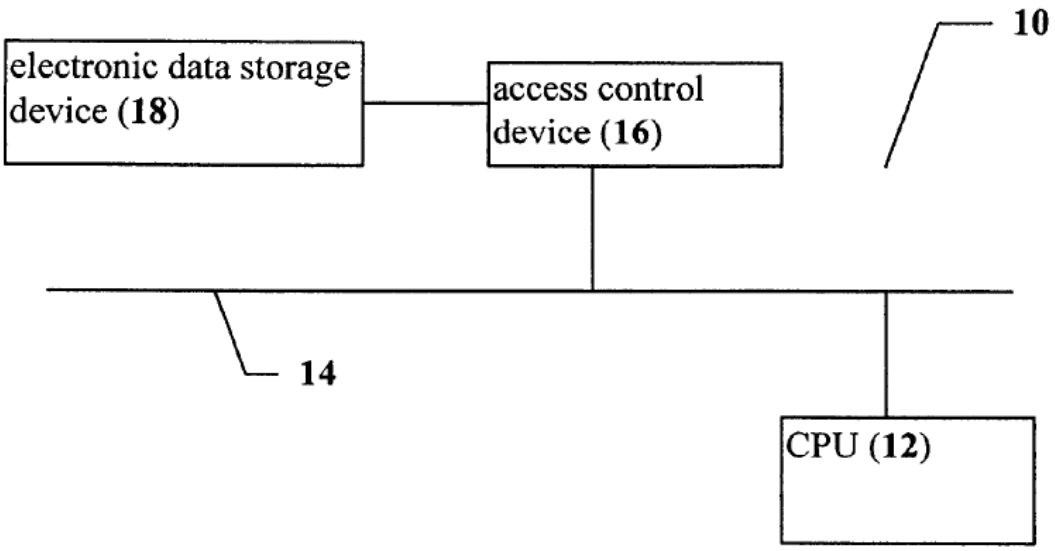
Ground #4: Claim 2 of the 537 Patent is invalid under (pre-AIA) 35 U.S.C. U.S.C. § 103(a) on the ground that it is obvious over Anderl (under obviousness in Ground #2) in view of Hendry. This ground is explained below and is supported by the Baker Declaration.

4. OVERVIEW OF THE 537 PATENT

The 537 Patent was filed on September 30, 1999 and issued on November 27, 2001. The 537 Patent generally relates to an access control device that controls all access to information stored in a data storage device, such as a hard disk drive or flash memory, according to various types of permissions. MICRON-1001, 537 Patent at 2:36-39, 4:26-30. As the background section of the 537 Patent acknowledges, it was well known to use operating systems or software programs on computers to control access to a data storage device. *Id*. at 1:34-60. For example, those systems and programs could allow a user to determine the level of permissions associated with a particular file on a data storage device. *Id*. at 1:51-55. However, the 537 Patent states that if the data storage device is stolen, the data on the storage device becomes unprotected since the software programs and operating system on the computer that implement the protections are stored and implemented separately. *Id*. at 1:61-67.

The 537 Patent purports to solve this problem by providing for an access control device—where the data stored on the data storage device could only be

accessed through the access control device, as illustrated below in Fig. 1. *Id*. at 3:8-11.



MICRON-1001, 537 Patent at Figure 1.

For example, the access control device can be a microprocessor that is implemented on the same chip as the electronic data storage device. *Id*. at 3:14-17. As shown above, the only path to the electronic data storage device (18) is directly through the access control device (16).

The "important feature" of the alleged invention in the 537 Patent is that it allows a plurality of different types of access to be combined in a single storage device. *Id*. at 4:66-5:1. The 537 Patent states that the prior art is generally "restricted to a single type of data access," but the alleged invention "is flexible and is able to store data according to several different access types within a single device." *Id*. at 5:1-6. For example, in the alleged invention, most data files are

preferably stored with a standard read/write permission, "R/W" data. *Id*. at 8:37-43.

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", data-based definition, rather than according to a "hard" definition which is implemented only in the hardware itself.

Id. at 5:6-12.

5. 537 PATENT PROSECUTION HISTORY

The application that led to the issuance of the 537 Patent was originally filed with 22 claims. MICRON-1002, Original Application at .005-.006. The claims at issue in this Petition, claims 1, 2, and 13, were originally claims 1, 2, and 13. *Id.*, Claims at .026-.032.

The Examiner rejected claims 1 and 2 as being anticipated by U.S. Patent No. 4,590,552 ("Guttag") and claim 13 as being obvious over Guttag in view of U.S. Patent No. 5,500,517 ("Cagliostro"). *Id.*, 11-21-2000 Rejection at .044-.049.

In its 3-21-2001 Response, the applicant amended claim 1 and argued that Guttag was different because the 537 invention (1) stored data according to the type of data or "soft characteristics," (2) provided access through a single input, (3) had fewer components than Guttag, (4) could divide the stored data into different portions, and (5) may include data in the access request for comparison to the stored data. *Id.*, 3-21-2001 Response at .060-.070.

In response, the Examiner rejected claims 1 and 2 as being anticipated by U.S. Patent No. 6,240,493 ("Hardwood") and claim 13 as being obvious over Hardwood in view of Cagiliostro. *Id.*, 6-4-2001 Rejection at .075-.082. However, the Examiner allowed dependent claims 26-28. *Id*. at .080. Claim 26 required that the electronic data storage device store the permission information. Specifically, claim 26 stated:

> 26. The system of claim 1, wherein said electronic data storage device also stores information appended to the stored data, said appended information featuring said at least one associated type of permission for accessing the stored data.

Id. at .063.

In its 9-05-2001 Response, the applicant amended claim 1 again, as follows, to incorporate the limitation of claim 26 by requiring that the "electronic storage device" also stores "information appended to the stored data, said appended information featuring said at least one associated type of permission for accessing

the stored data." *Id.*, 9-05-2001 Response at .084-.085. This amendment is illustrated below:

> 1. (Amended) 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.

In other words, the only alteration to the claim was that the "electronic data storage device" also stored the permission information as "information appended to the stored data," as well as the "stored data." The Examiner accordingly allowed the claims. *Id.*, Notice of Allowability at .093.

6. CLAIM CONSTRUCTION[3]

6.1. Applicable Law

A claim subject to *inter partes* review is given the "broadest reasonable construction in light of the specification of the patent in which it appears."[4] 37 C.F.R. § 42.100(b). Any ambiguity regarding the "broadest reasonable construction" of a claim term is resolved in favor of the broader construction absent amendment by the patent owner. Final Rule, 77 Fed. Reg. 48680, 48699 (Aug. 14, 2012).

---

[3] Petitioner expressly reserves the right to challenge in district court litigation one or more claims (and claim terms) of the 537 Patent for failure to satisfy the requirements of 35 U.S.C § 112, which cannot be raised in these proceedings. *See* 35 U.S.C. § 311(b). Nothing in this Petition, or the constructions provided herein, shall be construed as a waiver of such challenge, or agreement that the requirements of 35 U.S.C. § 112 are met for any claim of the 537 Patent.

[4] The district court, in contrast, affords a claim term its "ordinary and customary meaning . . . to a person of ordinary skill in the art in question at the time of the invention." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (*en banc*). Petitioner expressly reserves the right to argue different or additional claim construction positions under this standard in district court.

6.2. Construction of Claim Terms

All claim terms not specifically addressed in this Section have been accorded their broadest reasonable interpretation as understood by a person of ordinary skill in the art and consistent with the specification of the 537 Patent. Petitioner respectfully submits that the following terms should be construed for this IPR:

6.2.1. "integrated" (claim 13)

The term "integrated" is a limitation of dependent claim 13 of the 537 Patent. Specifically, claim 13 requires that the "access control device is integrated with said electronic storage device." MICRON-1001, 537 Patent at claim 13. The 537 Patent describes the prior art solution of using a computer as the access control device to be problematic since the software on the computer is "stored and implemented separately from the storage device itself" and if the storage device is stolen "the data becomes completely unprotected." *Id*. at 1:62-67. Accordingly, the 537 Patent describes that a solution to this problem would be an integrated device:

> A more useful solution would be implemented with the hardware of the electronic storage device **in a more integrated manner**, such that even if the storage device itself is stolen, the data could not be easily accessed. Furthermore, such integration would increase the difficulty of access by an unauthorized user.

Id. at 2:1-6 (emphasis added). The 537 Patent further explains that there is a need for an access control device that "is optionally integrated with the hardware of the storage device." *Id*. at 2:11-13. Thus, under the broadest reasonable interpretation standard, a person of ordinary skill in the art would have understood the plain and ordinary meaning of this term in the context of the 537 Patent to mean "**combined**." MICRON-1003, Baker Decl. ¶¶ 43-46.

7. PERSON HAVING ORDINARY SKILL IN THE ART

A person of ordinary skill in the art with respect to the technology described in the 537 Patent would be a person with a Bachelor of Science degree in electrical engineering, computer engineering, computer science or a closely related field, along with at least 2-3 years of experience in the design of memory devices. An individual with an advanced degree in a relevant field would require less experience in the design of memory devices. MICRON-1003, Baker Decl. ¶ 19.

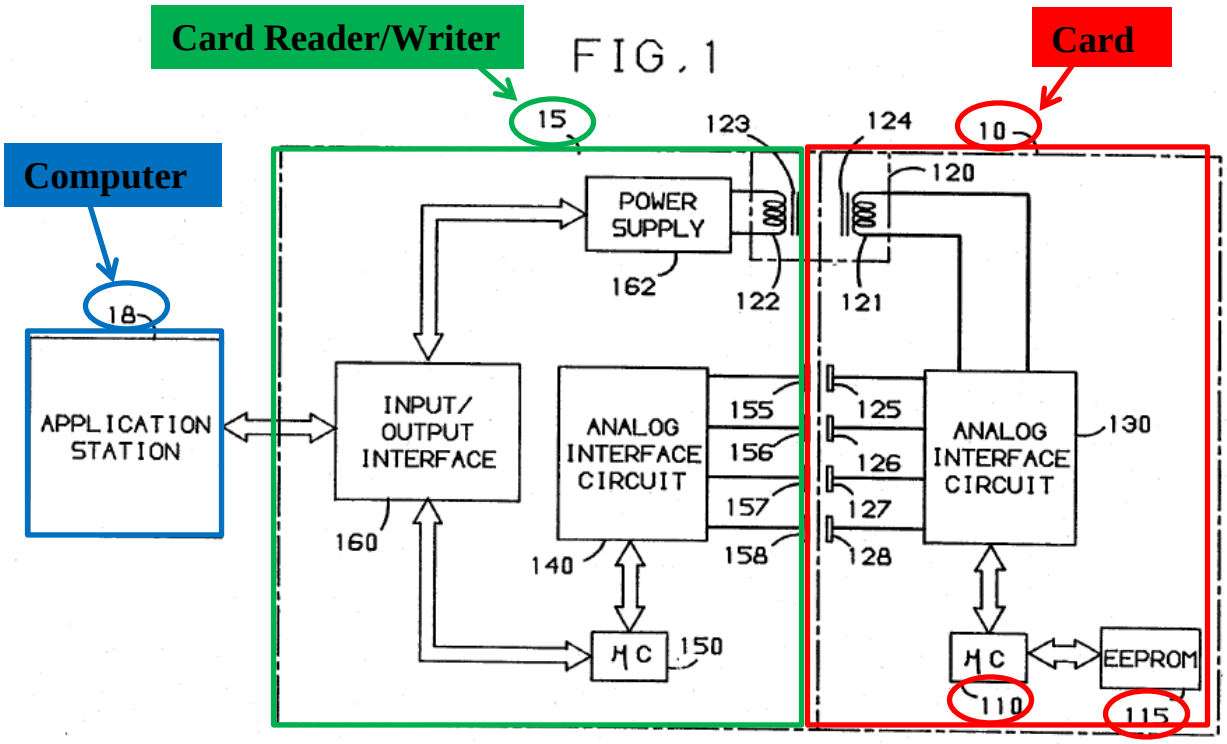
8. DESCRIPTION OF THE PRIOR ART

8.1. U.S. Patent No. 4,816,653 ("Anderl")

U.S. Patent No. 4,816,653 ("Anderl") (MICRON-1005) was filed on May 16, 1986. Anderl issued on March 28, 1989 to Ewald C. Anderl, Oren Frankel, and Avi Zahavi and is entitled "Security File System For A Portable Data Carrier." The original assignees were American Telephone and Telegraph Company and AT&T Information Systems Inc. Anderl is prior art to the 537 Patent under (pre-

AIA) 35 U.S.C. § 102(b) because the patent issued more than one year before the 537 application was filed.

Anderl discloses a high security, portable data carrier or smart card, typically the size of a standard plastic credit card, which includes both a microcomputer and an electrically erasable programmable read-only memory (EEPROM). MICRON-1005, Anderl at 1:53-60, 3:38-43. As illustrated in Fig. 1 below, the card is 10, the EEPROM is 115, and the microcomputer is 110.

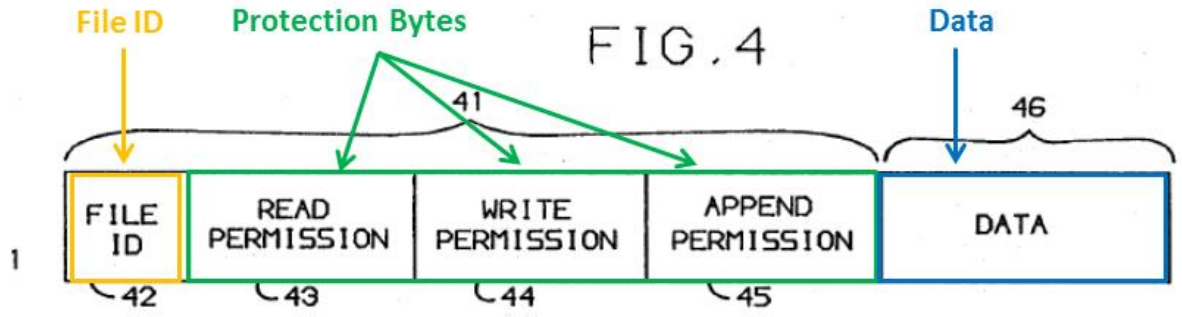


MICRON-1005, Anderl at Figure 1 (with annotations).

The card reader/writer is 15 and the computer workstation is 18. *Id*. at 3:24-30. The card reader/writer could be part of the computer workstation. *Id*. at 1:61-63. Thus, like the 537 Patent, Anderl discloses a computer with a card reader/writer

(*i.e.*, the computer workstation 18 with the card reader/writer 15) which is connected to a device (*i.e.*, the microcomputer 110) that is the only means of accessing a storage device (*i.e.*, the EEPROM 115). Notably, like the 537 Patent, Anderl discloses that the microcomputer is the only path through which access to the EEPROM is possible. The microcomputer, along with the operating system that it runs, thus protects access to the EEPROM and is connected to the EEPROM on the portable data carrier or smart card itself.

Anderl also provides for different permissions that are associated with the data stored on the EEPROM. *Id*. at 6:55-7:50. For example, a customer's personal information can reside in multiple files in the EEPROM on the card. *Id*. at 1:67-68. As illustrated below in Fig. 4, there are protection bytes that are stored in the same file as the data:



MICRON-1005, Anderl at Figure 4 (with annotations).

These protection bytes provide different permissions for accessing the stored data in the file. *Id*. at 6:66-7:45. These permissions are for respective files on the EEPROM. *Id*. at 6:57-60. In other words, different files may have different

permissions. *See id.* As to the exemplary permissions above, the field Read Permission 43 indicates the level at which read access to the EEPROM is permissible, the field Write Permission 44 indicates the level at which read/write access to the EEPROM is permissible, and Append Permission 45 indicates whether a user may append information to the file. *Id*. at 6:65-7:2, 7:38-45.

Anderl discloses six different security levels that relate to these file permissions. *Id*. at 2:13-22, 5:18-29. Specifically, Anderl discloses that a user may login at a specific security level:

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)

MICRON-1005, Anderl at Figure 2.

The protection bytes with the permission information can be set by security level. MICRON-1005, Anderl at 6:65-7:10. Thus, depending on the user's security level, he or she can perform various functions specified by the permissions

(e.g., reading the data in a file). *Id*. In addition, Anderl discloses that the above permissions can be set so that an additional password is necessary. *Id*. at 7:11-31. Thus, access to the file is both a function of the permissions in the file and the logged-in security level. *Id*. at 5:21-26, 6:15-19, 7:59-68.

The microcomputer runs an operating system (which is on a ROM). *Id*. at 3:33-37, 3:44-57. The operating system includes command primitives. *Id*. at 3:33-37. It is interpretation of these commands by the microcomputer that allows the smart card of Anderl to communicate with other devices (via the card reader/writer). *Id*. at 2:6-12, 3:49-57, 7:51-56, 7:59-68, 8:28-40.

Specifically, external devices send these commands to the smart card device and the microcomputer interprets them, which allows the microcomputer to control the security access for the smart card. *Id*. at 1:68-2:12, 3:33-37, 3:44-57, 5:21-27, 7:51-56, 7:59-68, 8:28-40. For example, a card user may attempt to gain access to a file by logging in at a security level. *Id*. at 7:59-68. Commands are sent to the microcomputer, which interprets them, so that the microcomputer can verify whether the user has a high enough security level for respective permissions. *Id*., *see also id*. at 2:6-12, 3:33-37, 3:44-57, 5:21-27, 7:54-56, 7:59-68.

As shown above, these permissions are file-specific and are fields at the beginning of each file. Thus, like the 537 Patent, Anderl discloses that there are

permissions appended to the stored data that determine how the stored data can be accessed.

In addition, Anderl discloses that the EEPROM and the microcomputer are combined together on a single smart card. *Id.* at Fig. 1. Indeed, Anderl also discloses that the EEPROM can be an integral part of the microcomputer. *Id*. at 3:53-55.

8.2. Smart Card Security and Applications ("Hendry")

Smart Card Security and Applications ("Hendry") (MICRON-1006) is a textbook that was published in 1997. The author of the textbook is Mike Hendry. Hendry is prior art to the 537 Patent under U.S.C. § 102(b) because the book was published more than one year before the 537 application was filed.

Hendry describes the evolution of the smart card which began in Japan in 1970. MICRON-1006, Hendry at .018, .046. "The 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 .047. Most memory cards of the time included protected areas which required a security code to access. *Id*. at .053. The code would be held secretly in the card. *Id*.

Hendry explains that for "maximum security and true portability of data," the smart card "must incorporate a microprocessor." *Id*. at .054. When a card incorporates a microprocessor, "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 .054-.055. Several IC manufacturer at the time produced single chips that included both the microprocessor and memory. *Id*.

9. GROUND #1: CLAIMS 1 AND 13 OF THE 537 PATENT ARE UNPATENTABLE AS ANTICIPATED BY ANDERL

As explained below, claims 1 and 13 of the 537 Patent are unpatentable as anticipated by Anderl under 35 U.S.C. § 102(b). Anderl discloses all of the limitations of claims 1 and 13 of the 537 Patent, and therefore anticipates these claims.

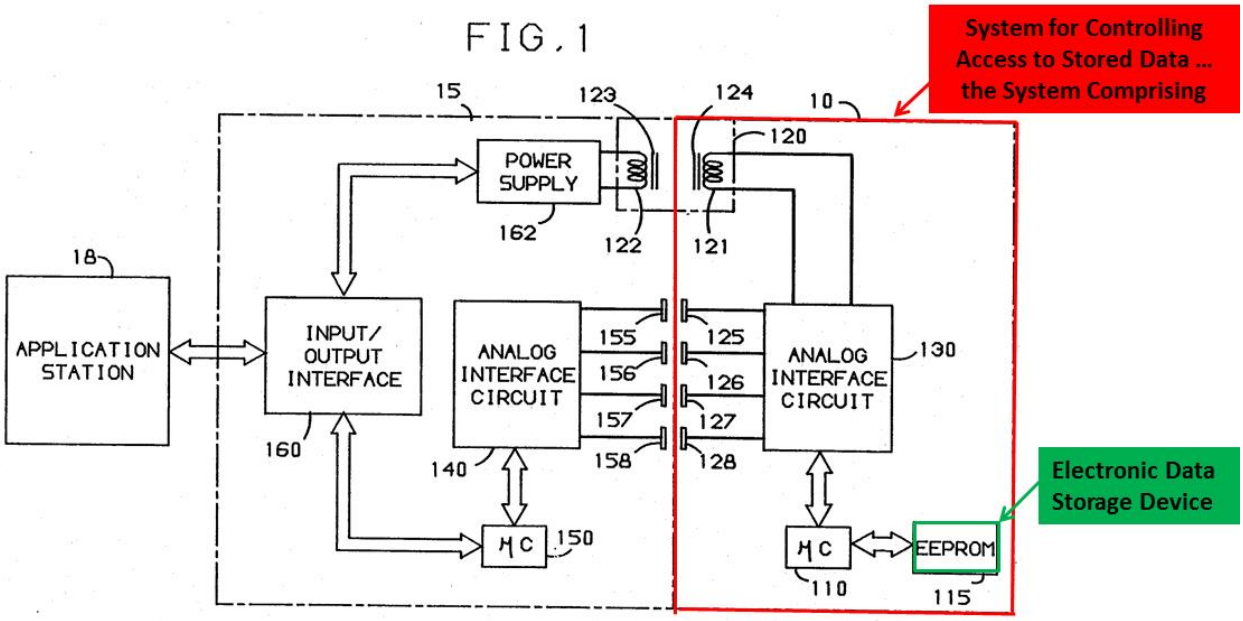
9.1. Claim 1 Is Anticipated By Anderl

9.1.1. [1.P] "A system for controlling access to stored data, the stored data having at least one associated type of permission, the system comprising:"

To the extent the preamble is limiting, Anderl discloses a system for controlling access to stored data, the stored data having at least one associated type of permission. *See* MICRON-1003, Baker Decl., Appx. A at ground 1, claim [1.P].

Anderl addressed the problem of "providing suitable security for the data" on a smart card that includes both a microcomputer and memory. MICRON-1005, Anderl at 1:34-37, 1:46-50. Accordingly, Anderl discloses a system that includes a "high security" smart card "typically the size of a standard plastic credit card." *Id.* at 1:7-10, 1:53-66, 3:19-32, Fig. 1. The smart card includes a microcomputer,

labeled 110 in Fig. 1, and an EEPROM, labeled 115 in Fig. 1. The microcomputer controls access to the EEPROM. *Id*. at 2:6-10, 3:33-43, 3:55-57, 7:51-68. Fig. 1 illustrates the interconnections between the components of the system in Anderl. *Id*. at 2:46-49.



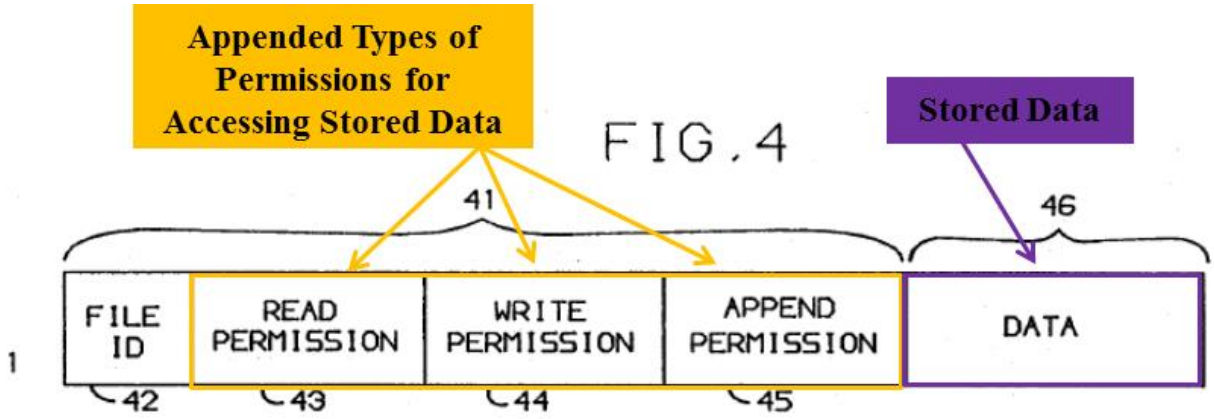
MICRON-1005, Anderl at Figure 1 (with annotations).

As shown above, the only access to the EEPROM is through the microcomputer, thereby providing a single secure path to the data on the EEPROM.

Files are stored in the EEPROM and include protection bytes which can provide permission information (*e.g.*, read or write permission) about the data stored in the file. *Id*. at 1:67-68, 6:49-51, 6:55-7:10, 7:14-27, 7:38-50. For example, the bytes can represent the login level that is necessary to read or write data to the file. *Id*. at 6:65-7:2. Anderl provides six different security levels that

can be used in conjunction with the protection bytes to control access to the data in the file. *Id*. at 2:13-26, 5:18-27, 7:2-10. The microcomputer on the card, which runs an operating system, will refuse access to the file unless the password required by the file is entered. *See, e.g.*, 1:68-2:12, 3:55-57, 6:15-19, 7:51-68.

The protection bytes may also include an additional password that is required to access the files. *Id*. at 7:14-27. The protection bytes and stored data in a file are illustrated in Fig. 4.



MICRON-1005, Anderl at Figure 4 (with annotations).

Because the protection bytes are associated with an individual file, each file may have its own security requirements. *Id*. at 2:29-32, 6:57-59. The details of the structure and operation of accessing the data on the smart card show in Fig. 1 are described with respect to the remaining limitations of the claim.

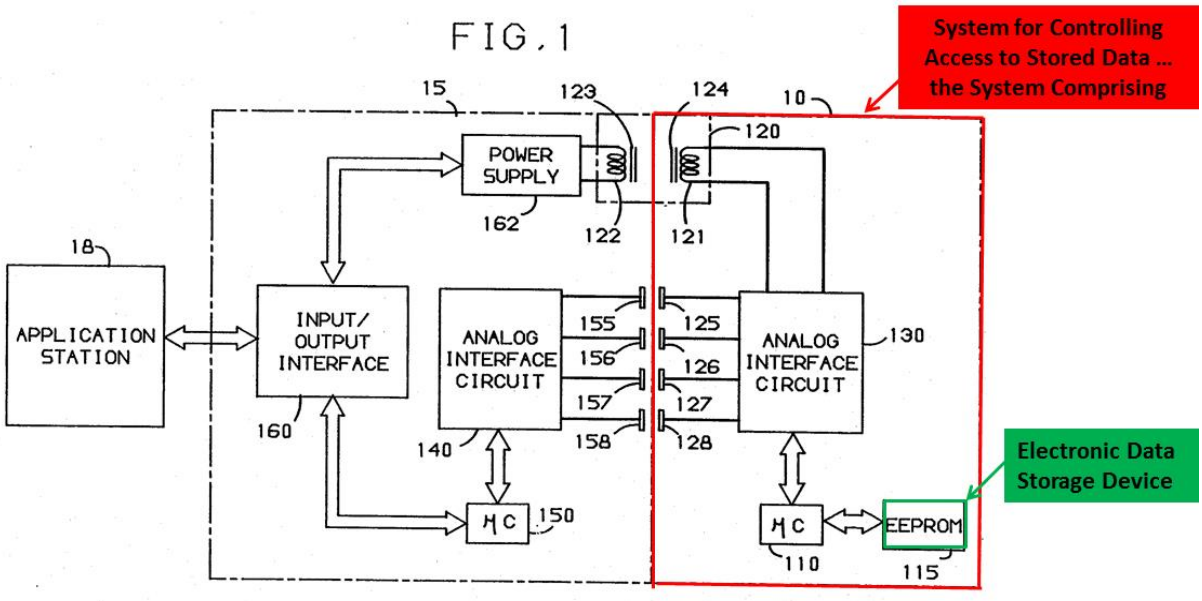
Thus, by disclosing card 10, which includes a microcomputer 110 running an operating system that controls access to EEPROM 115, and by disclosing that the EEPROM 115 stores data with permissions such as read, write, and append

permissions, Anderl discloses a system for controlling access to data stored in a file with an associated permission, such as a read or write permission, on a smart card.

9.1.2. [1.1.a] "an electronic data storage device for storing the stored data and information appended to the stored data,"

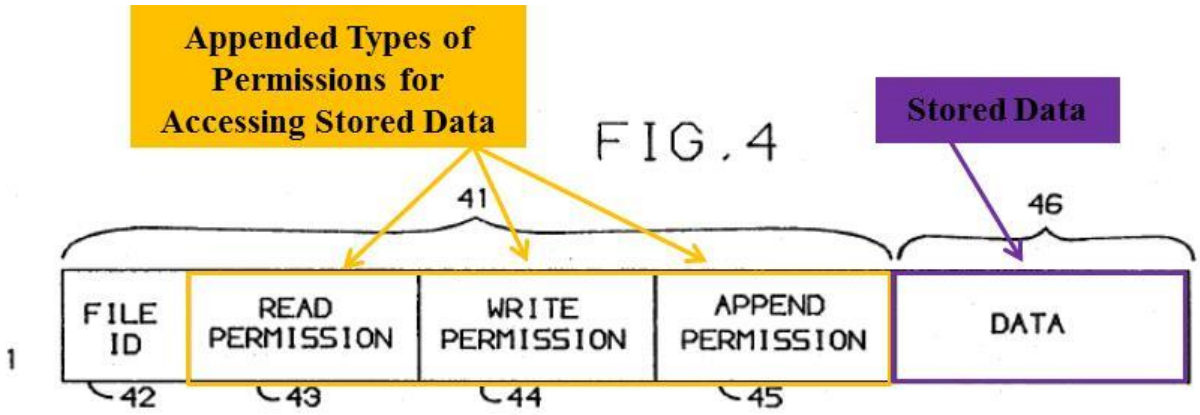
Anderl discloses an electronic data storage device for storing the stored data and information appended to the stored data. *See* MICRON-1003, Baker Decl., Appx. A at ground 1, claim [1.1.a].

Anderl describes that the smart card includes an electrical erasable programmable read-only memory (EEPROM). MICRON-1005, Anderl at 3:38-43, 3:49-53, 3:58-62, Fig. 1. This is illustrated in Fig. 1:



MICRON-1005, Anderl at Figure 1 (with annotations).

Anderl also describes that the EEPROM can store files that include data and protection bytes. *Id*. at 1:53-57, 1:67-2:5, 6:39-7:10, 7:14-27, 7:38-50. Fig. 4 illustrates information in a file. *Id*. at 2:57-59, 6:55-57. The protection bytes are appended to the stored data (*i.e.*, as fields at the beginning of each file) as illustrated below in Fig. 4.



MICRON-1005, Anderl at Figure 4 (with annotations).

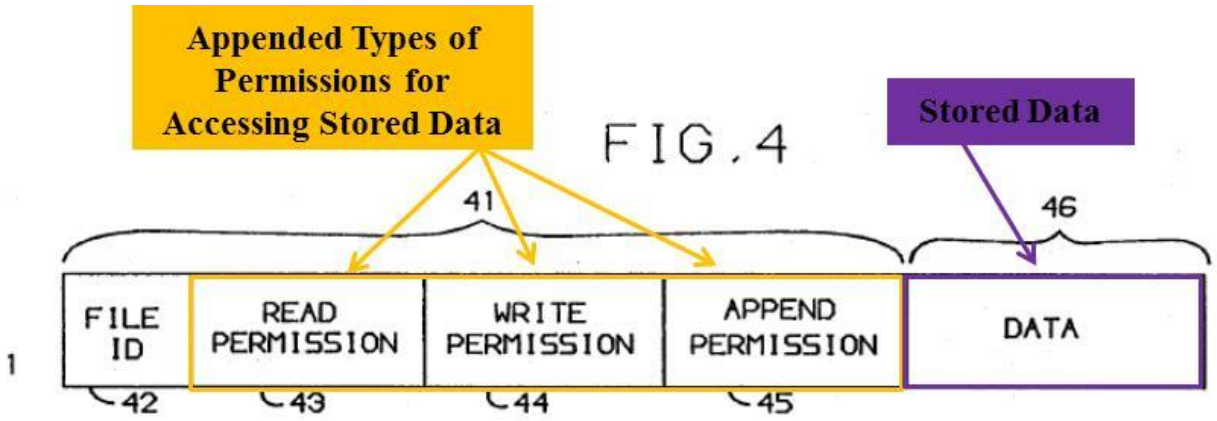
See also id. at 6:39-7:10, 7:14-27, 7:38-50.

Thus, by disclosing card 10, which includes an EEPROM 115 (*i.e.*, "electronic data storage device") that stores data and permissions for accessing that stored data, such as read, write, and append permissions, in a file, Anderl discloses an electronic data storage device for storing the stored data and information appended to the stored data.

9.1.3. [1.1.b] "said appended information featuring said at least one associated type of permission for accessing the stored data; and"

Anderl discloses that the appended information features at least one associated type of permission for accessing the stored data. *See* MICRON-1003, Baker Decl., Appx. A at ground 1, claim [1.1.b].

Anderl discloses that the protection bytes can include different types of permissions, such as read, write, or append permissions, for accessing the stored data. *See, e.g.*, MICRON-1005, Anderl at 5:18-27, 6:65-7:10, 7:14-27, 7:38-45. The protection bytes are stored at the beginning of a file, before the stored data. *Id.* at 2:57-59, 6:55-60, 7:46-47.



MICRON-1005, Anderl at Figure 4 (with annotations).

For example, the read permission can designate the minimum security level at which the file may be read. *Id.* at 6:66-68 ("The first byte 43 represents read permission designating the minimum level at which the file may be read…"). An appended protection byte could also include a requirement for an optional

password before access to the file is allowed. *Id*. at 7:15-18 ("[E]ach file on the card may include in its protection bytes a requirement that an optional password be provided before allowing access to a particular file."). If a user attempts to access a file with a login level lower than that required by the file, access will be denied. *Id*. at 6:9-19, 7:59-68. However, if a user attempts to access the file with a higher login level than required, access to the file will be granted. *Id*. at 7:27-45.

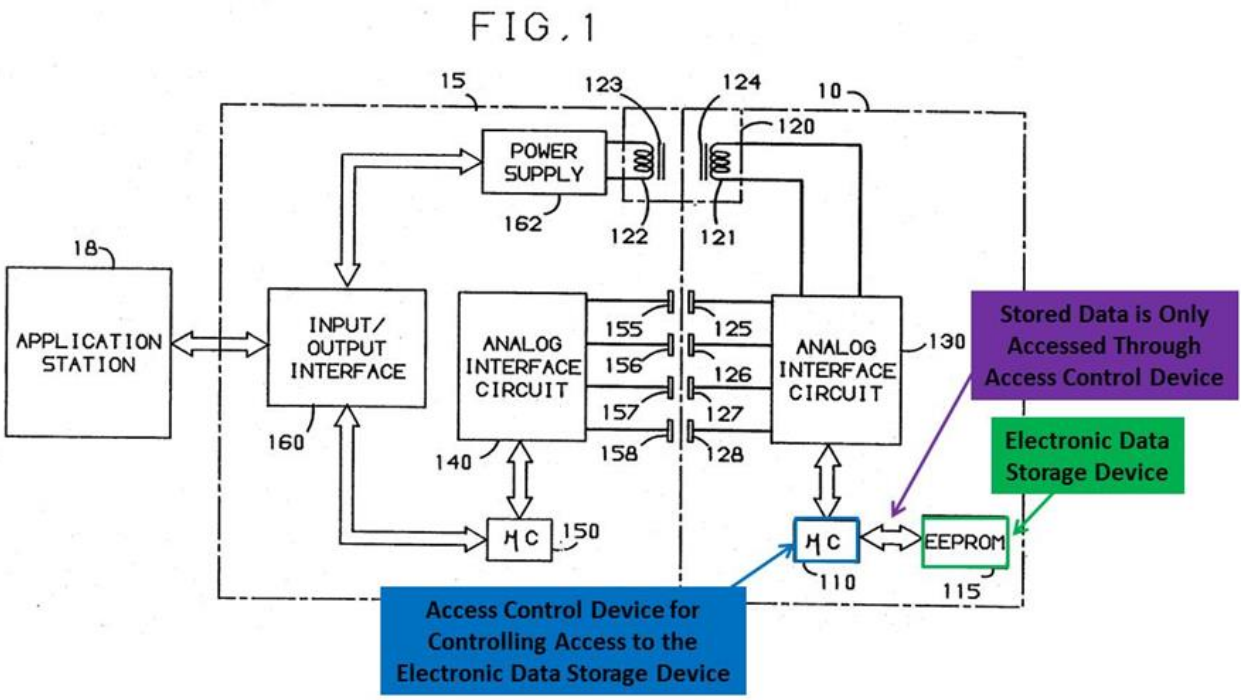
Thus, by disclosing data stored in a file with permission information stored in protection bytes at the beginning of the file that provides access to the data at certain security login levels, Anderl discloses that the appended information features at least one associated type of permission for accessing the stored data.

9.1.4. [1.2.a] "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"

Anderl discloses an access control device for controlling access to the electronic data storage device, such that the stored data is only accessed through the access control device. *See* MICRON-1003, Baker Decl., Appx. A at ground 1, claim [1.2.a].

Specifically, Anderl discloses that the microcomputer (*i.e.*, microcomputer 110 in Fig. 1) is the only way to access the stored data on the EEPROM (*i.e.*, EEPROM 115 in Fig. 1), as illustrated below in Fig. 1. Fig. 1 illustrates the

interconnections between the system components. MICRON-1005, Anderl at 2:46-49.



MICRON-1005, Anderl at Figure 1 (with annotations).

Microcomputer 110, which resides on card 10, runs an operating system that is stored on a ROM on the card. *See, e.g., id.* at 1:68-2:10, 3:33-37, 3:44-57, 7:54-56; MICRON-1003, Baker Decl. ¶ 53. The operating system includes a set of command primitives that may be sent from the station. *See id.* The microcomputer interprets those operating system command primitives which control security access for the files on the EEPROM. *See, e.g.*, MICRON-1005, Anderl at 3:55-57 ("The microcomputer 110 also interprets the command primitives from the station 18 received through the reader/writer 15."), 7:54-56

("These command primitives control the security access for the card…"), 3:49-53 ("Operating under firmware control provided by its internal read-only memory, the microcomputer 110 formats data that is transferred directly to the EE-PROM 115 and via the reader/writer 15 to the station 18."), 3:53-54 ("The entire EEPROM or a portion of it may be an integral part of the microcomputer…"). For example, a password is sent to the card via these command primitives. *Id*. at 1:68-2:10, 7:51-68, 8:17-19, 8:28-40. Interpreting these commands, the microcomputer will deny access to the stored data if the appropriate password required by the file is not entered. *Id*. at 2:6-12, 3:55-57, 5:24-27, 6:15-54, 6:65-7:10, 7:14-27, 7:38:45, 7:54-56, 7:59-68.

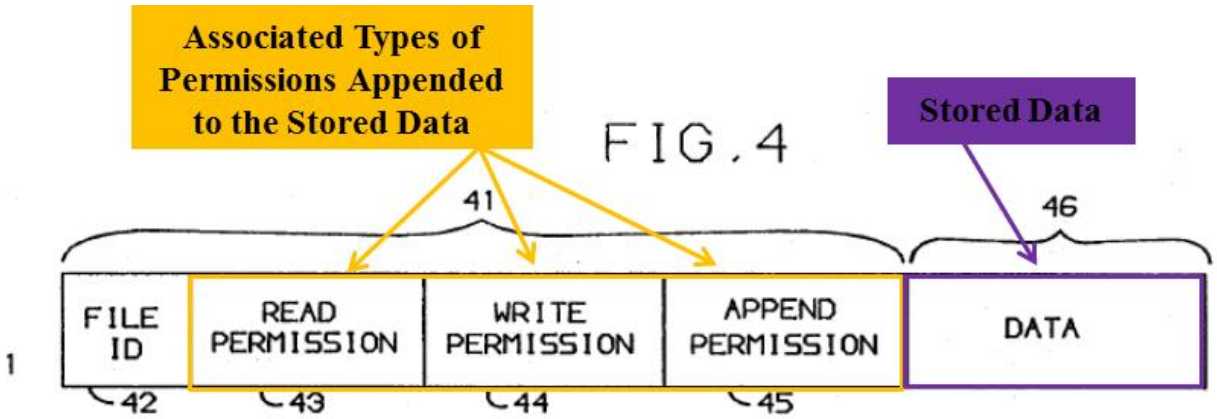
Thus, by disclosing that the microcomputer 110 on the card runs an operating system which controls access to the EEPROM 115 and is the only way to access EEPROM 115, Anderl discloses an access control device for controlling access to the electronic data storage device, such that the stored data is only accessed through the access control device.

9.1.5. [1.2.b] "such that said access control device determines access to the stored data according to at least one said associated type of permission."

Anderl discloses that the access control device determines access to the stored data according to the associated type of permission. *See* MICRON-1003, Baker Decl., Appx. A at ground 1, claim [1.2.b].

As discussed above, Anderl discloses that access to the data on the EEPROM ("stored data") is only possible through operating system command primitives that are interpreted by the microcomputer on the smart card. In other words, the microcomputer running the operating system controls access to the stored data on the smart card. MICRON-1005, Anderl at 7:54-55 ("These command primitives control the security access for the card…"), 2:6-10, 3:33-43, 3:49-57, 7:59-68.

The microcomputer grants access to the stored data in the file based on both the login level and the protection bytes in the file. *Id*. at 2:20-22 ("Access to [the card file system and the card commands] is a function of the authorized login level, the command requested and the file to be accessed."), 3:49-57, 7:51-56, 7:59-68. Anderl discloses that there can be six different security levels (login levels) on the card. *Id*. at 2:13-26, 5:18-27. In addition, the respective files on the card have protection bytes indicating what security level can access the respective file for each type of permission. *Id*. at 6:65-7:10, 7:14-27, 7:38-45, Fig. 4. In other words, the microcomputer controls access to the file with respect to each file permission according to whether the security level of the user is sufficient for each type of respective permission. An exemplary file is shown below with its corresponding permissions:



MICRON-1005, Anderl at Figure 4 (with annotations).

For example, if a user attempts to gain access to a file with a login level lower than that required by the file, permission to open the file is denied. *Id*. at 7:65-68 ("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."). This control can be specific to each type of permission for a file. *See, e.g., id.* at 7:3-10. That is, 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. *See, e.g., id.* at 7:6-10 ("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.").

Thus, by disclosing that the microcomputer running the operating system (*i.e.,* the "access control device") provides access to the stored data in a file depending on the specific permissions required by the protection bytes that are

stored with that data in the file, Anderl discloses that the access control device determines access to the stored data according to the associated type of permission.

9.2. Claim 13 Is Anticipated By Anderl

9.2.1. [13.P] "The system of claim 1, wherein"

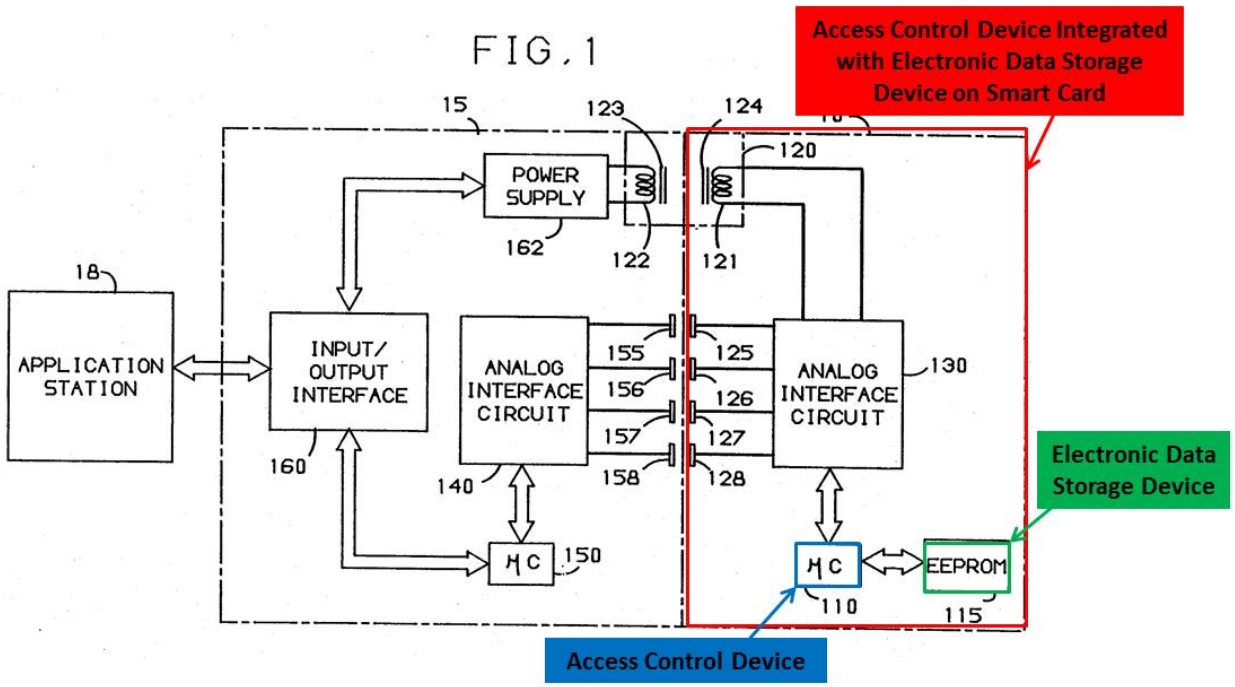
Anderl discloses the system of claim 1. *See* MICRON-1003, Baker Decl., Appx. A at ground 1, claim [1.P-1.2b and 13.P].

See analysis in Section 9.1 above.

9.2.2. [13.1] "said access control device is integrated with said electronic data storage device."

Anderl discloses that the access control device is integrated with the electronic data storage device. *See* MICRON-1003, Baker Decl., Appx. A at ground 1, claim [13.1]. As discussed in Section 6.2.1, under the broadest reasonable interpretation standard, one of ordinary skill in the art would have understood that "integrated" means "combined."

Anderl discloses that the microcomputer is on the same smart card as the EEPROM. MICRON-1005, Anderl at 1:53-66, 3:38-43. Accordingly, both devices are combined together on the smart card.



MICRON-1005, Anderl at Figure 1 (with annotations).

Anderl further discloses that the EEPROM can be an "integral part of the microcomputer." *Id.* at 3:53-54. Accordingly, Anderl not only discloses that the microcomputer can be combined with the EEPROM on the card, but discloses that the EEPROM can actually be part of the microcomputer. Anderl thus discloses that the microcomputer (i.e., the "access control device") is integrated with the EEPROM (i.e., the "electronic data storage device").

10. GROUND #2: CLAIMS 1 AND 13 OF THE 537 PATENT ARE UNPATENTABLE AS OBVIOUS OVER ANDERL

As explained below, claims 1 and 13 of the 537 Patent are unpatentable as obvious over Anderl under 35 U.S.C. § 103(a). Anderl renders obvious all of the

limitations of claims 1 and 13 of the 537 Patent, and therefore at least renders these claims obvious.

10.1. Claim 1 Is Obvious Over Anderl

10.1.1. [1.P] "A system for controlling access to stored data, the stored data having at least one associated type of permission, the system comprising:"

To the extent the preamble is limiting, Anderl discloses a system for controlling access to stored data, the stored data having at least one associated type of permission. *See* MICRON-1003, Baker Decl., Appx. A at ground 2, claim [1.P].

See analysis in Section 9.1.1 above.

10.1.2. [1.1.a] "an electronic data storage device for storing the stored data and information appended to the stored data,"

Anderl discloses an electronic data storage device for storing the stored data and information appended to the stored data. *See* MICRON-1003, Baker Decl., Appx. A at ground 2, claim [1.1.a]

See analysis in Section 9.1.2 above.

10.1.3. [1.1.b] "said appended information featuring said at least one associated type of permission for accessing the stored data; and"

Anderl discloses that the appended information features at least one associated type of permission for accessing the stored data. *See* MICRON-1003, Baker Decl., Appx. A at ground 2, claim [1.1.b].

See analysis Section 9.1.3 above.

10.1.4. [1.2.a] "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"

Anderl at a minimum renders obvious an access control device for controlling access to the electronic data storage device, such that the stored data is only accessed through the access control device. *See* MICRON-1003, Baker Decl., Appx. A at ground 2, claim [1.2.a].

As discussed above in Section 9.1.4, Anderl discloses this limitation. The entire point of Anderl is to provide "suitable security for the data on the card." MICRON-1005, Anderl at 1:47-49. Anderl recognizes that the only way to protect the files on the EEPROM is to have the microcomputer control access—and be the only means of access—to the file system on the EEPROM. In other words, unless the microcomputer vetted each request through the operating system to access the files, anyone could access the files. Anderl explicitly states this unsecure access does not occur, noting that "direct access to the card file system and its commands are not allowed to the normal user." *Id*. at 2:10-12.

However, if the Board finds that Anderl does not expressly disclose this limitation, it would have been obvious to one of ordinary skill in the art to have the microcomputer control access to the EEPROM such that the stored data is only accessed through the microcomputer. In other words, to the extent that Anderl does not expressly disclose that the EEPROM is only accessed through the

microcomputer, it would have been obvious to adapt Anderl so that the EEPROM could only be accessed through the microcomputer. MICRON-1003, Baker Decl., Appx. A at ground 2, claim [1.2.a]. Indeed, Anderl explicitly discloses multiple times that the operating system command primitives, which the microcomputer interprets, "control the security access for the card" and "manipulate the card file system in accordance with rules to maintain card security." MICRON-1005, Anderl at 2:6-10, 3:33-37, 7:51-56, 7:59-68. Fig. 1 also does not disclose any other path to the data stored on the EEPROM except through the microcomputer. *See id.* at Fig. 1. Thus, it would have been obvious to one of ordinary skill in the art that the microcomputer would run the operating system and provide the sole route of accessing the EEPROM.

Moreover, this would have provided "suitable security for the data on the card." *Id*. at 1:47-49. The entire point of the invention in Anderl was to provide a "system for securing the data" contained in a "portable data carrier," such as a smart card. *Id*. at 1:7-10. Providing a mechanism, such as the microcomputer, between the user and the EEPROM as the sole access point to the EEPROM would have allowed such security regardless of where the card was utilized. This would have been a common sense solution to one of ordinary skill in the art based on the disclosure in Anderl. MICRON-1003, Baker Decl., Appx. A at ground 2, claim [1.2.a].

Finally, Anderl discloses that the EEPROM could be "an integral part of the microcomputer." MICRON-1005, Anderl at 3:53-55. This would have suggested to one of ordinary skill in the art that the EEPROM could be on the same chip as the microcomputer. MICRON-1003, Baker Decl., Appx. A at ground 2, claim [1.2.a]. In such a case, providing access to the EEPROM through the microcomputer would have been an obvious solution to monitor access to the files on the EEPROM. *Id*. In other words, 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*.

Accordingly, it would have been obvious to follow Anderl's teachings regarding security and create a smart card where the microcomputer controls access to the EEPROM and the EEPROM is only accessed through the microcomputer.

10.1.5. [1.2.b] "such that said access control device determines access to the stored data according to at least one said associated type of permission."

Anderl discloses that the access control device determines access to the stored data according to at least one associated type of permission. *See* MICRON-1003, Baker Decl., Appx. A at ground 2, claim [1.2.b].

See analysis in Section 9.1.5 above.

10.2. Claim 13 Is Obvious Over Anderl

10.2.1. [13.P] "The system of claim 1, wherein"

Anderl renders obvious the system of claim 1. *See* MICRON-1003, Baker Decl., Appx. A at ground 2, claim [1.P]-[1.2.b] and [13.P].

See analysis in Section 10.1 above.

10.2.2. [13.1] "said access control device is integrated with said electronic data storage device."

Anderl discloses the access control device is integrated with the electronic data storage device. *See* MICRON-1003, Baker Decl., Appx. A at ground 2, claim [13.1].

See analysis in Section 9.2.2 above.

11. GROUND #3: CLAIM 2 OF THE 537 PATENT IS UNPATENTABLE AS OBVIOUS OVER ANDERL IN VIEW OF HENDRY

As explained below, claim 2 of the 537 Patent is unpatentable as obvious over Anderl (as an anticipatory reference in Ground 1) in view of Hendry under 35 U.S.C. § 103(a). Anderl in combination with Hendry discloses all of the limitations of claim 2 of the 537 Patent, and therefore renders the claim obvious.

11.1. Claim 2 Is Obvious Over Anderl In View of Hendry

Anderl discloses that the EEPROM on the smart card could be an "integral part of the microcomputer." MICRON-1005, Anderl at 3:53-55. Hendry supplements that disclosure and provides that numerous manufacturers made chips that included both the microcomputer/microprocessor and the memory for smart

cards on the same chip. MICRON-1006, Hendry at .054-.055. One of ordinary skill in the art would have been motivated to combine Anderl and Hendry for multiple reasons. *See* MICRON-1003, Baker Decl. ¶ 62.

First, a person of ordinary skill in the art would have been motivated to combine Hendry and Anderl based on the nature of the problem to be solved. Both Hendry and Anderl address security for data on smart cards. MICRON-1006, Hendry at .019; MICRON-1005, Anderl at 1:47-49, 1:53-57. Given that both of these references address the problem of protecting data on smart cards, it would have been obvious to combine these references to arrive at a security solution. *See* MICRON-1003, Baker Decl. ¶ 63. In particular, given that Hendry is a book, one of ordinary skill would have considered Hendry to be a good resource to consider when evaluating security options for data on smart cards. *Id.*

Second, one of ordinary skill in the art would have understood that combining two references related to smart cards would have led to predictable results according to known methods. Both Hendry and Anderl discuss smart cards in detail. *See, e.g.*, MICRON-1005, Anderl at 1:53-57; MICRON-1006, Hendry at .016. Placing the memory and the microprocessor on a single chip for a smart card was a design choice. *See* MICRON-1003, Baker Decl. ¶ 64. For example, Hendry explained that several manufacturers made single chips that included both the memory and the microcomputer for a smart card. MICRON-1006, Hendry at .054-

.055. It was understood to yield predictable results because it was so well known. Those of ordinary skill in the art were motivated to place the microcomputer and the EEPROM on the same chip as microprocessor and memory size decreased. *See* MICRON-1003, Baker Decl. ¶ 64. This would have provided an easier to use, more integrated solution. *Id*. This was a predictable result of placing the two devices on a single chip.

11.1.1. [2.P] "The system of claim 1, wherein

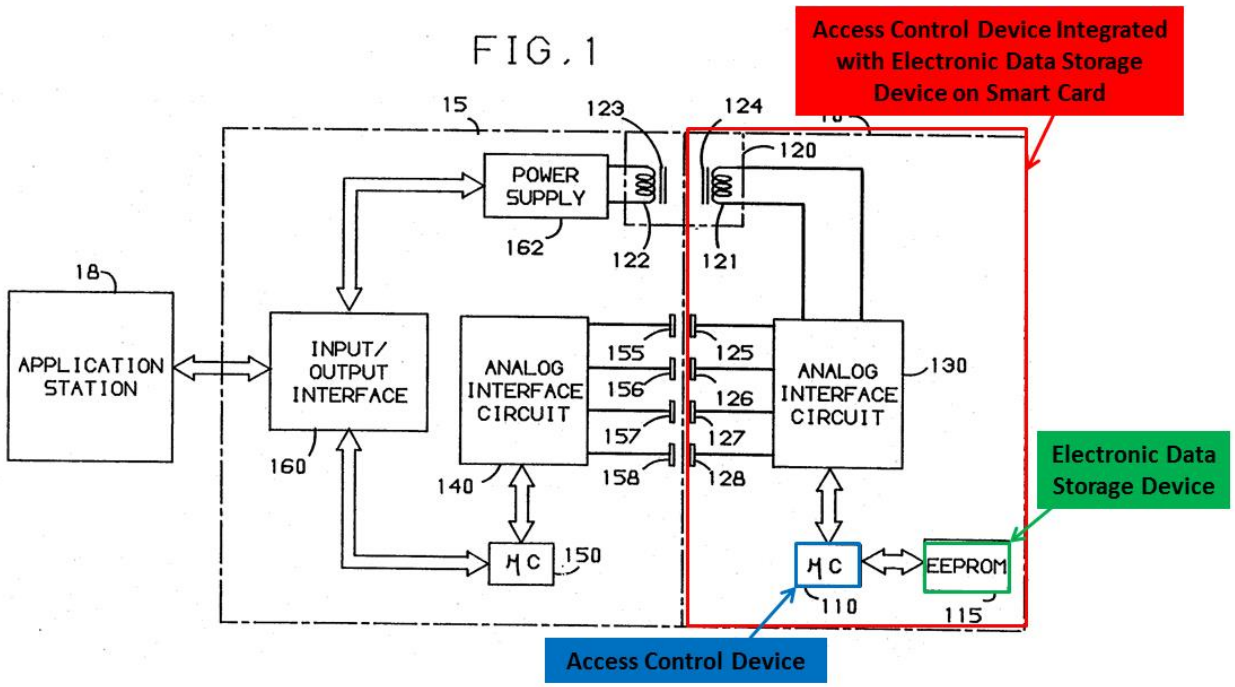
As discussed above, Anderl anticipates (Ground 1) the system of claim 1. *See* MICRON-1003, Baker Decl., Appx. A at ground 1, claim [1.P]-[1.2.b].

See analysis in Section 9.1 above.

11.1.2. [2.1] "said electronic data storage device and said access control device are implemented on a single chip."

Anderl in view of Hendry renders obvious a system where the electronic data storage device and the access control device are implemented on a single chip. *See* MICRON-1003, Baker Decl., Appx. A at ground 3, claim [2.1].

Anderl discloses that the microcomputer (i.e., the "access control device") and the EEPROM (i.e., the "electronic data storage device") are connected together on the same smart card. MICRON-1005, Anderl at 1:34-37, 1:53-66, 3:38-43, Fig. 1.



MICRON-1005, Anderl at Figure 1 (with annotations).

Moreover, Anderl discloses that the "entire EEPROM" could be "an integral part of the microcomputer." *Id*. at 3:49-55. This would have suggested to one of ordinary skill in the art that the EEPROM and the microcomputer could be on a single chip. *See* MICRON-1003, Baker Decl., Appx. A at ground 3, claim [2.1]. Hendry explicitly discloses that it was well known to include the microcomputer/microprocessor and the memory on a single chip and that several manufacturers made chips which included both on a single chip. MICRON-1006, Hendry at .055. Combining these two devices so that the microcomputer and EEPROM would be on the same chip would have been obvious given the industry trend to incorporate multiple devices onto a single chip. *See* MICRON-1003, Baker Decl., Appx. A at ground 3, claim [2.1]. Indeed, at this time, system on a chip

(SOC) technology that incorporated multiple modules onto a single chip, *e.g.*, a processor and a memory module such as DRAM or EEPROM, was growing in popularity. *Id*.

Thus, Anderl in view of Hendry renders obvious including a microcomputer/microprocessor (*i.e.*, the "access control device") and the memory (*i.e.*, the "electronic data storage device") on a single chip in a smart card.

12. GROUND #4: CLAIM 2 OF THE 537 PATENT IS UNPATENTABLE AS OBVIOUS OVER ANDERL IN VIEW OF HENDRY

As explained below, claim 2 of the 537 Patent is unpatentable as obvious over Anderl (as an obviousness reference in Ground 2) in view of Hendry under 35 U.S.C. § 103(a). Anderl in combination with Hendry discloses all of the limitations of claim 2 of the 537 Patent, and therefore renders the claim obvious.

12.1. Claim 2 Is Obvious Over Anderl In View of Hendry

One of ordinary skill in the art would have been motivated to combine Anderl and Hendry for multiple reasons. *See* MICRON-1003, Baker Decl. ¶¶ 62-64.

See analysis in Section 11.1 above.

12.1.1. [2.P] "The system of claim 1, wherein

As discussed above, Anderl renders obvious (Ground 2) the system of claim 1. *See* MICRON-1003, Baker Decl., Appx. A at ground 2, claim [1.P]-[1.2.b].

See analysis in Section 10.1 above.

12.1.2. [2.1] "said electronic data storage device and said access control device are implemented on a single chip."

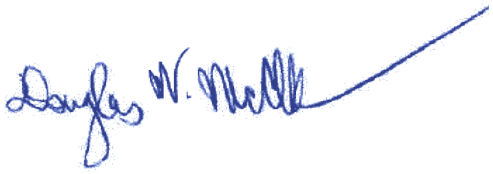
Anderl in view of Hendry renders obvious a system where the electronic data storage device and the access control device are implemented on a single chip. *See* MICRON-1003, Baker Decl., Appx. A at ground 4, claim [2.1].

See analysis in Section 11.1.2 above.

13. CONCLUSION

For the reasons set forth above, *inter partes* review of claims 1, 2, and 13 of the 537 Patent is requested.

Respectfully submitted,



Dated: December 14, 2015

By: _____

Douglas W. McClellan
Lead Counsel for Petitioner
Registration No. 41,183
Weil, Gotshal & Manges LLP
700 Louisiana, Suite 1700
Houston, TX 77002
Telephone: 713-546-5313

CERTIFICATE OF SERVICE

The undersigned certifies, in accordance with 37 C.F.R. § 42.105 and § 42.6(e), that service was made on the Patent Owner as detailed below.

Date of service	December 14, 2015
Manner of service	EXPRESS MAIL
Documents served	Petition for *Inter Partes* Review of U.S. Pat. No. 6,324,537 with Micron's Exhibit List Power of Attorney Exhibits MICRON-1001 through MICRON-1011
Persons served	Patent Owner's Address of Record: BGL P.O. Box 10395 Chicago, IL 60610 Additional Addresses Known as Likely to Effect Service: Brian E. Farnan Farnan LLP 919 North Market Street, 12th Floor Wilmington, DE 19801 bfarnan@farnanlaw.com Edward C. Flynn Cohen & Grace, LLC 105 Braunlich Drive, Suite 300 Pittsburgh, PA 15237 eflynn@cohengrace.com

/ Jeremy Jason Lang /
Jeremy Jason Lang
Back-Up Counsel for Petitioner
Registration No. 73,604