

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD., and
SAMSUNG ELECTRONICS, AMERICA, INC.,

Petitioners

v.

TRUESIGHT COMMUNICATIONS LLC,

Patent Owner

Case IPR2025-00123

U.S. Patent No. 8,745,749

Petition for *Inter Partes* Review of

U.S. Patent No. 8,745,749

Table of Contents

PETITIONERS’ EXHIBIT LIST	vi
LISTING OF CHALLENGED CLAIMS.....	viii
I. INTRODUCTION	1
II. GROUNDS FOR STANDING.....	1
III. STATEMENT OF PRECISE RELIEF REQUESTED FOR EACH CLAIM CHALLENGED	1
IV. OVERVIEW OF THE <i>'749PAT</i>	2
A. Specification.....	2
B. Prosecution History	10
V. PRIOR ART.....	11
A. <i>Maeda</i>	11
B. <i>Hamann</i>	13
C. <i>AAPA</i>	15
D. <i>Hirota</i>	18
E. <i>Lu</i>	20
F. <i>Matsukawa</i>	21
VI. LEVEL OF ORDINARY SKILL IN THE ART	21
VII. CLAIM CONSTRUCTION	21
A. “File System”	22
VIII. DETAILED EXPLANATION OF GROUNDS.....	25

A.	Ground 1: <i>Maeda-Hamann-AAPA</i> Renders Claims 1, 14-16, 18, 22-24 Obvious	25
1.	Claim 1	25
	a. [1pre].....	25
	b. [1a].....	26
	c. [1b].....	30
	d. [1c].....	31
	e. [1d].....	35
	f. [1e].....	39
2.	Motivation To Combine.....	40
3.	Claim 14.....	47
	a. [14pre].....	47
	b. [14a].....	47
	c. [14b].....	50
	d. [14c].....	55
	e. [14d].....	56
	f. [14e].....	56
	g. [14f]	56
	h. [14g].....	57
4.	Claim 15.....	59
5.	Claim 16.....	60
6.	Claim 18.....	63
	a. [18pre].....	63

	b.	[18a].....	63
	c.	[18b].....	63
	d.	[18c].....	63
	e.	[18d].....	63
	f.	[18e].....	64
7.		Claim 22.....	64
	a.	[22pre].....	64
	b.	[22a].....	64
	c.	[22b].....	64
	d.	[22c].....	64
	e.	[22d].....	64
	f.	[22e].....	64
	g.	[22f]	64
	h.	[22g].....	65
8.		Claim 23.....	65
9.		Claim 24.....	65
B.		Ground 2: <i>Maeda-Hamann-AAPA-Hirota</i> Renders Claims 2, 6-8, and 19 Obvious	65
	1.	Claim 2.....	65
	2.	Motivation To Combine.....	69
	3.	Claim 6.....	70
	4.	Claim 7.....	73
	5.	Claim 8.....	74

6.	Claim 19.....	75
C.	Ground 3: <i>Maeda-Hamann-Hirota-Lu</i> Renders Claims 3-5, 20-21 Obvious	75
1.	Claim 3	75
2.	Motivation To Combine.....	78
3.	Claim 4.....	79
4.	Claim 5	80
5.	Claim 17.....	81
6.	Claim 20.....	83
7.	Claim 21	83
8.	Claim 25.....	83
D.	Ground 4: <i>Maeda-Hamann-AAPA-Matsukawa</i> Renders Claim 13 Obvious	84
1.	Claim 13.....	84
2.	Motivation To Combine.....	85
3.	The Board Should Not Exercise Its Discretion Under §325(d) To Deny Institution	85
IX.	SECONDARY CONSIDERATIONS	88
X.	THE DISCRETIONARY FACTORS FAVOR INSTITUTING TRIAL	88
XI.	MANDATORY NOTICES UNDER 37 C.F.R. §42.8.....	88
A.	Real Parties-in-Interest.....	88
B.	Related Matters.....	88
C.	Lead and Backup Counsel.....	89
D.	Service Information.....	89

E.	Power of Attorney	90
XII.	FEES	90

PETITIONERS' EXHIBIT LIST

Exhibit No.	DESCRIPTION
1001	U.S. Patent 8,745,749 (“’749 <i>Pat</i> ”)
1002	Declaration of Erez Zadok
1003	Curriculum Vitae of Erez Zadok
1004	File History of U.S. Patent 8,745,749 (Application No. 13/078,323) (“’749 <i>FH</i> ”)
1005	U.S. Provisional Patent Application 61/413,926
1006	U.S. Patent 6,611,907 (“ <i>Maeda</i> ”)
1007	US Patent Publication No. 2002/0080190A1 (“ <i>Hamann</i> ”)
1008	U.S. Patent 6,789,192 (“ <i>Hirota</i> ”)
1009	CN100468438C (“ <i>Lu</i> ”) (with certified translation)
1010	US Patent Publication No. 2012/0272065 (“ <i>Matsukawa</i> ”)
1011	Intellectual Property (IP) Information from the SD Card Association (SD-3C LLC) https://www.sd-3c.com/IPInformation.aspx
1012	A Dictionary of Computing, 6th ed., Oxford University Press (2008), pp. 34 (“backing store”), 194 (“file”) and 196 (“file system”).
1013	Screen Shot of http://www.4centity.com/about.aspx (4C Entity - About Us)
1014	Microsoft Computer Dictionary, 3rd ed., 1997, excerpts (“Microsoft Computer Dictionary”)
1015	DOD Standard, Department of Defense Trusted Computer System Evaluation Criteria, December 26, 1985 (“Orange Book”)

Exhibit No.	DESCRIPTION
1016	U.S. Publication No. 2005/0273858 (“Zadok Patent Publication”)
1017	Smart Card Handbook by Rankl and Effing, 1999-2000, John Wiley & Sons, Ltd., excerpts (“Smart Card Handbook”)
1018	C. P. Wright, M. Martino, and E. Zadok. NCryptfs: A secure and convenient cryptographic file system. In <i>Proceedings of the Annual USENIX Technical Conference</i> , pages 197–210, San Antonio, TX, June 2003. USENIX Association. (“NCryptfs”).
1019	SD Association – Fact Sheet (https://www.sdcard.org/about-sda/fact-sheet/)
1020	November 1, 2024, letter from Ryan Nishimoto to Alfred Fabricant

LISTING OF CHALLENGED CLAIMS

Reference	Claim Limitation
Claim 1	
[1pre]	1. A method for generating a virtual secure digital (SD) card, the method comprising:
[1a]	reading a media key block and media identification for an SD card;
[1b]	storing the media key block and the media identification;
[1c]	creating a file system for secure data on a storage device for storage of secure data corresponding to a secure data area of the SD card; and
[1d]	creating a file system for user data on the storage device for storage of user data corresponding to a user data area of the SD card,
[1e]	wherein a size of the file system for secure data is determinant on a size of the file system for user data, the determination based on a lookup table providing a relationship between the sizes.
Claim 2	
[2]	2. The method of claim 1, wherein the file system for secure data is encrypted.
Claim 3	
[3]	3. The method of claim 2, wherein the file system is encrypted with an encryption key, the encryption key derived from computer system information and the encryption key not stored by the computer system.

Claim 4	
[4]	4. The method of claim 2, wherein the file system is encrypted with an encryption key, the encryption key derived from a computer system and stored by the computer system.
Claim 5	
[5]	5. The method of claim 2, wherein the file system is encrypted with an encryption key, the encryption key derived from a computer system and stored by the computer system within a trusted host.
Claim 6	
[6]	6. The method of claim 2, wherein the file system for secure data and the file system for user data are located on different physical partitions of the storage device.
Claim 7	
[7]	7. The method of claim 2, wherein the file system for secure data and the file system for user data are located on different logical partitions of the storage devices.
Claim 8	
[8]	8. The method of claim 2, wherein the file system for secure data and the file system for user data are within an existing file system.

Claim 13	
[13]	13. The method of any one of claims 1 through 5, wherein the media identification comprises random data not allocated from the SD card.

Claim 14	
[14pre]	14. A method using a virtual secure digital (SD) card, the method comprising:
[14a]	determining if the virtual SD card is provisioned;
[14b]	provisioning the virtual SD card in response to the virtual SD card not being provisioned, the provisioning including:
[14c]	creating a file system for secure data on a storage device for storage of secure data corresponding to a secure data area of the SD card; and
[14d]	creating a file system for user data on the storage device for storage of user data corresponding to a user data area of the SD card,
[14e]	wherein a size of the file system for secure data is determinant on a size of the file system for user data, the determination based on a lookup table providing a relationship between the sizes;
[14f]	accessing the data stored in the secure area of the provisioned virtual SD card; and
[14g]	extracting the data from the secured area of the provisioned virtual SD card.

Claim 15	
[15]	15. The method of claim 14, further comprising performing an authentication using Authenticated Key Encryption (AKE) before

Claim 15	
	accessing the data in the secure area of the provisioned virtual SD card.

Claim 16	
[16]	16. The method of claim 14 or 15, wherein data received from an application program through Authenticated Key Encryption (AKE) is first decrypted.

Claim 17	
[17]	17. The method of claim 14, wherein data received from an application program through Authenticated Key Encryption (AKE) is encrypted with another key before storing the data in the secure area of the provisioned virtual SD card.

Claim 18	
[18pre]	18. A non-transitory computer readable medium configured to store instructions that, when executed, cause at least one processor to:
[18a]	read a media key block and media identification for an SD card;
[18b]	store the media key block and the media identification;
[18c]	create a file system for secure data on a storage device for storage of secure data corresponding to a secure data area of the SD card; and
[18d]	create a file system for user data on the storage device for storage of user data corresponding to a user data area of the SD card,
[18e]	wherein a size of the file system for secure data is determinant on a size of the file system for user data, the determination based on a lookup table providing a relationship between the sizes.

Claim 19	
[19]	19. The computer readable medium of claim 18, wherein the file system for secure data is encrypted.

Claim 20	
[20]	20. The computer readable medium of claim 19, wherein an encryption key is derived from a computer system information, the encryption key not stored by the computer system.

Claim 21	
[21]	21. The computer readable medium of any one of claims 18, 19, or 20, wherein the encryption key is derived from a computer system and stored by the computer system.

Claim 22	
[22pre]	22. A non-transitory computer readable medium configured to store instructions that, when executed, cause at least one processor to:
[22a]	determine if a virtual SD card is provisioned;
[22b]	provision the virtual SD card in response to the virtual SD card not being provisioned, wherein to provision the virtual SD card includes to:
[22c]	create a file system for secure data on a storage device for storage of secure data corresponding to a secure data area of the SD card; and

Claim 22	
[22d]	create a file system for user data on the storage device for storage of user data corresponding to a user data area of the SD card,
[22e]	wherein a size of the file system for secure data is determinant on a size of the file system for user data, the determination based on a lookup table providing a relationship between the sizes;
[22f]	access the data stored in the secure area of the provisioned virtual SD card; and
[22g]	extract the data from the secured area of the provisioned virtual SD card.

Claim 23	
[23]	23. The computer readable medium of claim 22, further comprising: performing an authentication using Authenticated Key Encryption (AKE) before accessing the data in the secure area of the provisioned virtual SD card.

Claim 24	
[24]	24. The computer readable medium of claim 23, wherein data received from an application program through Authenticated Key Encryption (AKE) is first decrypted.

Claim 25	
[25]	25. The computer readable medium of claim 23, wherein data received from an application program through Authenticated Key Encryption (AKE) is encrypted with another key before storing the data in the secure area of the provisioned virtual SD card.

I. INTRODUCTION

Petitioners request *inter partes* review of claims 1-8 and 13-25 of the '749*Pat.*

II. GROUNDS FOR STANDING

Petitioners certify that the '749*Pat* is available for IPR, that Petitioners are not barred or estopped from requesting IPR, and that Petitioners file this Petition within one year of service of Patent Owner's ("PO") district court complaint.

III. STATEMENT OF PRECISE RELIEF REQUESTED FOR EACH CLAIM CHALLENGED

Petitioners respectfully request review and cancellation under 35 U.S.C. §311 as follows:¹

Ground	Claims	Basis ²
1	1, 14-16, 18, 22-24	§103: Maeda-Hamann-AAPA
2	2, 6-8, 19	§103: Maeda-Hamann-AAPA-Hirota

¹ Petitioners do not concede that any challenged claims satisfy other requirements for patentability that cannot be raised in IPR.

² Petitioners' obviousness grounds do not require the bodily incorporation of components from one reference into another, but instead are directed to the application of the teachings of one reference to another.

Ground	Claims	Basis ²
3	3-5, 17, 20, 21, 25	§103: Maeda-Hamann-AAPA-Hirota-Lu
4	13	§103: Maeda-Hamann-AAPA-Matsukawa

Each reference pre-dates the earliest priority date to which the Challenged Claims may be entitled, which is no earlier than January 11, 2010:

Reference	Date	Pre-AIA Art At Least Under
US6,611,907 (“ <i>Maeda</i> ”)	08/26/2003 (issued)	§102(b)
US2002/0080190A1 (“ <i>Hamann</i> ”)	06/27/2002 (published)	§102(b)
Applicant Admitted Prior art (“ <i>AAPA</i> ”)		AAPA
US6,789,192 (“ <i>Hirota</i> ”)	09/07/2004 (issued)	§102(b)
CN100468438C (“ <i>Lu</i> ”)	03/26/2009	§102(b)
US2012/0272065 (“ <i>Matsukawa</i> ”)	02/10/2009 (filed) 10/25/2012 (published)	§102(e)

IV. OVERVIEW OF THE ’749PAT

A. Specification

The ’749pat discloses a “system (and a method) ... for generating a virtual

secure digital (SD) card.” *’749Pat*, Abstract. The specification states that “[s]ecure Digital (SD) cards **are in wide use for many storage applications**,” and that “[t]hey are most commonly used to store audio (MP3 players), pictures (digital cameras), and full motion video (camcorders and HD camcorders).” *’749Pat*, 1:17-20.³ The specification further notes that SD cards “provide[] an acceptable portable storage medium to transfer unprotected content between different devices, especially for the video capture devices mentioned above.” *Id.*, 1:20-23. The patent states that while “[c]onsumers are familiar with the SD card’s basic storage capabilities, ... they are mostly unaware of its security features (the S in Secure Digital).” *Id.*, 1:29-31. According to the patent, this is because “there are very few applications that use this advanced functionality.” *Id.*, 1:31-32. The patent states that digital rights management (“DRM”) is an example of such an application. *Id.*, 1:32-35.

The *’749Pat* recognizes that SD cards use an industry standard DRM known as “content protection for recordable media,” or “CPRM,” and that while CPRM specifies how DRM-protected content can be transferred to other CPRM-complaint devices, it does not provide any standardized method for transferring such content to non-CPRM complaint devices. *Id.*, 1:59-2:25.

The *’749Pat* discloses provisioning a virtual SD card by detecting an SD card,

³ All **bold**/*italics*/underline added unless noted.

reading its media key block and media identification, and storing each on the virtual card. The system also creates a file system for secure data storage corresponding to the SD card's secure data area and creates a file system for user data for storage of user data in an SD card's user data area. *Id.*, 3:4-13. Fig. 2 discloses an exemplary system that reads and writes to SD cards:

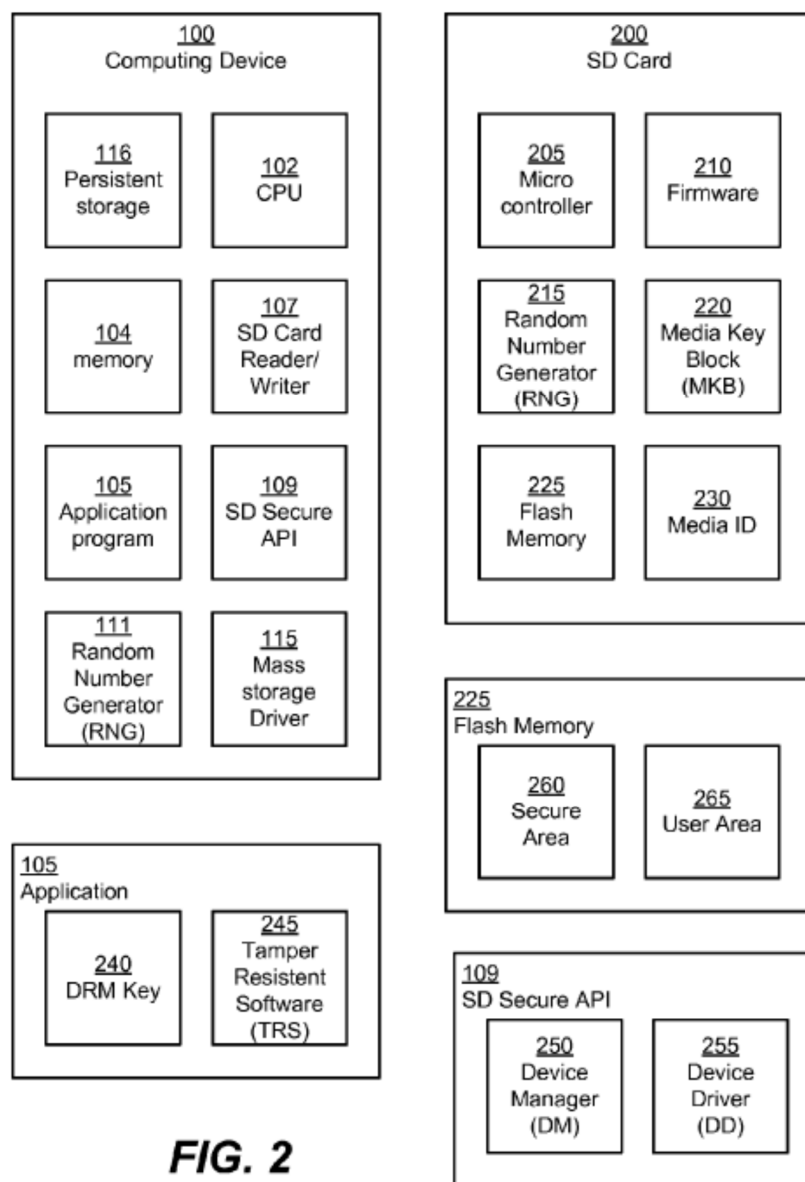


FIG. 2

The system includes a computing device 100 containing, *inter alia*, an SD card reader/writer 107.

Fig. 2 also shows SD card 200, and is described in a section of the specification entitled “Typical SD Card Architecture and Functions.” *Id.*, 4:43. According to the ’749*Pat*, “SD card 200 must conform to the specifications developed and enforced by the SD ASSOCIATION.” *Id.*, 4:45-46.

Thus, the patent admits that a “typical” SD card “includes a microcontroller 205, firmware 210, a random number generator (RNG) 215, a media key block (MKB) 220, flash memory 225, and a media identifier (MID) 230.” ’749*Pat*, 4:56-60. The ’749*Pat* further admits that in “typical” SD cards, “[d]ata is stored within the flash memory 225, which is partitioned into two areas: Secure Area 260 and User Area 265.” *Id.*, 4:60-62. In “typical” SD cards, “secured area 260 may be implemented as a physical or logical device within the SD card as chosen by the SD card's original equipment manufacturer (OEM),” with secure area's 260 size being “determined at design time **according to the SD card specifications**. *Id.*, 4:63-5:1. The ’749*Pat* further admits “that every SD card is provisioned with a secure area 260, even though it may never be used by any application,” and also admits that the user area 265 of a “typical” SD card “may be implemented in the same manner as the secure area 260,” and “also may be either physical or logical partitions depending on implementation within the SD card.” *Id.*, 5:1-6.

The '749Pat also admits to several other features of “typical,” i.e., prior art, SD cards. The patent admits that in “typical” SD cards, DRM key 240 is stored in the computer system 100 “and used to complete an authenticated key exchange with the SD card 200.” *Id.*, 5:42-44. In particular, the '749Pat admits that in SD cards, “the authenticated key exchange is used to gain access the SD card secure area 260 in accordance with the Authenticated Key Exchange (AKE) used by Content Protection for Recordable Media (CPRM) specifications for use with SD cards.” *Id.*, 5:44-49. As of the priority date, POSITAs would have known that “CPRM” specifications were promulgated by the “4C Entity,” which “was formed in 1999 to address the interoperability challenge of sharing premium content among a wide range of digital devices.” <http://www.4centity.com/about.aspx> (EX1013). *Zadok*, ¶¶144-146. Finally, the '749Pat admits that “typical” SD cards have a “media key block (MKB) 220 [that] is structured in accordance with the CPRM specification for SD Cards.” *Id.*, 6:3-4.

The '749Pat's virtual SD card architecture is shown in Fig. 3:

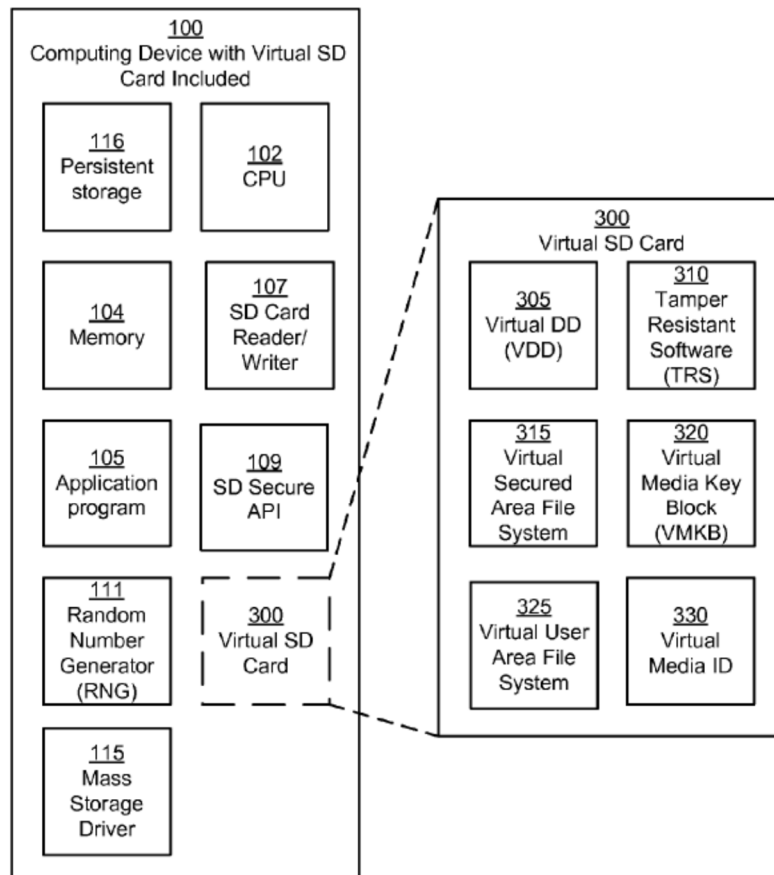


FIG. 3

The “virtual SD card 300 implements in software the functionality previously implemented by SD card 200 in hardware.” ’749Pat, 6:6-8. Virtual SD card 300 includes, *inter alia*, a virtual secure area filed system 315, virtual media key block 320, virtual user area file system 325, and virtual media identification (ID) 330. *Id.*, 6:37-40. Virtual secure area filed system 315 and virtual user area file system 325 can either “be implemented as file systems within an encrypted file” or “as physical or logical partitions on the same or separate devices, with or without encryption

depending on the overall system security requirements.” *Id.*, 6:50-56.

The '749*Pat* states that “secured area file system 315 is configured as a storage area for secure data.” *Id.*, 6:64-65. To protect the data in that secured storage area, the data is encrypted using an encryption key. This encryption key “is derived from the computing device's unique information (*e.g.*, processor serial number, bios serial number, device serial number), and hidden information effectively binding the file systems to the computer system 100” in which the virtual SD card is operating. *Id.*, 7:2-6.

The method for provisioning virtual SD cards is shown in Fig. 4:

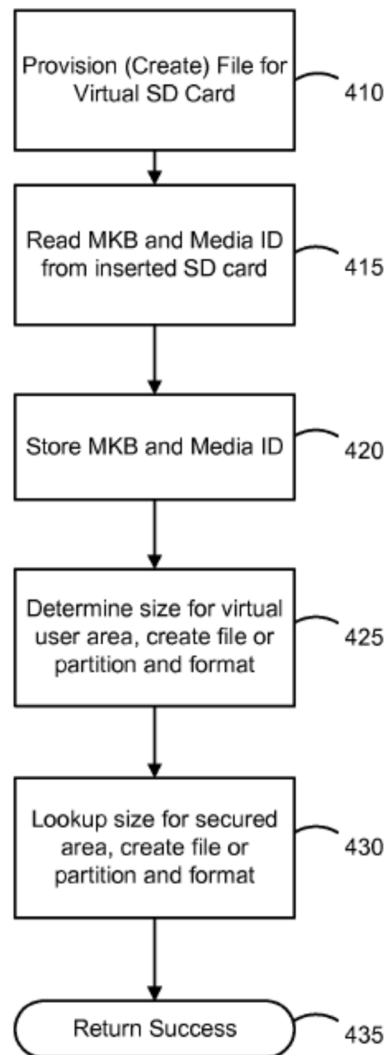


FIG. 4

See also '749Pat, 7:45-58. This method includes creating a file or partition on the storage 116 formatted for the virtual user area 325. The size of the secured area file system 315 is determined at step 425 in accordance with SD card specifications, which requires that “[t]he size of the virtual secured area file system 315 is a table lookup from SD ASSOCIATION specifications based on the size of the virtual user

area file system 325.” ’749*Pat*, 7:59-67.

B. Prosecution History

The ’749*Pat* was filed on 04/01/2011, and claimed the benefit of provisional application 61/413,926, filed on 11/15/2010. For purposes of this petition, Petitioners assume the priority date is 11/15/2010. The original application contained 27 claims. On 07/01/2013, the Examiner issued an office action. In addition to certain rejections under 35 U.S.C. §§ 101 and 112, the Office Action rejected claims 1, 10, 15-18 19, and 24-27 as obvious, and indicated that claims 2-9 and 11-14 would be allowable if rewritten in independent form. *EX1004* at 74-88. In the “statement of reasons for the indication of allowable subject matter,” the Examiner indicated the following:

The technique of memory allocation as set forth in claim 2 wherein a lookup table is utilized to allocate memory shared between user data and secure data in a virtual SD card appears to be novel and unobvious.

Id. at 83. Application claim 2 recited that “a size of the file system for secure data is determinant on a size of the file system for user data, the determination based on a lookup table providing a relationship between the sizes.” *Id.* at 174.

On 10/01/2013, patentee responded to the Office Action by amending application claim 2 to include the limitations of application claim 1, and amending independent application claims 15, 19 and 24 to include application claim 2’s

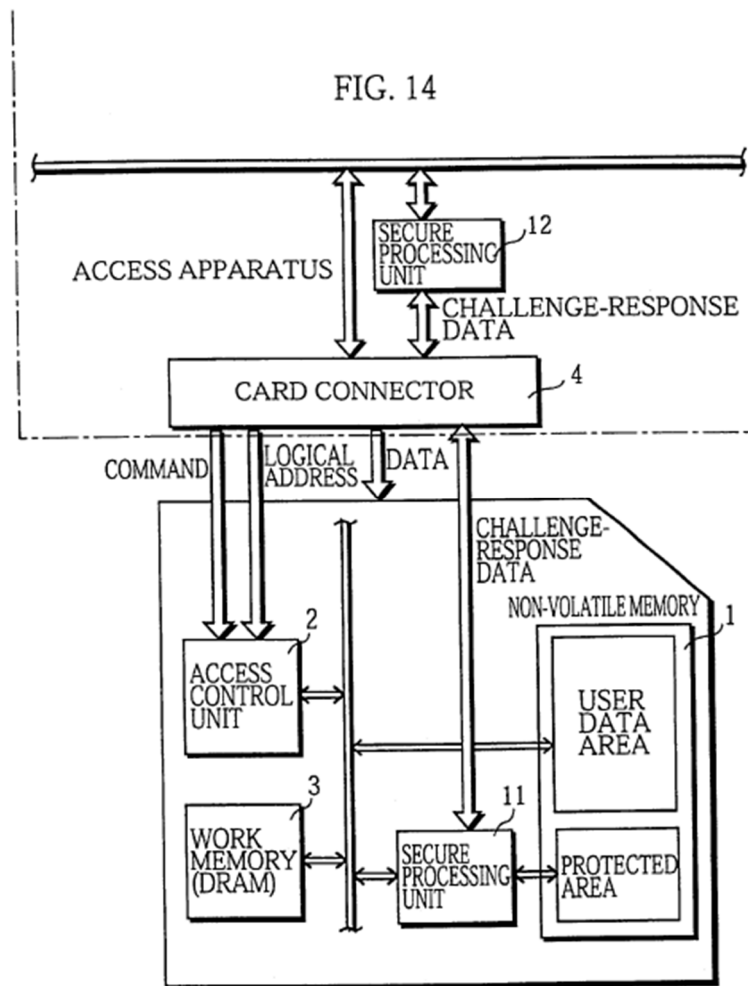
limitations. *Id.* at 45-54. *Id.* at 174.

V. PRIOR ART

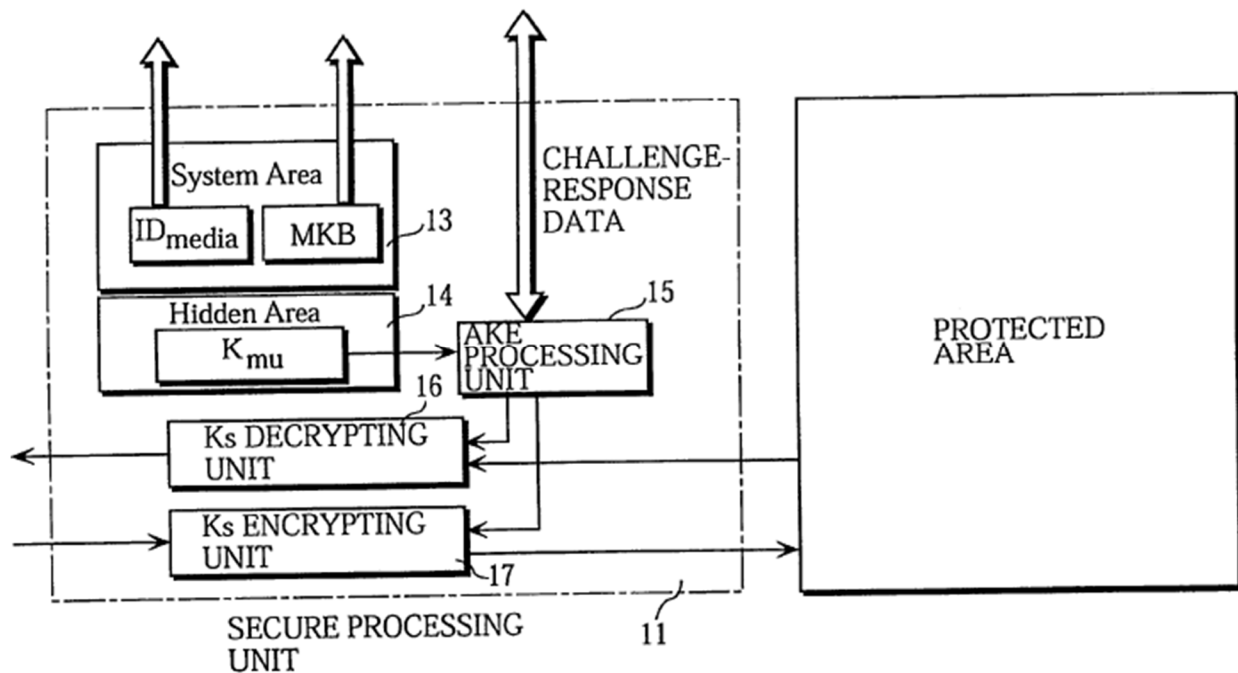
A. *Maeda*

Maeda issued on 08/26/2003, making it prior art under pre-AIA 35 U.S.C. §102(b). Persons having ordinary skill in the art (“POSITAs”) would have recognized that *Maeda* discloses the general architecture of SD Cards. *Zadok*, ¶165.⁴ Fig. 14 shows *Maeda*’s architecture:

⁴ *Maeda* is designated as an “essential patent” by the SD Card Association. *See EX1011*.



As seen, *Maeda*'s SD cards have a non-volatile memory storage area where a "user can gain access (the user data area), and an area that stores data securely (the protected area)." *Maeda*, 13:30-33. As is also seen, this SD card also has a secure processing unit 11, the details of which are shown in Fig. 15:



Maeda's SD cards have a "system area 13," in which SD cards read and store a media key block and media ID from an "access apparatus 200." *Id.*, 13:49-54. *Maeda* discloses that before accessing the secure area of an SD card, AKE processing unit 15 performs "authentication and key exchange," or "AKE." *Id.*, 13:62-14:3. *Maeda* also discloses that data stored within the secure data file system is encrypted. *Id.* at 14:57-62; *see also id.*, 13:62-67, 14:3-31.

Maeda further discloses that the size of the file system for secure data and the file system for user data are calculated such that they each have a size that is relative to the other. *See id.* at 15:12-21, 17:1-11, Figs. 16, 17, and Claim 7.

B. *Hamann*

Hamann published on 06/27/2002, making it prior art under pre-AIA 35

U.S.C. §102(b). *Hamann* describes a system for the “secure back-up and usage of secure copies of smart card data objects, especially in the case when the smart card is lost or damaged or data objects stored on the smart card are not accessible or destroyed.” *Hamann*, ¶[0001]. *Hamann*’s method “provid[es] a virtual smart card (VSC) having the same defined logical file structure and the same content of data objects as its assigned real smart card...” *Id.*, ¶[0014]. *Hamann* describes a smart card as “any programmed data carrier used in any portable device, like mobile phone, digital personal assistant etc., to securely hold subscriber specific information” (*id.*, ¶[0002]) and a VSC as “a software implemented version of a real smart card providing the equivalent functionality of a real smart card” (*id.*, ¶[0015]).

Hamann discloses “a VSC control program handling the creation, the security and the read/write process of the VSC.” *Id.*, ¶[0015]. The result is a “VSC having a logical file structure comprising a public area, a private area, a secure key area, password area, and an unique identifier area.” *Id.*, ¶[0016]. The VSC file system is shown in Fig. 1 (annotated):

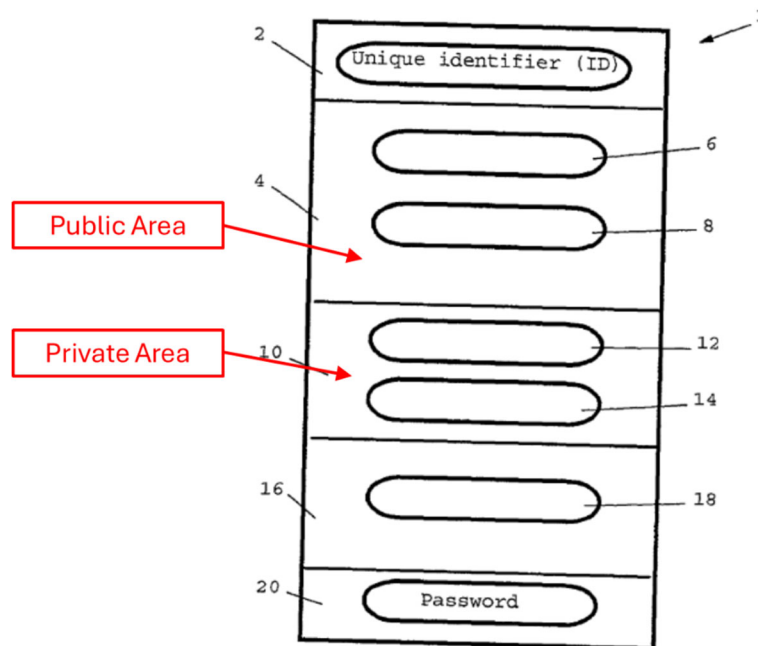


FIG. 1

As seen, the file system for *Hamann's* VSC includes a public area and a private area. The public area stores “public data objects having no access conditions,” while the private area stores “private objects” that have been encrypted. *Id.*, ¶¶[0025]-[0027].

C. *AAPA*

The *'749Pat* admits that SD cards “are in wide use for many storage applications.” *'749Pat*, 1:17-18. The *'749Pat* further admits that SD cards “must conform to the specifications developed and enforced by the SD ASSOCIATION.” *Id.*, 4:45-47. Even putting aside the *'749Pat's* admissions, POSITAs reviewing the patent would have known that the SD Association existed before the *'749Pat's* priority date, as did its SD card specifications. *Zadok*, ¶182.

Patentee's admissions in the '749Pat regarding the fact that the structure, function and operation of SD cards were prior art are binding, and can be used when determining whether a claim is obvious. *Pharmastem Therapeutics, Inc. v. Viacell, Inc.*, 491 F.3d 1342, 1362 (Fed. Cir. 2007); *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1570 (Fed. Cir. 1988).

According to The Director's 06/09/2022 Updated Guidance On The Treatment Of Statements Of The Applicant In The Challenged Patent In Inter Partes Reviews Under § 311, "[a] patentee's admissions regarding the scope and content of the prior art under § 103 can be used, for example, to: (1) supply missing claim limitations that were generally known in the art prior to the invention..." Guidance, at 4. The Director's Guidance also states that "[a]dmissions may include statements in the specification of the challenged patent such as 'It is well known that ... ,' 'It is well understood that ... ,' or 'One of skill in the art would readily understand that ... ,' or may describe technology as 'prior art,' 'conventional,' or 'well-known.'" See also *McCoy v. Heal Sys., LLC*, 850 F. App'x 785, 789 (Fed. Cir. 2021) ("By characterizing certain parts as conventional in the specification, the patentee effectively admits that such things would be known to a POSA").

As discussed in §IV.A, the '749Pat describes the "**Typical** SD Card Architecture and Functions" ('749Pat, 4:43-6:4) and the fact that SD cards "**must** conform to the specifications developed and enforced by the SD ASSOCIATION"

(’749*Pat*, 1:17-18). Referring to “typical” SD cards is no different than stating these disclosures are “well known,” “well understood,” “prior art,” or “conventional,” which the Director’s Guidance indicates are prior art admissions. Thus, any descriptions of the structure, function, and operation of “typical” SD cards, as well as any statements regarding the contents of the SD Card Association’s specifications are Applicant Admitted Prior Art, and can be used to “supply missing claim limitations that were generally known in the art prior to the invention.” *See also Unified Patents Inc. v. Autoloxer LLC*, IPR2017-01271, Paper 7 (PTAB October 2, 2017), where the Board instituted trial on an obviousness challenge relying on the challenged patent’s admission that an industry standard described a claim feature. *Id.*, at 15-16.

That the ’749*Pat* states that SD cards “**must** conform” to the SD Card Association’s specifications demonstrates thatPOSITAs would have understood that the ’749*Pat*’s description of various features of SD cards were in the prior art. *Zadok*, ¶183.

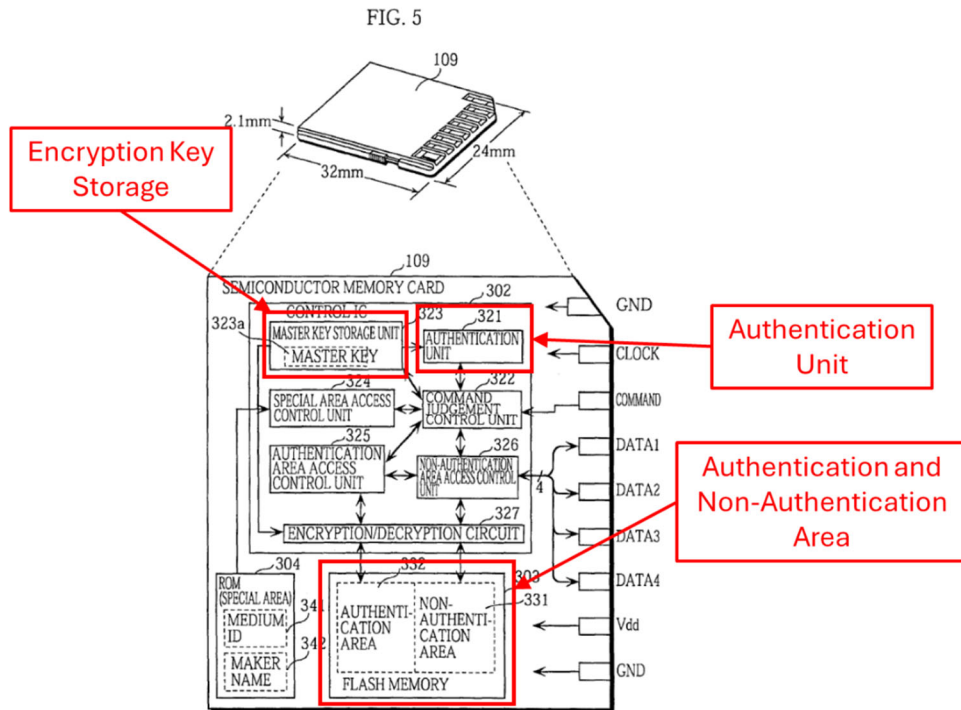
The ’749*Pat* provides extensive details regarding “typical” SD cards, as described in §IV.A. A key prior art admission in the ’749*Pat* is that the “size of the **secured area file system 315 is determined at provisioning time according to the SD card specifications. The size of the virtual secured area file system 315 is a table lookup from SD ASSOCIATION specifications** based on the size of the

virtual user area file system 325. '749*Pat*, 7:62-8:2.

D. *Hirota*

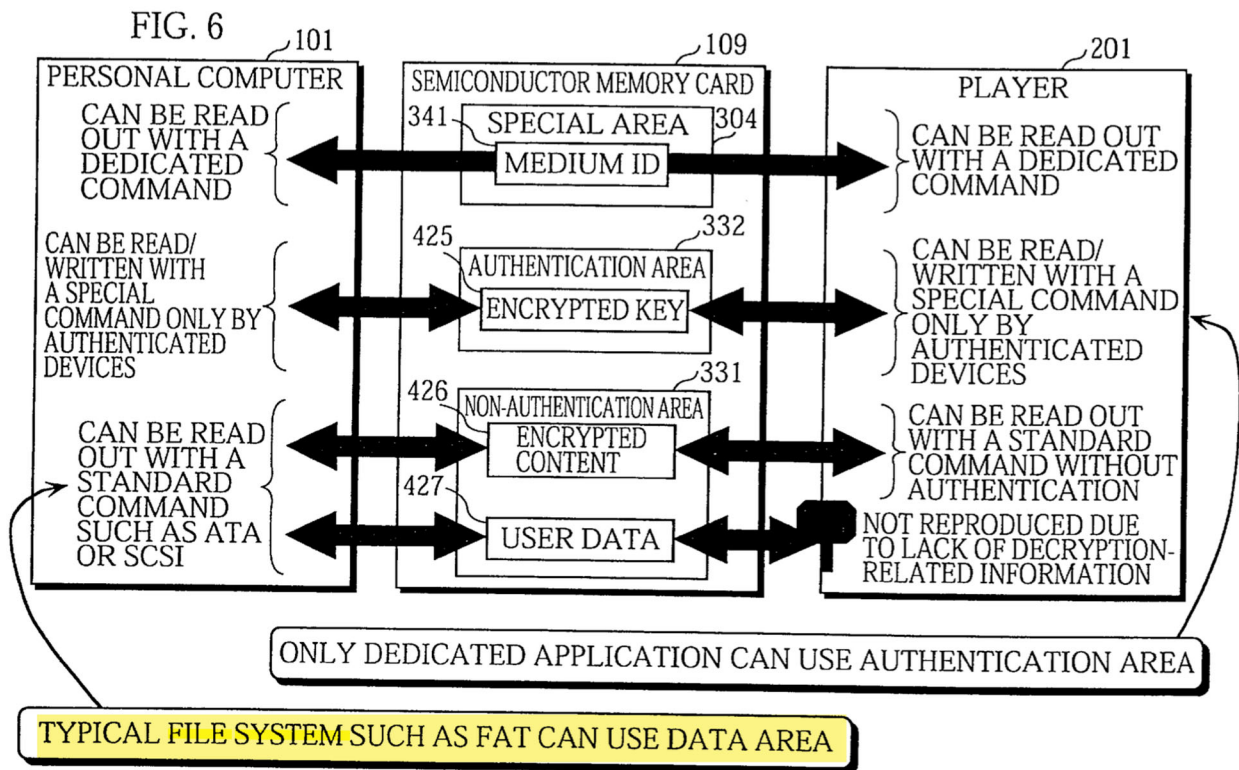
Hirota issued on 09/07/2004, making it prior art under pre-AIA 35 U.S.C. §102(b). *Hirota* discloses “a semiconductor memory card that can be used as a storage medium for storing digital contents and as a storage medium for storing general-purpose computer data (not an object of copyright protection).” *Hirota* at 2:3-7.⁵ Similar to *Maeda*, *Hirota* discloses that its semiconductor memory card includes flash memory 303 having “an authentication area and a non-authentication area,” which is shown in Fig. 5 (annotated):

⁵ *Hirota*, is designated as an “essential patent” by the SD Card Association. *See* <https://www.sd-3c.com/IPInformation.aspx>.



See also *Hirota*, 10:27-36.

Hirota's Fig. 6 (annotated below) provides additional information regarding its storage architecture:



As can be seen, *Hirota's* non-authentication area 331 includes both encrypted content 426 and user data 427. *See also Hirota*, 12:47-51. *Hirota* also discloses that the encryption key 425 for encrypted content 426 is stored in authentication area 332. *Id.*, 12:51-54.

E. *Lu*

Lu was published on 03/11/2009, making it prior art under pre-AIA 35 U.S.C. §102(b). *Lu* discloses “encryption and decryption methods for implementing hardware and software binding.” *Lu* at 1. *Lu* discloses that to effect this binding, an encryption key is derived from the computer system. *See Lu* at Abstract; *see also Lu* at 5.

F. *Matsukawa*

Matsukawa has a priority date of 02/10/2009, was published on 10/25/2012, making it prior art under pre-AIA 35 U.S.C. §102(e). *Matsukawa* discloses an authentication method for use in memory devices, including SD cards. *Matsukawa*, ¶¶[0003], [0007]. *Matsukawa* states that SD cards and host computers “generate the same session key for each authentication process between the host computer and the recording medium (SD card).” *Id.*, ¶[0007]. To do so, *Matsukawa* discloses a “media ID generating module 130 [having] the function of generating the media ID in such a manner as not to duplicate a media ID generated in the past.” *Id.*, ¶[0051].

VI. LEVEL OF ORDINARY SKILL IN THE ART

POSITAs at the time of the alleged invention of the '749*Pat*, which for purposes of this proceeding is no earlier than 11/15/2010, would have had a bachelor's degree computer science, computer engineering, or equivalent degree, and approximately two years of experience working in the computer science or engineering field. Additional experience might substitute for less education and vice versa. Additionally, POSITAs in November 2010 would have been familiar with the design and implementation of data storage and/or file systems, as well as storage security and privacy techniques. *Zadok*, ¶¶33-34.

VII. CLAIM CONSTRUCTION

Petitioners are unaware of any relevant prior claim construction

determinations. *See* 37 C.F.R. §42.100(b). Given the close correlation and substantial identity between the prior art and the challenged claims, Petitioners believe that no express constructions of the claims are necessary, except as noted herein.

A. “File System”

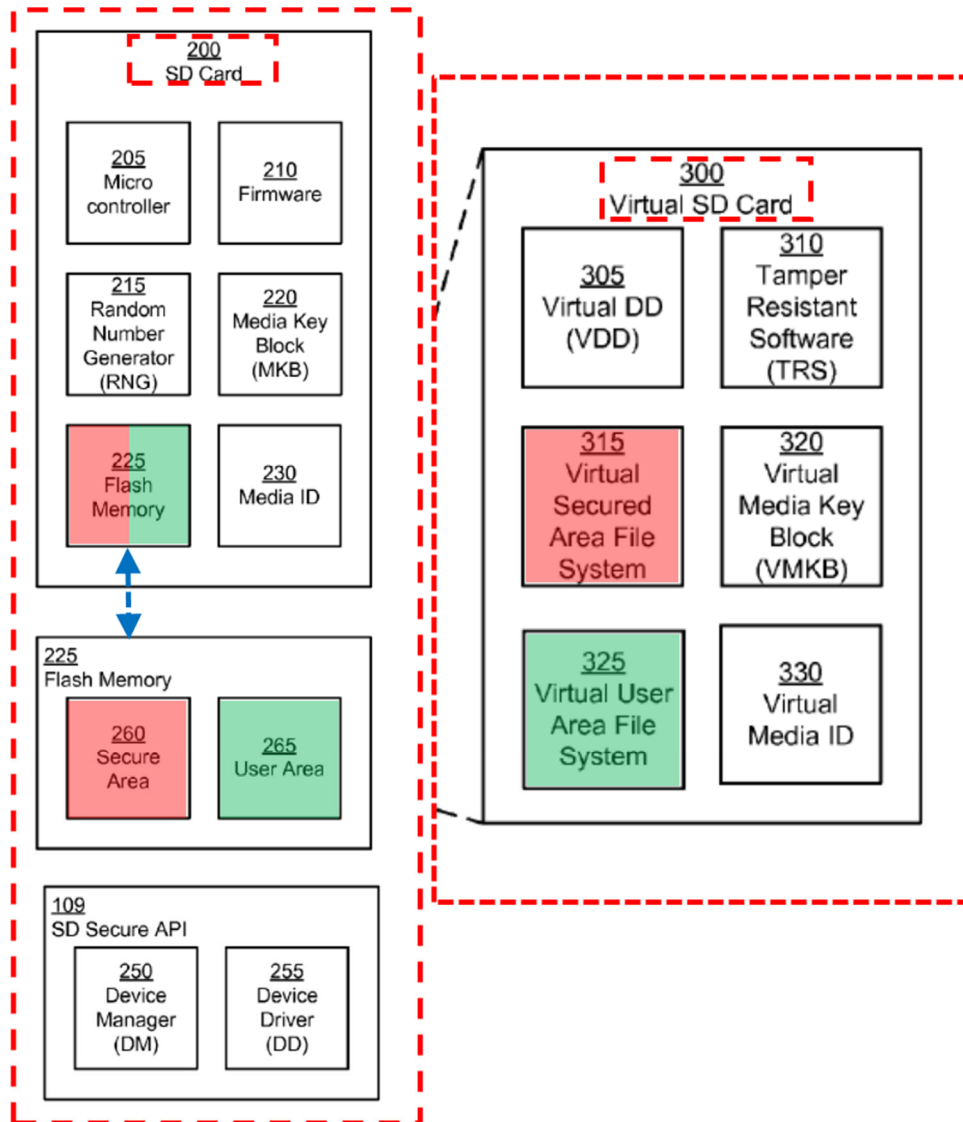
The independent claims of the '749*Pat* recite “a **file system** for secure data on a storage device for storage of secure data corresponding to a secure data area of the SD card” and “a **file system** for user data on the storage device for storage of user data corresponding to a user data area of the SD card.” The patent does not explicitly define what it means by the term “file system.” Normally, the term “file system” means a “[t]he part of a computer’s backing store where files are held.”⁶ *EX1012*, p. 196. *Zadok*, ¶200.

Certain claims, *e.g.*, challenged claims 2-3 and 19 recite that “the file system

⁶ A “backing store” is “memory on which information is held for reference but not for direct execution. . . The term may be used either in an absolute sense, in which case it usually refers to a disk, or it may be used in a relative sense to refer to the device next down in the memory hierarchy” and “file” is “[a] collection of information, referred to by *file name; for example, a user-created document, program data, or the program itself.” *See EX1012*, pp. 34, 194.

for secure data is encrypted.” Moreover, when referring to “file systems,” the *'749Pat* explains that “the system creates a file system for secure data storage corresponding to the SD card's secure data area and creates a file system for user data for storage of user data corresponding to the SD card's user data area.” *'749Pat*, 3:8-11. The *'749Pat* goes on to state that “[t]he secured area file system 315 is configured **as a storage area for secure data**” (*id.*, 6:64-65) and that the “user area file system file system 325 is a **storage area for unsecured data**.” (*id.*, 7:26-27).

Thus, POSITAs would have understood that when the *'749Pat* refers to a “file system” for either secure data or user data, it is referring to a storage area that stores either secure data or user data), which is consistent with the ordinary meaning discussed above. *Zadok*, ¶203. That this is the case is seen by comparing how the *'749Pat* depicts a physical and virtual SD cards. The right-hand side of Fig. 2 shows the various portions of a “typical” SD card 200. The right-hand side of Fig. 3 shows the various portions of virtual SD card 300. Below, each are placed side-by-side and are color-coded to show corresponding components:



As can be seen, a typical SD card 200 has a “secure area 260,” highlighted in red, and a “user area 265,” highlighted in green. The virtual SD card 300 is essentially the same, having a “virtual secured area file system 315,” highlighted in red, and a “virtual user area file system 325,” highlighted in green. Thus, POSITAs would have understood that the term “file system” means “a storage area.” *Zadok*, ¶¶203-204.

VIII. DETAILED EXPLANATION OF GROUNDS

A. Ground 1: *Maeda-Hamann-AAPA* Renders Claims 1, 14-16, 18, 22-24 Obvious

1. Claim 1

a. [1pre]⁷

To the extent the preamble is limiting, *Maeda-Hamann-AAPA* discloses/suggests this feature. *Zadok*, ¶¶205-210. *Maeda* discloses the architectural features of SD cards, which, by the priority date, was well-known, as they had been available to the public for years, a fact that the '749*Pat* admits. '749*Pat*, 1:17-18 (“Secure Digital (SD) cards are in wide use for many storage applications.”). The '749*Pat* states that SD cards were required to conform to industry standards promulgated by the SD Association, the standards setting organization that developed the devices. *Id.*, 4:45-46 (“The SD card 200 **must conform** to the specifications developed and enforced by the SD ASSOCIATION.”). Thus, POSITAs would have been familiar with SD cards, their architecture, and their uses. *Zadok*, ¶205. Indeed, *Maeda* (and the *AAPA*) demonstrates that SD card architecture was well-known to POSITAs before the priority date. *Id.*

⁷ The claim language is reproduced in LISTING OF CHALLENGED CLAIMS.

Hamann discloses “a method and system for secure back-up and usage of secure copies of smart card data objects.” *Hamann*, ¶[0001]. To do so, *Hamann* “provid[es] a virtual smart card (VSC) having the same defined logical file structure and the same content of data objects as its assigned real smart card...” *Id.*, ¶[0014]. *Hamann*’s VSC is “a software implemented version of a real smart card providing the equivalent functionality of a real smart card. *Id.*, ¶[0015]. *Hamann* describes a smart card as “any programmed data carrier used in any portable device ... to securely hold subscriber specific information.” *Id.*, ¶[0002]. While *Hamann* does not explicitly disclose that the smart card being virtualized is an SD card, POSITAs would have understood that SD cards fall within *Hamann*’s smart card definition, as SD cards are data carriers that are portable and can be used in portable devices. *Zadok*, ¶¶206-207. Indeed, POSITAs would not have found meaningful differences between smart cards and SD cards in the context of the ’749Pat. *Id.*

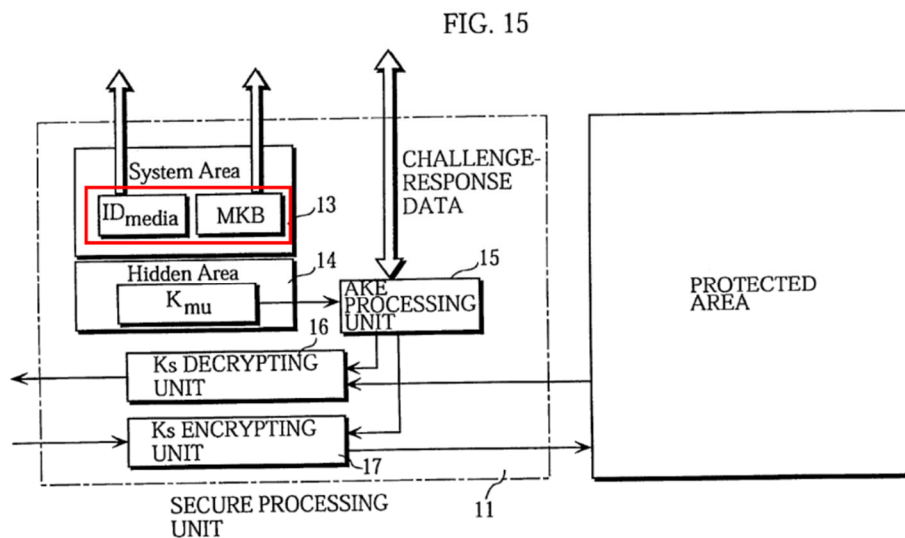
Because *Maeda* and the *AAPA* describe an SD card, and *Hamann* discloses virtualizing similar memory cards, *Maeda-Hamann-AAPA* discloses the preamble. POSITAs would have been motivated to combine *Maeda*, the *AAPA* and *Hamann* for the reasons discussed in §VIII.A.2.

b. [1a]

Maeda-Hamann-AAPA discloses/suggests this feature. *Zadok*, ¶¶211-222.

This element requires reading the media key block and media identification “for an SD card,” which POSITAs would understand includes reading these items from a physical SD card, although they could be read from elsewhere. The *'749Pat* admits that prior art SD cards stored both the media key block (“MKB”) and media identification (*see '749Pat*, 4:57-60). Note that POSITAs would have understood that an SD card’s “media identification” is a number, a portion of which is unique to a particular SD card, and that SD cards use the “media key block” to encode and decode data stored therein. *Zadok*, ¶212.

Maeda also discloses SD card media IDs and media key blocks. *See* Fig. 15 (annotated):



Consistent with SD card standards described in the *AAPA*, *Maeda* discloses that “[t]he system area 13 is a read-only area storing a media key block (MKB) and a media-ID,” and that “[t]he MKB and media-ID stored in this area cannot be

rewritten.” *Maeda*, 13:49-51.

Maeda also discloses that its SD card “is connected to an access apparatus 200, and the MKB and media-ID is read by that access apparatus 200.” *Id.*, 13:52-54. Thus, POSITAs would have recognized that *Maeda* discloses this element. *Zadok*, ¶¶213-215.

To create its VSC, *Hamann* discloses that the physical smart card must be read by a reader, shown in Fig. 2:

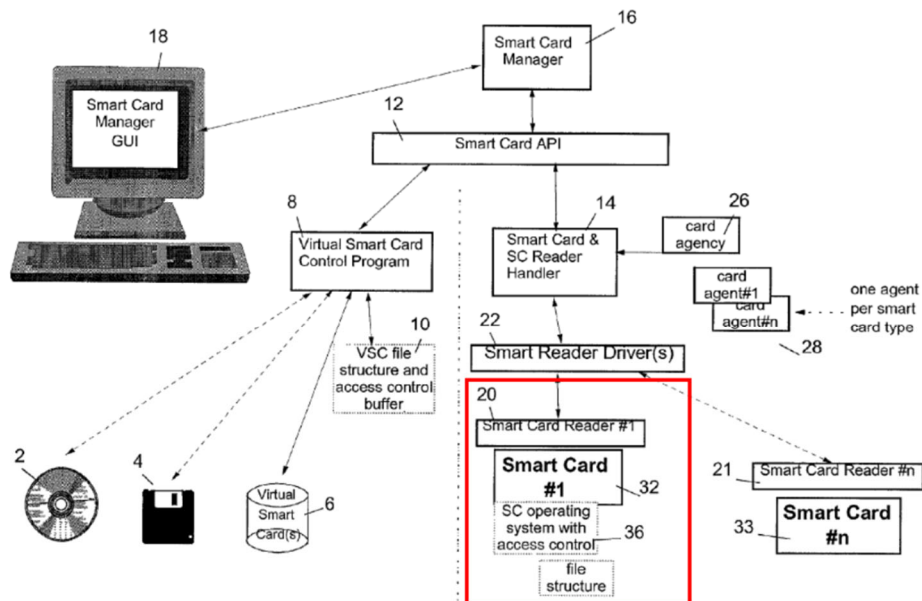


FIG. 2

See also *Hamann*, ¶[0043]. To create a VSC, the “smart card is inserted into a smart card reader and the smart card manager is started.” *Id.*, ¶[0048]. After entering a password, *Hamann*’s “smart card manager displays all public and private data objects stored on the smart card.” *Id.*, ¶[0049]. POSITAs would have understood that when *Hamann* virtualizes an SD card like that described in *Maeda* (and the

AAPA), the SD card's media key block and media identification would be read, just as claimed. *Zadok*, ¶¶216-217.

Moreover, the smart cards that *Hamann* virtualizes are similar to the SD cards described in *Maeda* and the *AAPA*. *Hamann* discloses that its VSC has “the same defined logical file structure and the same content of data objects as its assigned real smart card...” *Id.*, ¶[0014]. *Hamann* further discloses that its VSC has “public area, a private area, a secure key area, password area, and an unique identifier area.” *Id.*, ¶¶[0014], [0025]-[0030]. POSITAs would have recognized that this is similar to SD cards, which have a user data area and a protected area that stores data securely. *Maeda*, 13:30-33. *Hamann* also discloses that its VSC has a “unique identifier (ID),” which *Hamann* states “should be specified using the serial number of the real smart [sic: card] to be assigned to the new VSC.” *Hamann*, ¶[0050]. POSITAs would have recognized that the “serial number of the real smart [card]” is analogous to an SD card's media identifier (*e.g.*, both being unique numbers), and would have further understood that for *Hamann* to assign a unique identifier using that serial number, it would have had to read it, just as claimed. *Zadok*, ¶¶219-220.

Thus, when the smart card being virtualized using *Hamann* is an SD card like that in *Maeda* (and the *AAPA*), the *Maeda-Hamann* combination would read the MKB and media-ID stored on *Maeda*'s (and the *AAPA*'s) SD card. *Id.*, ¶221.

c. [1b]

Maeda-Hamann-AAPA discloses/suggests this feature. *Zadok*, ¶¶223-228. As discussed in §VIII.A.1.b, *Maeda* discloses that SD cards have media key blocks and a media-IDs. POSITAs would have understood that when using *Hamann* to create a virtual SD card like those in *Maeda* (and the *AAPA*), *Hamann*'s VSC control program will store the virtual SD card on a storage medium, such as a hard disk. *Hamann*, ¶[0040]. POSITAs would have further understood that the SD card's media key block and media identification would be stored on that media since *Hamann* discloses that the VSC it creates has "the same defined logical file structure and the same content of data objects as its assigned real smart card..." *Hamann*, ¶[0014]. *Zadok*, ¶¶223-224.

Moreover, as discussed in §VIII.A.1.b, *Hamann* discloses that its VSC has a "unique identifier (ID)" that uses "the serial number of the real smart [sic: card] to be assigned to the new VSC." *Hamann*, ¶[0050]. As discussed, POSITAs would have understood that the "serial number of the real smart [card]" is analogous to an SD card's media identifier. Therefore, POSITAs would have understood that *Hamann*, suggests storing *Maeda*'s (and the *AAPA*'s) media identifier. *Zadok*, ¶225.

Hamann's Fig. 1 shows the file structure of its VSC, and it shows that its unique ID (i.e., the claimed "media identification") is stored as part of its VSC:

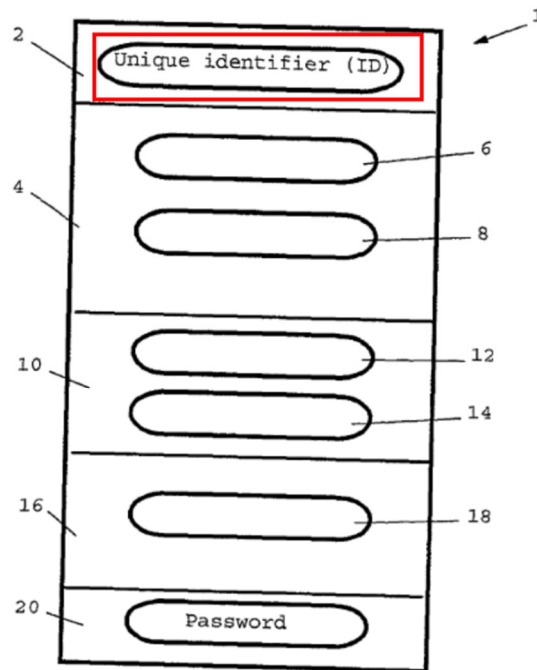
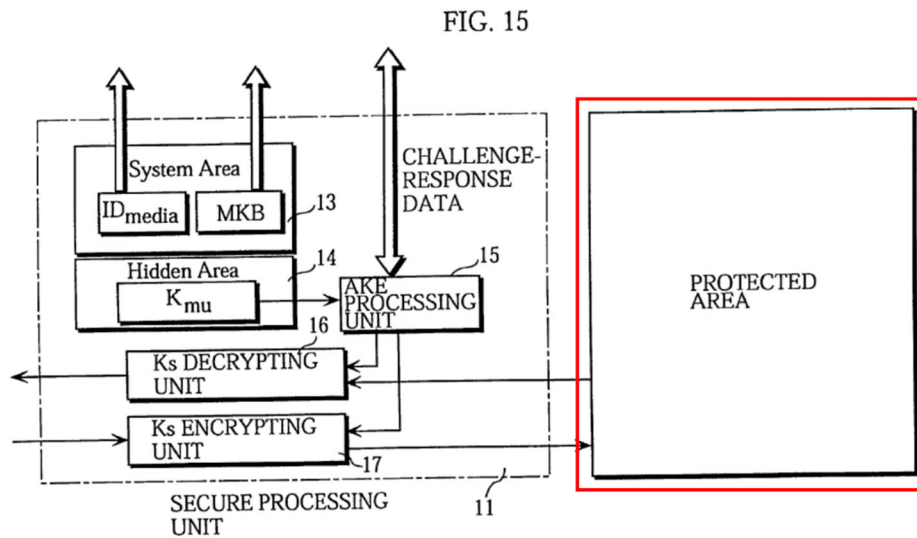
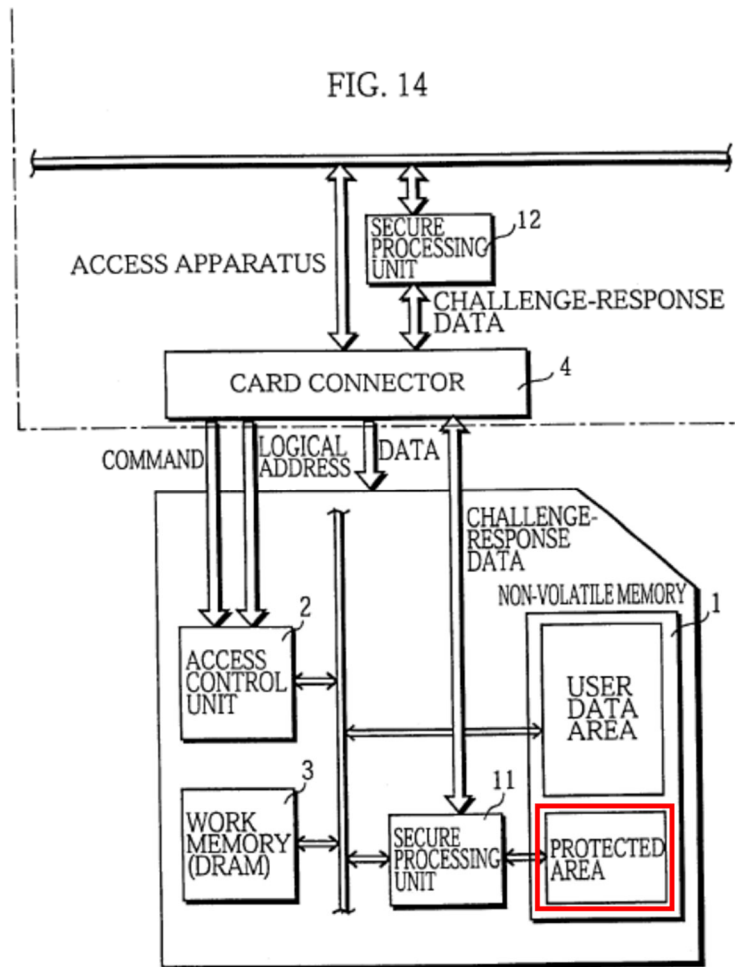


FIG. 1

Thus, when the smart card being virtualized using *Hamann* is an SD card like that in *Maeda* (and the *AAPA*), POSITAs would have understood that the *Maeda-Hamann* combination would store *Maeda*'s (and the *AAPA*'s) media key block and the media identification as part of its virtual SD card. *Zadok*, ¶¶226-227.

d. [1c]

Maeda-Hamann-AAPA discloses/suggests this feature. *Zadok*, ¶¶229-237. *Maeda* discloses that SD cards have what it refers to as a "protected area," shown, *e.g.*, in Figs. 14-15 (annotated):



Maeda discloses that its SD cards have a non-volatile memory storage area where a

“user can gain access (the user data area), and **an area that stores data securely (the protected area)**.” *Maeda*, 13:30-33. *See also, id.*, 2:61-3:3, 13:36-41. *Zadok*, ¶¶229-230.

Likewise, the *AAPA* admits that “typical,” i.e., prior art, SD cards included a “file system for secure data on a storage.” *’749Pat*, 4:60-62 (“Data is stored within the flash memory 225, which is partitioned into two areas: **Secure Area 260** and User Area 265.”). Indeed, the *’749Pat* admits “that every SD card is provisioned with a secure area 260, even though it may never be used by any application.” *Id.*, 5:1-3. *Zadok*, ¶231.

As discussed, *Hamann* discloses that its “virtual smart card (VSC) [has] the same defined logical file structure and the same content of data objects as its assigned real smart card.” *Hamann*, ¶[0014]. Thus, POSITAs would have understood that when *Hamann*’s teachings are used to virtualize an SD card as in *Maeda* (and the *AAPA*), the resulting virtual SD card would have the “same defined logical file structure and the same content of data objects as its assigned real smart card.” *Zadok*, ¶232. This means that the resulting virtual SD card would have a “file system,” i.e., a “storage area” of a virtual SD card, “for secure data on a storage device for storage of secure data corresponding to a secure data area of the SD card,” just as claimed. *Id.*

Note also that *Hamann* creates a VSC having private area 10, as seen in Fig.

1 (annotated):

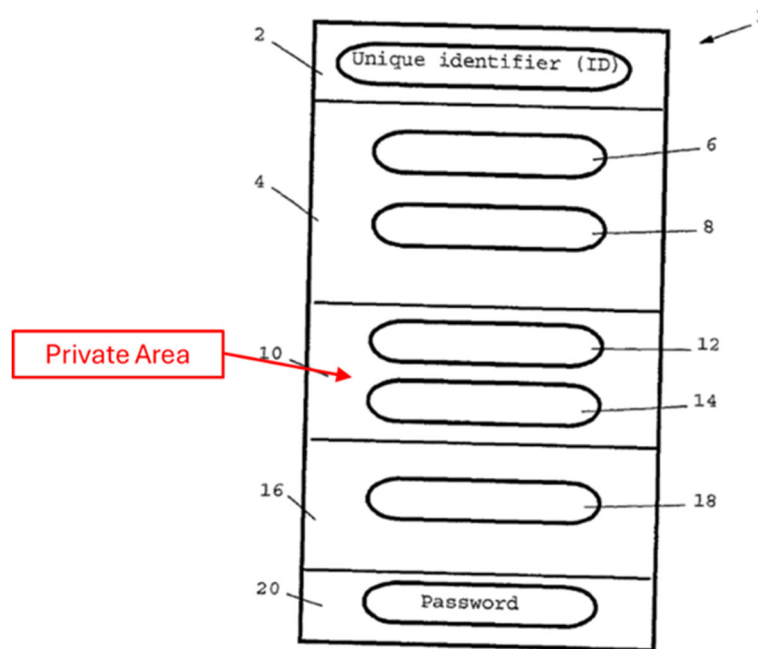


FIG. 1

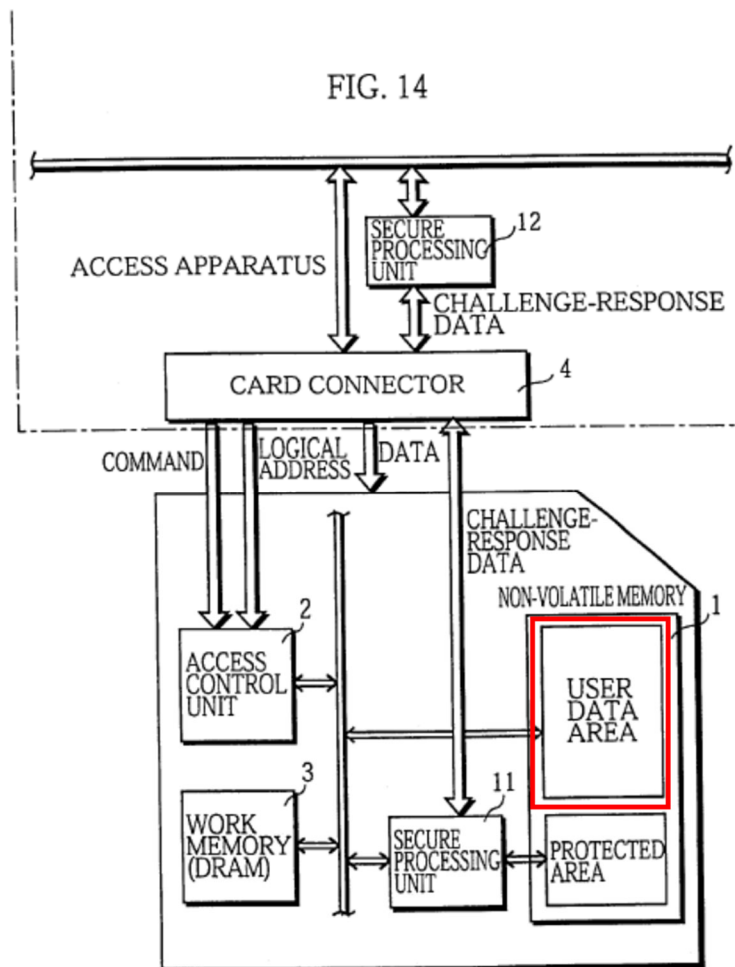
Hamann describes the private area in Fig. 1. *See Hamann*, ¶¶[0025]-[0027] (“[0025] The logical file structure of the VSC (1) is preferably defined by the following data areas: ... [0027] (a private area (10) in which private objects being encrypted are placed; private objects may only be accessed providing a password (10), *e.g.* account no (12) and key information (14)”). *Zadok*, ¶¶233-234.

Hamann discloses “a VSC control program handling the creation, the security and the read/write process of the VSC,” which generates a “**VSC having a logical file structure** comprising a public area, **a private area**, a secure key area, password area, and an unique identifier area.” *Id.*, ¶¶[0015]-[0016]. *Hamann’s* private area

stores “private objects” are “being encrypted.” *Id.*, ¶¶[0016], [0027]. POSITAs would have understood that *Hamann*’s “private area,” which has a “logical file structure,” corresponds to the claimed “file system for secure data on a storage device for storage of secure data corresponding to a secure data area of the SD card,” especially when combined with *Maeda* (and the *AAPA*). *Zadok*, ¶¶235-236.

e. [1d]

Maeda-Hamann-AAPA discloses/suggests this feature. *Zadok*, ¶¶238-247. *Maeda* discloses that SD cards have what it refers to as a “user data area,” shown, *e.g.*, in Fig. 14 (annotated):



Maeda discloses that its SD cards have a non-volatile memory storage area where a **“user can gain access (the user data area),** and an area that stores data securely (the protected area).” *Maeda*, 13:30-33. *See also, id.*, 2:61-3:3, 13:36-41. *Maeda* further discloses that its user data area is “for recording user data.” *Maeda*, 1:60-61. As discussed, *Maeda* discloses that SD cards use an FAT file system. *See e.g.*, Figs 1C, 5, 12-13, 10:51-67, 11:11-25. *Zadok*, ¶¶238-239.

Likewise, the *AAPA* discloses that “typical,” *i.e.*, prior art, SD cards included a “file system for secure data on a storage device.” *See ’749Pat*, 4:60-62 (“Data is

stored within the flash memory 225, which is partitioned into two areas: Secure Area 260 and **User Area 265**.”). Thus, POSITAs would have realized that prior art SD cards like those described in *Maeda* (and the *AAPA*) included “a file system for user data on the storage device for storage of user data,” just as claimed. *Zadok*, ¶¶240-241.

As discussed, *Hamann* discloses that its VSC has “the same defined logical file structure and the same content of data objects as its assigned real smart card.” *Hamann*, ¶[0014]. Thus, POSITAs would have understood that when *Hamann*’s teachings are used to virtualize an SD card as in *Maeda* (and the *AAPA*), the resulting virtual SD card would have “same defined logical file structure and the same content of data objects as its assigned real smart card.” *Zadok*, ¶242. This means that the resulting virtual SD card would have a “file system,” i.e., a “storage area” of a virtual SD card, “for user data on the storage device for storage of user data corresponding to a user data area of the SD card,” just as claimed. *Id.*

Note also that *Hamann* creates a VSC having public area 4, as seen in Fig. 1 (annotated):

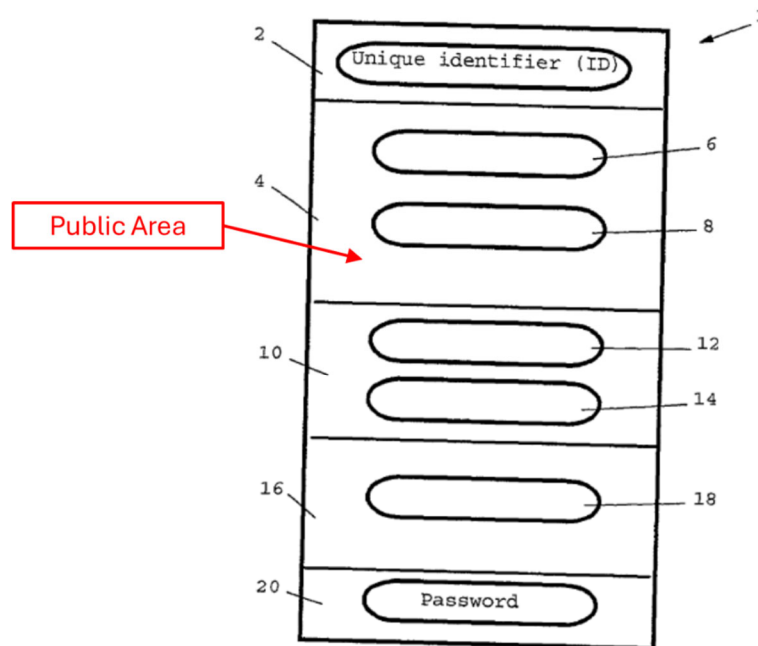


FIG. 1

Hamann describes the public area in Fig. 1. See *Hamann*, ¶¶[0025]-[0026] (“[0025] The logical file structure of the VSC (1) is preferably defined by the following data areas: [0026] (a public area (4) in which public data objects having no access conditions are placed, e.g. Certificate (6) and address (8)”). *Zadok*, ¶¶243-244.

Hamann discloses “a VSC control program handling the creation, the security and the read/write process of the VSC,” which generates a “**VSC having a logical file structure** comprising **a public area**, a private area, a secure key area, password area, and an unique identifier area.” *Id.*, ¶¶[0015]-[0016]. *Hamann* discloses that “[t]he data objects contained in the public area hav[e] no access restrictions...” *Hamann*, ¶¶[0016], [0026], [0027]. POSITAs would have understood that

Hamann's “public area,” which has a “logical file structure,” corresponds to the claimed “file system for user data on the storage device for storage of user data corresponding to a user data area of the SD card,” especially when combined with *Maeda* (and the *AAPA*). *Zadok*, ¶¶245-246.

f. [1e]

Maeda-Hamann-AAPA discloses/suggests this feature. *Zadok*, ¶¶248-257. *Maeda* discloses that the size of the file system for secure data and the file system for user data are calculated such that they each have a size that is relative to the other. *Maeda*, at 15:12-21. *See also id.*, 17:1-11, Figs. 16, 17, Claim 7. Thus, *Maeda* recognized that the size of the size of its protected area (i.e., “file system for secure data”) was determinant on the size of its user data area (i.e., “file system for user data”), and POSITAs would have recognized that *Maeda* was suggesting that the size of its protected area was related to the size of its user data area. *Zadok*, ¶¶248-253.

Despite this suggestion, *Maeda* does not disclose that the size of protected area relative to the size of its user data is determined “based on a lookup table providing a relationship between the sizes,” as claimed. However, the *'749Pat* admits that this was in the prior art. In particular, the *'749Pat* states that “secure area’s 260 size is determined at design time according to the SD card specifications.” *'749Pat*, 4:66-5:1. The *'749Pat* admits that in SD cards, the size of the file system

for secure data is “determinant on a size of the file system for user data,” and that this “determination [is] based on a lookup table providing a relationship between the sizes:”

A size of the secured area file system 315 is determined at provisioning time according to the SD card specifications. The size of the virtual secured area file system 315 is a table lookup from SD ASSOCIATION specifications based on the size of the virtual user area file system 325. The process creates a file or partition on the storage 116 that is accordingly formatted for the virtual secured area 315.

'749Pat, 7:62-8:2. Thus, the feature recited in element [1e] is *AAPA*. *Zadok*, ¶¶254-255.

The reason the independent claims were allowed was because patentee amended them to include this element. *See* Section IV.B. There is no evidence in the prosecution history that the Examiner knew about patentee’s admissions regarding this feature. Given these admissions, the Examiner was plainly wrong that that this feature was novel and not in the prior art. *Zadok*, ¶256.

2. Motivation To Combine

POSITAs would have been motivated to combine *Maeda*, the *AAPA*, and *Hamann*. *Zadok*, ¶¶258-283. **First**, both *Maeda* and the *AAPA* disclose the same technology, an SD card, with its protected area, user area, etc. POSITAs would have

recognized that *Maeda* discloses SD cards. *Maeda*, 2:61-3:3 Likewise, Applicant admitted that SD cards were well known, in typical use, and standardized. '749*Pat*, 4:43-46. POSITAs would have been motivated to use features that were contained in industry standards (and indeed would have been essentially forced to do so), and thus would have been motivated to use the lookup table feature, which the *AAPA* admits is required by SD card standards. *Zadok*, ¶¶259-261.

Second, both *Maeda* and the *AAPA* disclose/suggest that the sizes of the user and protected areas are related to each other. *Maeda* discusses the need to configure the sizes of the user and protected areas. EX1006, *Maeda*, 3:3-13. Similarly, the *AAPA* admits that the sizes of the user and protected areas are related and must conform to (and “enforced” by) the SD Association’s specifications. '749*Pat*, 7:62-67. Thus, *Maeda* and the *AAPA* both suggest that the sizes of the user and protected areas are related and configurable. *Zadok*, ¶¶262-265. POSITAs would have understood that a simple, fixed size relationship may not suffice because SD cards come in different sizes. Instead, POSITAs would expect there to be multiple such fixed size associations, possible one ratio for each size of SD card. POSITAs would have been familiar with simple computer data structures such as tables and arrays. Just as two-column spreadsheets were in widespread use, tables can easily relate numerical sizes of user areas to protected areas. Moreover, POSITAs would have been motivated to substitute features like those in *Maeda* for features that are

required by industry standards. Thus, POSITAs would have been motivated to use the SD Associations lookup table feature from the *AAPA* because it was mandated by industry standards. *Id.*, ¶265.

Third, Matsushita, *Maeda*'s assignee, was a founding member of the SD association. See https://en.wikipedia.org/wiki/SD_Association. POSITAs would have been looking for SD card information from those who worked the most on it (e.g., members of an association, vendors, their patents, and other documents and specifications). *Zadok*, ¶267.

Fourth, because *Maeda* and the *AAPA* disclose the same underlying SD card technology, combining them would have been trivial and would not have required extensive experimentation or impose undue burden. For the same reasons, the combination would have yielded predictable results. Lastly, POSITAs would have had a high expectation of success because the *AAPA* does nothing more than describe more details of an already standardized SD card technology. *Zadok*, ¶268.

POSITAs also would have been motivated to combine *Hamann* with *Maeda* and the *AAPA*.

First, SD cards (*Maeda-AAPA*) and smart cards (*Hamann*) are very similar technologies. Both are semiconductor, solid state storage devices, with a small form factor. Both include a microprocessor, volatile and non-volatile memory, and input/output methods. Both support file systems to store various files. Both include

strong mechanisms to secure the data (*e.g.*, authentication, encryption, and more). Both support different device sizes and hence file system sizes. And both were standardized by their respective standards-body organizations. POSITAs familiar with smart cards would have readily recognized the great similarities to SD cards, and vice versa. *Zadok*, ¶270.

Indeed, POSITAs would have expected success in making the *Maeda-Hamann-AAPA* combination, as the architectures in each are fairly similar. For example, *Hamann*'s "smart card" and *Maeda*'s SD card (and the *AAPA*'s SD card) have similar data formats (*e.g.*, protected area, user area) and encryption. *See Hamann*, ¶[0016] ("VSC having a logical file structure comprising a public area, a private area, a secure key area, password area, and an [sic] unique identifier area."); *see also Maeda*, 6:66-7:2, 13:30-33. Thus, virtualizing *Maeda*'s SD card would have been well within POSITAs' abilities, especially in view of *Hamann* and *Maeda*'s detailed teachings. *Zadok*, ¶271.

Second, *Maeda* and *Hamann* describe one key motivation being the protection of data through backups. Almost every user has at one point or another lost data and tried to recover it from backups (or, in hindsight, wish they had backed up their important data ahead of time).

Maeda discloses an embodiment where "the extended attribute is stored in at least one of the protected area and a backup area. ... The backup area is managed

separately from the normal partition in the user area. ... New extended attributes that cannot be defined in a FAT file system can be set for each file by storing such attributes in the protected area or the backup area.” *Maeda*, 26:39-51, Fig. 32.

Similarly, *Hamann*’s main purpose is “[b]ack-up and usage of secure copies of smart card data objects” (*Hamann*, Title). Indeed, *Hamann* states that “[i]t is therefore object of the present invention to provide an improved system and method allowing easy and secure back-up of the content of a smart card.” *Hamann*, ¶[0008].

Any storage technology can be used to back up data, from mere floppy diskettes, to hard disks, and of course SD cards and smart cards. POSITAs using *Maeda* and interested in data backups would have sought out other references that disclose backup methods and would have found *Hamann*—especially as *Hamann* aims to make backups of important data easier to achieve.

POSITAs would have also recognized that when users employ technologies to secure data (*e.g.*, SD cards, smart cards), they are most likely going to store critical information that must be protected (*e.g.*, encrypted, authenticated). Therefore, it is exactly that kind of critical information that must also be backed up, to protect against the loss, damage, or corruption of physical storage devices.

POSITAs would have required little to no experimentation because they are merely applying the same technique—storing and backing up data files securely—to different yet standardized devices. At most, POSITAs would have had to update

their code from using an SD Card standard file-access API (e.g., read/write methods) to using a different yet standard API to access files on smart cards. This is well within POSITAs' abilities. *Zadok*, ¶¶272-277.

Third, more than a decade before the '749*Pat* was filed, many forms of virtualization were already well known. Virtualization improves the versatility and flexibility of computer systems, allows better resource utilization and sharing, and much more. Well before 2010, virtualization of many resources had become a commonplace technique. *Zadok*, ¶278.

Hamann teaches that virtualizing memory cards allows memory cards to be backed up more easily. *Hamann*, ¶[0002]. POSITAs would have recognized that virtualizing SD Cards like those described in *Maeda* (and the *AAPA*) would provide this benefit to users, as *Hamann* suggests. For example, *Maeda* teaches that users may store content such as music and images on the memory card disclosed therein. *Maeda*, 25:64-26:3. POSITAs would have recognized that the ability to backup such content (whether DRM protected content or a user's unprotected content) would have been beneficial to users, as it would prevent loss of their content if the user lost their card, or they experience an SD card hardware failure.

Indeed, *Hamann* suggests this, stating that “[a]n essential advantage of this invention is that **backed-up smart card data objects in the VSC** allows the user to continue working with the [sic] most of the applications **if the real smart card lost**

or damaged.” *Hamann*, ¶[0019]. Given *Hamann*’s explicit teachings, POSITAs would have understood the benefits provided by backing up SD cards using virtualization like those in the *Maeda-AAPA* combination using *Hamann*’s teachings. *Zadok*, ¶¶278-280.

Fourth, POSITAs would have been motivated to combine the *AAPA* with *Maeda* and *Hamann* because the use of lookup tables to vary conditions based on known variables was well-known, and thus POSITAs would have understood that using a table to select the size of the secure area based on the size of the user data was a simple, efficient, and cost-effective method. *Zadok*, ¶281.

POSITAs would have been further motivated to make this combination because, as the ’749pat admits, using a lookup table for determining the size of the protected area was required by the SD card specification. POSITAs seeking to virtualize an SD-card based on the *Maeda-Hamann* combination would have naturally looked to the *AAPA* to determine the relationship between the total size of an SD card and the protected area and user area. Indeed, the fact that this feature is required by the industry standard (charged with enforcing it) would have motivated POSITAs to use this feature. Implementing tables and similar data structure would have been well within a POSITA’s expertise and would not have required undue burden. *Zadok*, ¶¶282-283.

3. Claim 14

a. [14pre]

To the extent the preamble is limiting, *Maeda-Hamann-AAPA* discloses/suggests this feature. *Zadok*, ¶¶284-287. As discussed in §VIII.A.1, *Hamann* discloses virtualizing smart cards, and when combined with *Maeda* (and the *AAPA*) results in a virtual SD card. *Hamann* also discloses using its VSC. *Hamann*, ¶[0015] (“**The VSC is created and used** by a VSC control program handling the creation, the Security and the read/write process of the VSC.”); *see also* ¶[0053] (“In a case of los[s] of a[] data object on the real smart card either **the VSC can be used directly as temporary ‘smart card’** of the previously saved objects or may be transferred back to the real smart card using the same steps as described before in the opposite direction, i.e. copy the data objects from the VSC and paste them to the real smart card.”). Thus, *Maeda-Hamann-AAPA* discloses the preamble.

b. [14a]

Maeda-Hamann-AAPA discloses/suggests this feature. *Zadok*, ¶¶288-296. As discussed in §VIII.A.1.b, *Hamann* discloses that its system has one or more smart card readers. *See e.g. Hamann*, ¶[0043] and Fig. 2. As shown in Fig. 3A (annotated), *Hamann* discloses that when a smart card is inserted into a reader, the VSC program’s graphical user interface (“GUI”) displays the card readers as well as the identity of any inserted smart cards:

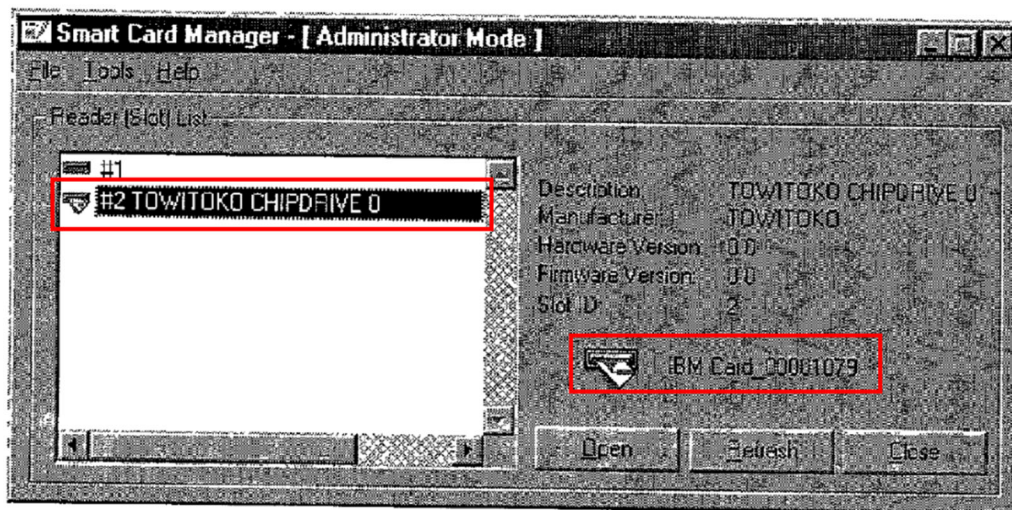


FIG.3A

In this example, *Hamann*'s GUI shows that card reader #2 has a smart card named "IBM Card_00001079" inserted therein. Indeed, *Hamann* discloses that "[t]he GUI of the smart card manager **displays all available smart card readers and VSCs.**" *Hamann*, ¶[0049].

As shown in Fig. 3K (annotated), once provisioned (*see* §VIII.A.3.c), this same GUI will display all available card readers and also the provisioned VSC:

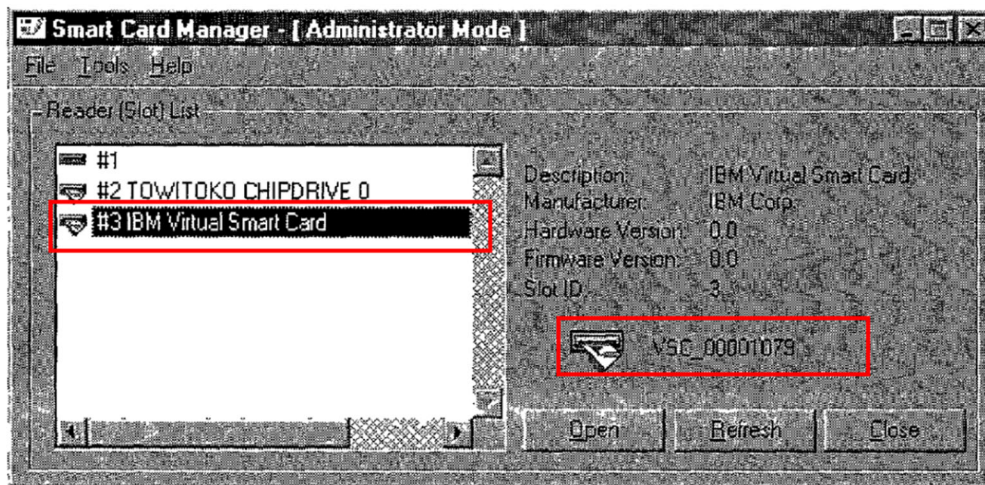


FIG. 3K

In this example, *Hamann*'s GUI shows that card reader #3 is actually a VSC named "VSC_00001079." *Hamann*, ¶[0051].

Given these teachings, POSITAs would have understood that *Hamann*'s GUI identifies all available smart cards, including both physical smart cards that have been inserted into one of *Hamann*'s card readers (e.g., "IBM Card_00001079"), and any VSCs that have been created (e.g., "VSC_00001079"). *Hamann*, ¶[0049]. Thus, when a user inserts a smart card into *Hamann*'s system, *Hamann*'s GUI would inform the user whether a virtual version of that smart card had been set up on its system. *Zadok*, ¶¶288-292.

The '749*Pat* refers to a "provisioning process for creating the virtual SD card..." '749*Pat*, 7:46-49. Given this, POSITAs would have understood that "determining if the virtual SD card is provisioned," means determining whether a

virtual SD card has been “created.” *Zadok*, ¶¶293-294. Petitioners recognize that other steps recited in claim 14 use the term “creating.” *See* elements [14c]-[14d]. To the extent “provision/provisioned/provisioning” must mean something other than “create/created/creating,” POSITAs would have understood that the term means “set up/setting up,” which *Hamann* discloses. *Zadok*, ¶294.

As discussed in §VIII.A.1.a, *Hamann* does not explicitly disclose virtualizing SD cards. However, as also discussed there, SD cards fall within the scope of *Hamann*’s smart card definition. Moreover, *Hamann* suggests and thus would have motivated POSITAs to virtualize SD cards like those described in *Maeda* and the *AAPA*, as discussed in §VIII.A.2. *Zadok*, ¶295.

c. [14b]

Maeda-Hamann-AAPA discloses/suggests this feature. *Zadok*, ¶¶297-307. As discussed in §VIII.A.3.b, *Hamann*’s GUI informs a user as to whether a VSC has been provisioned. *See Hamann*, Fig. 3A, ¶[0049]. *Hamann*’s “Smart Card Manager” provisions the unprovisioned VSC as follows. After inserting a smart card into a reader, all the objects on that card are displayed, with any private objects being displayed if a password is provided. *Hamann*, ¶[0049] and Figs. 3B-3E. *Zadok*, ¶297. To start the provisioning process, the user selects the “Copy All” command from the GUI, as shown in Fig. 3F (annotated):

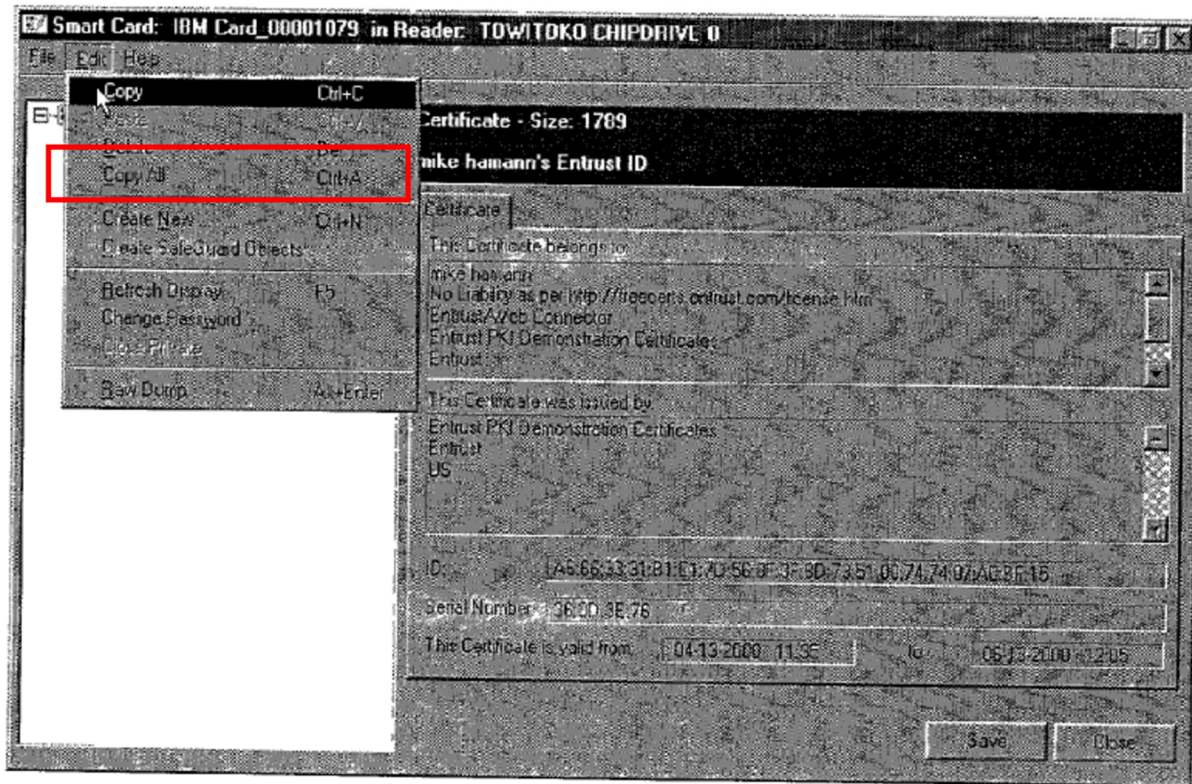


FIG. 3F

Hamann, ¶[0049] (“By selecting the ‘Copy command from the Edit menu of the smart card manager GUI’ (see FIG. 3F) the smart card manager stores the selected objected in an intermediate buffer. Furthermore, the smart card manager GUI offers via the Edit menu the possibility to copy all objects stored in the smart card (see FIG. 3F).”).

Next, using the “Tools” menu in the GUI, a user invokes the “VSC Manager,” as shown in Fig. 3G (annotated):

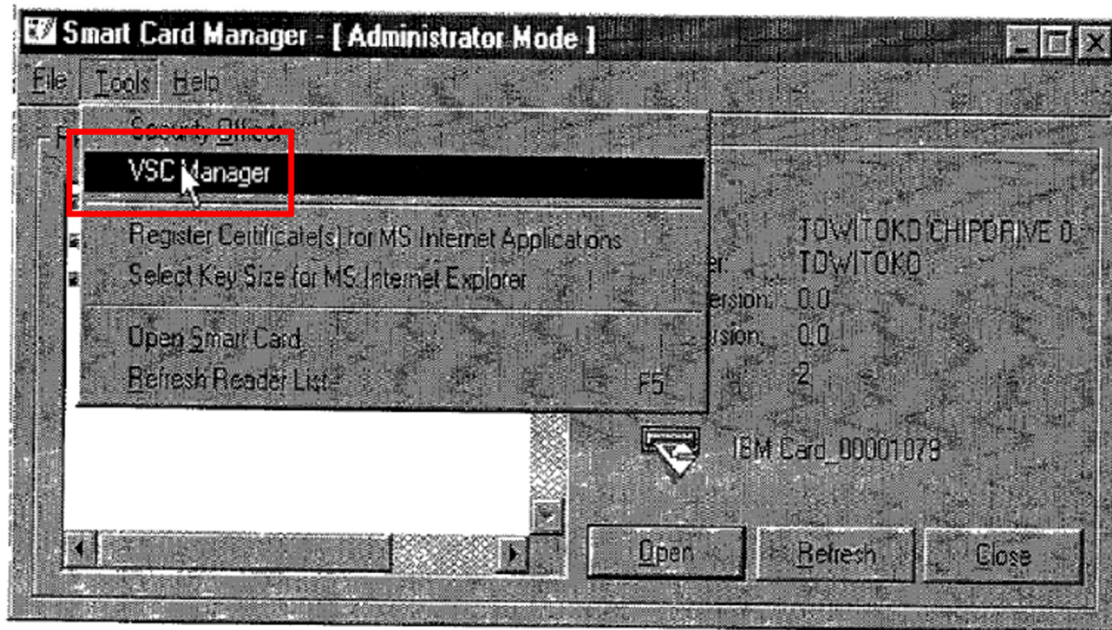


FIG. 3G

Hamann, ¶[0050] (“The virtual smart card control program may be started from the ‘Tools’ menu as shown in FIG. 3G.”). This “opens a menu having a button for creating a new VSC,” as shown in Fig. 3H (annotated):

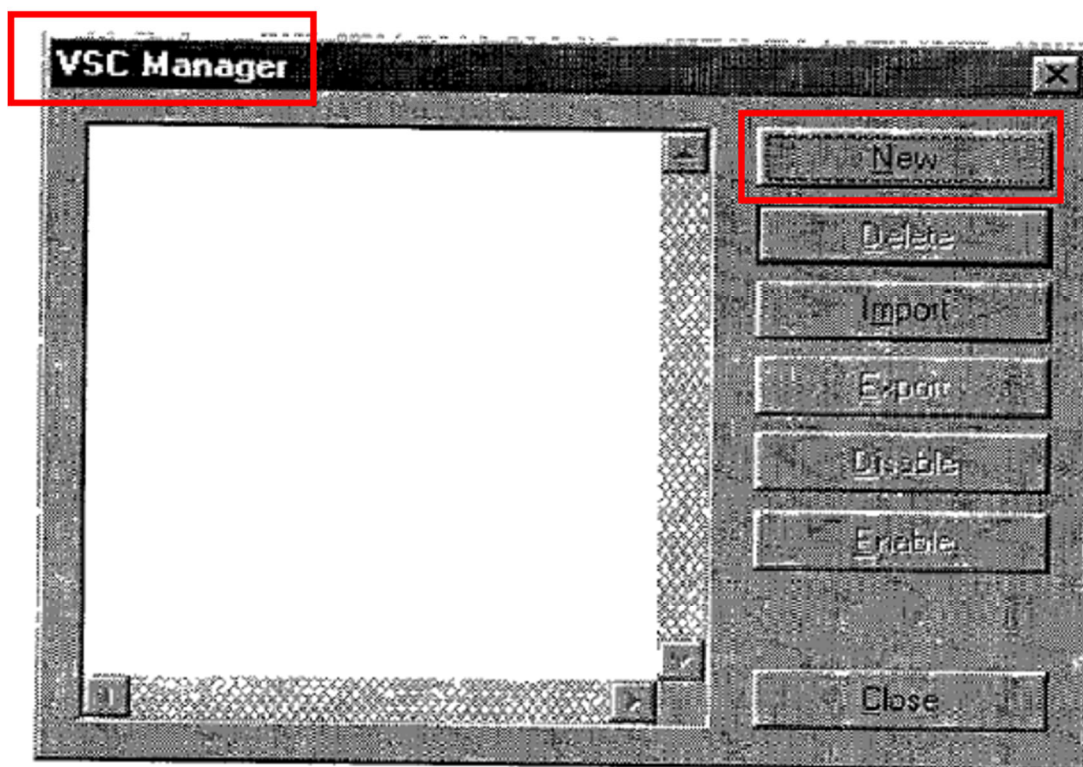


FIG. 3H

“A new VSC can be created by pressing the button ‘New.’” *Hamann*, ¶[0050]. As discussed in §§VIII.A.1.b-VIII.A.1.c, *Hamann* discloses creating an ID for the VSC (analogous to the media ID of an SD card) that is “specified using the serial number of the real smart to be assigned to the new VSC.” *Id.* This is shown in Fig. 3I (annotated):

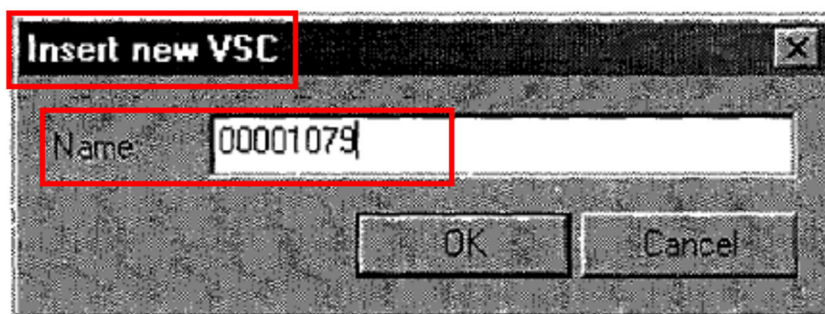


FIG. 3I

Once the VSC has been created with the ID based on the real smart card, the user clicks on the “Close” button shown in Fig. 3J (annotated):

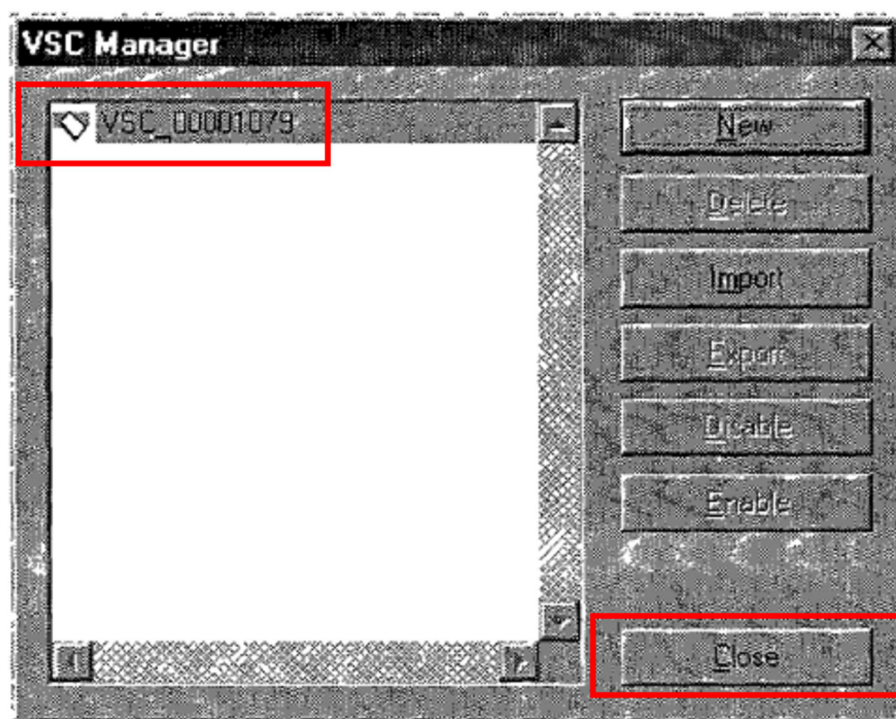


FIG. 3J

Hamann, ¶[0050]. As discussed, *Hamann*’s VSC manager then “displays the created

VSC in the ‘Reader List’ as ‘IBM Virtual Smart Card’ and the smart [card] label ‘VSC 00001079’”:

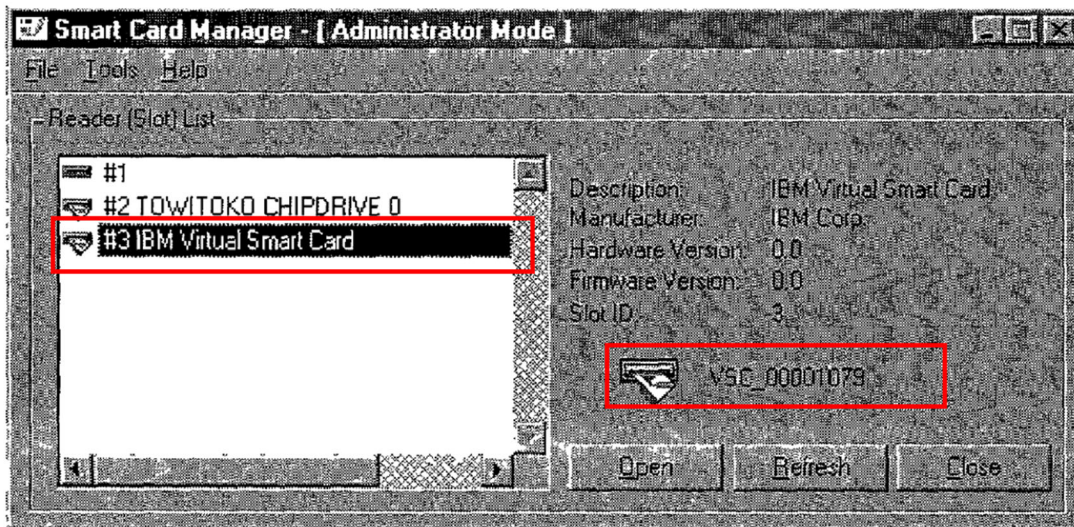


FIG. 3K

Hamann, ¶[0051]. Thus, POSITAs would have understood that *Hamann* discloses provisioning a VSC in response to the VSC not being provisioned. *Zadok*, ¶¶298-305.

As discussed in §VIII.A.1.a, *Hamann* does not explicitly disclose virtualizing SD cards. However, as also discussed there, SD cards fall within the scope of *Hamann*’s smart card definition. Moreover, *Hamann* would have motivated POSITAs to virtualize SD cards like those described in *Maeda* and the *AAPA*, as discussed in §VIII.A.2. *Zadok*, ¶306.

d. [14c]

See §VIII.A.1.d.

e. [14d]

See §VIII.A.1.e.

f. [14e]

See §VIII.A.1.f.

g. [14f]

Maeda-Hamann-AAPA discloses/suggests this feature. *Zadok*, ¶¶311-316. POSITAs would have understood that data can be accessed from the secure area of physical SD cards, as disclosed in *Maeda*. *See e.g., Maeda*, 13:42-45 (“The following is an explanation of the secure processing unit 11 provided in order to **perform secure reading and writing to and from the protected area** in the nonvolatile memory 1.”). *Zadok*, ¶311. The *AAPA* also admits that data can be accessed from the secure area of physical SD cards. ’749*Pat*, 4:43-63 (“**Typical** SD Card Architecture and Functions ... Both **secure data** and unsecure (user) data are stored in a persistent manner **so that it can be retrieve at a later time.**”).

Hamann discloses that VSCs are “a software implemented version of a real smart card providing the equivalent functionality of a real smart card.” *Hamann*, ¶[0015]. *Hamann* further teaches that its VSCs can be read from and written to, as it discloses that “[t]he VSC is created and used by a VSC control program handling the creation, the security **and the read/write process of the VSC.**” *Id. See also id.*, ¶[0017] (“All data objects can be **stored and retrieved on/from the virtual smart**

card's public and private area ...”). Finally, as discussed in §VIII.A.1.d, *Hamann*'s VSC has a “private area” (see *Hamann*, ¶¶[0016], [0027]) corresponding to the “file system for secure data on a storage device for storage of secure data corresponding to a secure data area of the SD card,” just as claimed.

Given this, POSITAs would have understood that the data stored in the *Maeda-Hamann-AAPA* virtual SD card that was provisioned could be accessed. *Zadok*, ¶¶312-315. Indeed, POSITAs would have recognized that one purpose of virtualizing a physical SD card, as suggested by *Hamann*, would be to allow accessing data stored in the virtual secure area. *Id.*

h. [14g]

Maeda-Hamann-AAPA discloses/suggests this feature. *Zadok*, ¶¶317-323. According to the '749*Pat*, “extracting” data refers to decrypting data stored therein to return data from the secured area of the virtual SD card. See '749*Pat*, 8:32-38 (“If a **read operation, the process fetches and decrypts 560 data from the virtual secure area file system 315** using the key derived from the computing device unique information. The process encrypts 565 the data with the AKE key for transport to the application program 105. **The process returns (or retrieves or extracts) data from the virtual secure area 315** to the application program 105.”).

Maeda discloses that when reading data from its protected area (i.e., the physical SD card's secured area), the data is decrypted, i.e., “extracted.” See e.g.,

Maeda, 15:2-8 (“**Reading and writing of data to and from the protected area is performed following decryption** performed by the Ks decrypting unit 16 and encryption performed by the Ks encrypting unit 17, so the protected area can only be accessed when the semiconductor memory card 100 and a connected access apparatus 200 have performed AKE processing successfully.”).

As discussed, *Hamann* discloses that its VSCs have functionality that is equivalent to real smart cards, that its VSCs have a “private area” and that the data stored in this private area can be accessed. *See Hamann*, ¶¶[0015]-[0016], [0027]. *Hamann* discloses that data stored in its VSC’s private area is encrypted, and that it can be “**accessed [by] providing** a password (10), *e.g.* account no (12) **and key information** (14).” *Id.*, ¶[0027]. Thus, POSITAs would have understood that *Hamann* also discloses decrypting, *i.e.*, “extracting,” data from its private area. *Zadok*, ¶¶318-320.

POSITAs thus would have understood that when virtualizing an SD card like that described in *Maeda* using *Hamann*’s virtualization teachings, the data stored in *Maeda*’s protected area (which corresponds to the claimed “secure area”), would be decrypted, *i.e.*, “extracted.” *Id.*, ¶321. POSITAs would have been motivated to combine these references for the reasons discussed in §VIII.A.2. *Id.*, ¶322. Thus, *Maeda-Hamann-AAPA* renders claim 14 obvious.

4. Claim 15

Maeda-Hamann-AAPA discloses/suggests this claim. *Zadok*, ¶¶324-331. *Maeda* discloses that “the protected area **can only be accessed when the semiconductor memory card 100** and a connected access apparatus 200 **have performed AKE processing successfully.**”⁸ *Maeda*, 15:2-8. POSITAs would have therefore understood that *Maeda*’s physical SD cards perform the claimed “authentication using Authenticated Key Encryption (AKE) before accessing the data in the secure area” of physical SD cards. *Zadok*, ¶¶327-328.

As discussed, *Hamann* discloses that its VSCs are “a software implemented version of a real smart card providing **the equivalent functionality of a real smart card.**” *Hamann*, ¶[0015]. Thus, POSITAs would have recognized that when

⁸ *Maeda* notes that “AKE” stands for “Authentication and Key Exchange.” *Maeda*, 13:62-63. While claim 15 of the ’749*Pat* refers to “AKE” as “Authenticated Key Encryption,” POSITAs would have understood that *Maeda*’s terminology and the “AKE” described in the ’749*Pat* specification (*see e.g.*, ’749*Pat*, 5:44-49 referring to “Authenticated Key Exchange”) is correct. The ’749*Pat* also states that AKE is performed in accordance with the Content Protection for Recordable Media (CPRM) specifications (’749*Pat*, 5:44-49), which POSITAs would have known refers to the same “AKE” process as in *Maeda*. *Zadok*, ¶¶324-326.

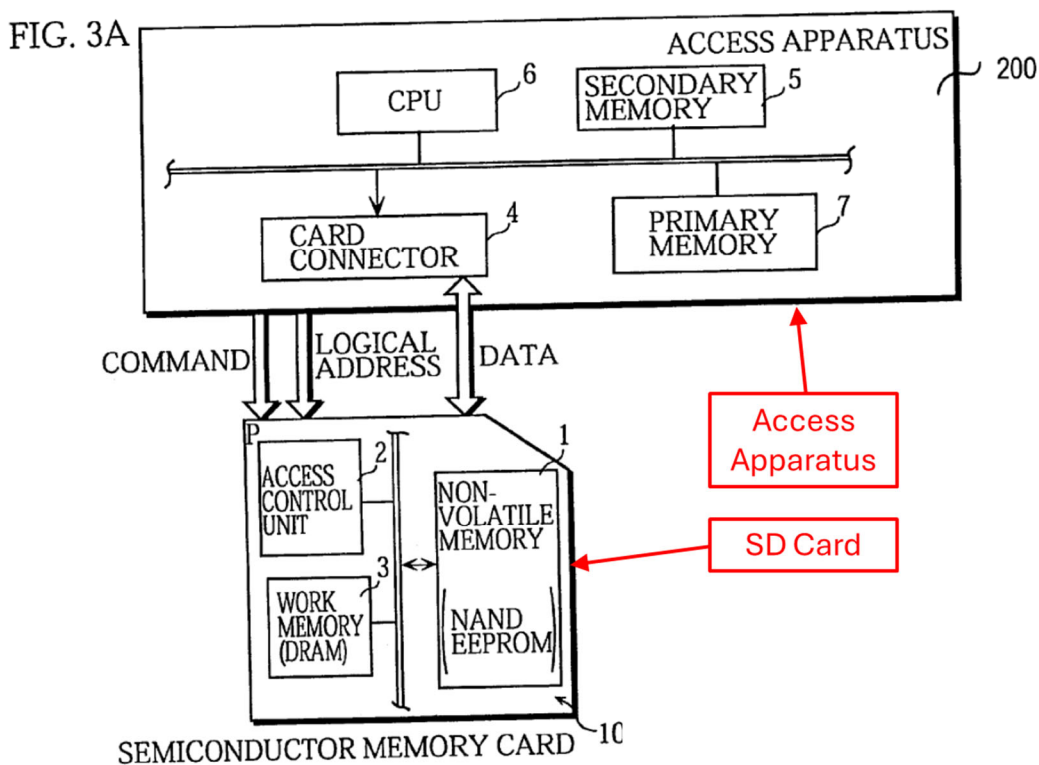
applying *Hamann's* teachings to *Maeda*, the resulting virtual SD card would have the “equivalent functionality” as a physical SD card, meaning that a virtual SD card would function in essentially the same. Indeed, POSITAs would have understood that for a virtual SD card to operate in the same manner with the same level of security as a physical SD card, the virtual version would have to perform authentication in the same manner as the real version. As *Maeda* discloses, SD cards perform AKE before accessing the data in their secure area, just as claimed. *Zadok*, ¶¶329-330. Thus, claim 15 is obvious.

5. Claim 16

Maeda-Hamann-AAPA discloses/suggests this claim. *Zadok*, ¶¶332-346. The '749*Pat* discloses that application programs are located on the computer system in which the virtual SD card is implemented. *See e.g.*, '749*Pat*, Fig. 3. Because this claim refers to “data received from an application program,” POSITAs would have understood that this claim is directed to a “write” operation, and corresponds to the “decrypt data with AKE key” portion of step 555 shown in Fig. 5. '749*Pat*, 8:22-28. *Zadok*, ¶333.

Maeda discloses that “[w]hen encrypted data to be written into the protected area is output from the access apparatus 200 connected to the semiconductor memory card 100, the Ks decrypting unit 16 uses the session key Ks to decrypt this data which has already been encrypted by session key Ks before

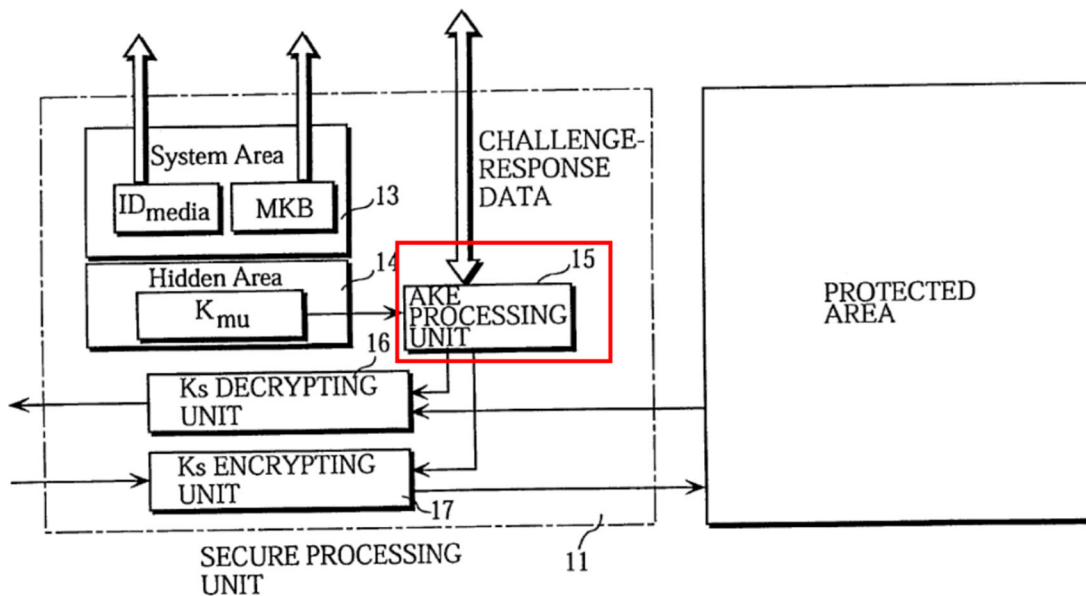
being output.” *Maeda*, 14:57-62. *Maeda* also discloses that “data **obtained by this decryption** is written into the protected area, as the original data.” *Id.*, 62-63. Note that *Maeda*’s “access apparatus” is the device the SD card is inserted into. *See e.g.*, Fig. 3A (annotated):



Examples of such “access apparatus 200” include personal computers. *See Maeda*, 6:25-28. POSITAs would have understood that personal computers would have application programs running thereon that would write data to the connected SD card. *Zadok*, ¶¶334-341.

Maeda also discloses “AKE processing unit 15,” shown in Fig. 15:

FIG. 15



As shown, *Maeda's* AKE processing unit 15 is coupled to Ks decrypting and encrypting units 16-17. *Maeda* discloses that for data to be successfully written to the protected area, it must have gone through an AKE process. *Maeda*, 15:2-8 (“... **the protected area can only be accessed when the semiconductor memory card 100 and a connected access apparatus 200 have performed AKE processing successfully.**”). *Zadok*, ¶¶342-343.

Thus, *Maeda* discloses that in physical SD cards, “data received from an application program through Authenticated Key Encryption (AKE) is first decrypted,” just as claimed. *Id.*

As discussed, *Hamann* discloses that its VSC is “a **software implemented version of a real smart card** providing the **equivalent functionality of a real smart card.**” *Id.*, ¶[0015]. Thus, POSITAs would have understood that when

applying *Hamann*'s teachings regarding virtualization of smart cards to *Maeda*, the resulting virtual SD card would have functioned in the same manner as *Maeda*'s physical SD card. *Zadok*, ¶345. Thus, claim 16 is obvious.

6. Claim 18

a. [18pre]

See §VIII.A.1.a. Note that *Hamann* discloses that it virtualizes smart cards using “virtual smart card control program 18,” which *Hamann* discloses is stored on a computer usable medium. *Hamann*, claim 8. POSITAs would have understood that a such a program would comprise instructions and that such instructions would be stored in a non-transitory medium and executed by a processor. *Zadok*, ¶348. POSITAs would have been motivated to combine *Maeda-Hamann-AAPA* for the reasons discussed in §VIII.A.2. *Id.*

b. [18a]

See §VIII.A.1.b.

c. [18b]

See §VIII.A.1.c.

d. [18c]

See §VIII.A.1.d.

e. [18d]

See §VIII.A.1.e

f. [18e]

See §VIII.A.1.f.

7. Claim 22

a. [22pre]

See §VIII.A.3.a. POSITAs would have understood that *Hamann* discloses the “non-transitory computer readable medium” features of this claim. *See* §VIII.A.6.a. For motivation to combine, *see* §VIII.A.2

b. [22a]

See §VIII.A.3.b.

c. [22b]

See §VIII.A.3.c.

d. [22c]

See §VIII.A.3.d.

e. [22d]

See §VIII.A.3.e.

f. [22e]

See §VIII.A.3.f.

g. [22f]

See §VIII.A.3.g.

h. [22g]

See §VIII.A.3.h.

8. Claim 23

See §VIII.A.4

9. Claim 24

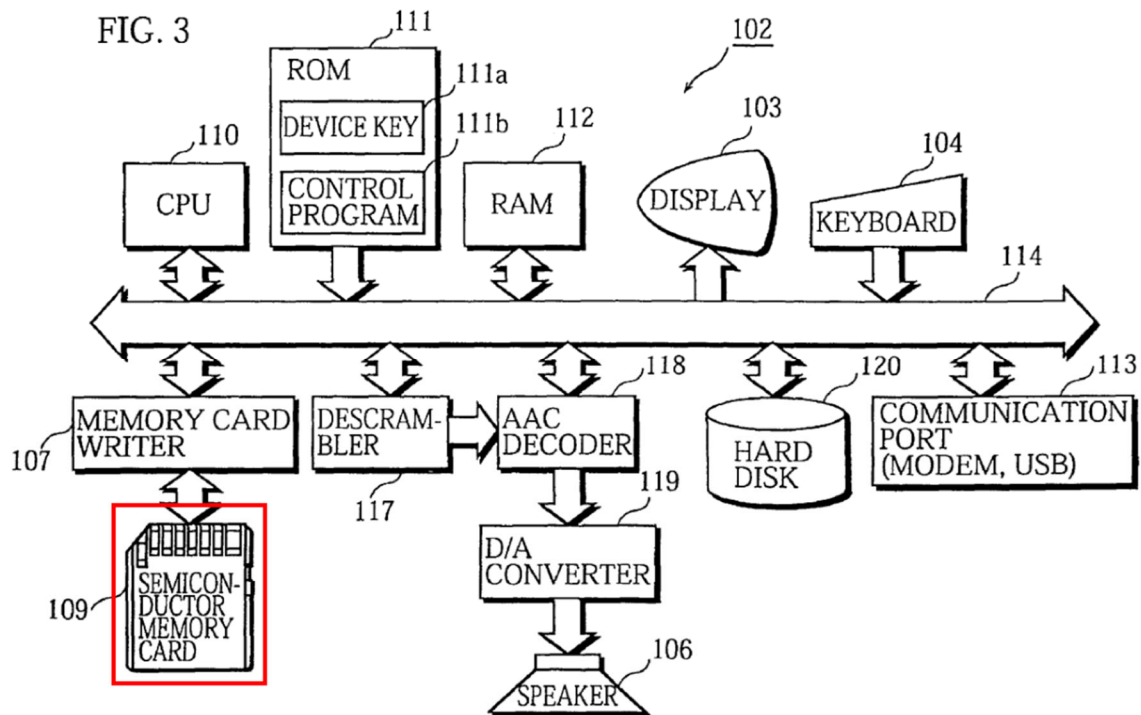
See §VIII.A.5.

B. Ground 2: *Maeda-Hamann-AAPA-Hirota* Renders Claims 2, 6-8, and 19 Obvious

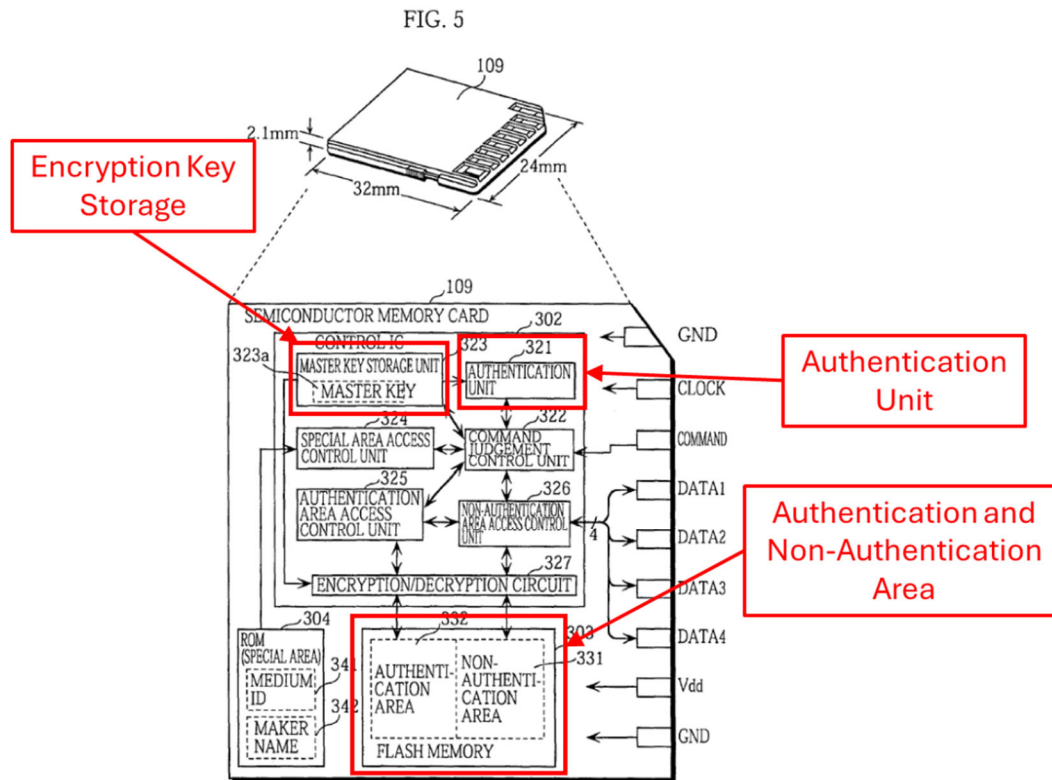
1. Claim 2

Maeda-Hamann-AAPA-Hirota discloses/suggests this claim. *Zadok*, ¶¶366-378. As discussed in §VIII.A.1.d, *Maeda* and the *AAPA* disclose that physical SD cards have a “protected area” that, when virtualized using *Hamann*’s teachings, results in a “file system,” i.e., a “storage area” of a virtual SD card, “for secure data on a storage device for storage of secure data corresponding to a secure data area of the SD card,” just as claimed. Claim 2 requires that the “file system for secure data” be encrypted. *Maeda* discloses that encrypted data is “to be written into the protected area...” (*Maeda*, 14:57-63) but does not explicitly state that its protected area is encrypted.

Hirota, like *Maeda*, discloses a semiconductor memory card that can be inserted into a computer, as shown in Fig. 3 (annotated):

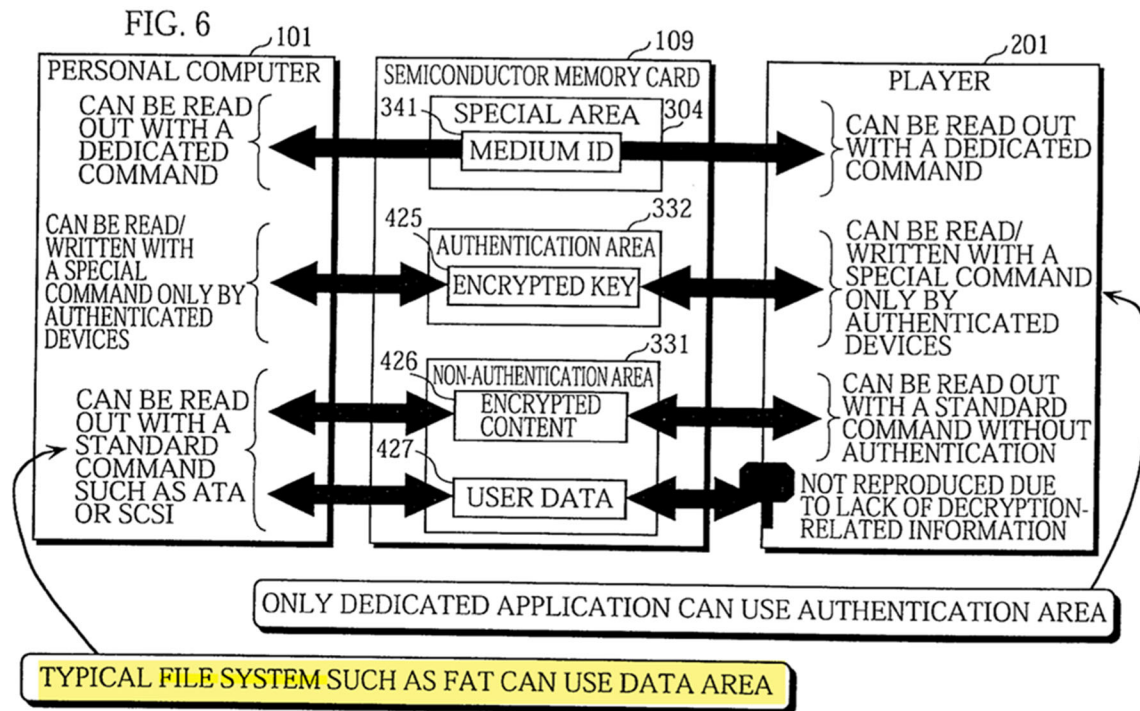


Hirota's semiconductor memory card can store digital data. *Hirota* at 2:3-7. Like *Maeda*, *Hirota* discloses that its semiconductor memory card includes flash memory 303 having “an authentication area and a non-authentication area,” shown in Fig. 5 (annotated):



See also Hirota, 10:27-36. Zadok, ¶¶369-371.

Hirota's Fig. 6 provides additional information regarding its storage architecture:



Hirota's “authentication area 332 stores an encryption key 425” which is a secret key used for decrypting the encrypted content 426 stored in the non-authentication area 331.” *Hirota*, 12:51-54. Thus, *Hirota's* “authentication area” is similar to *Maeda's* “protected area,” since *Maeda* teaches that its “protected area is used to store secret[] information, such as an encryption key used for encrypting data” *Maeda*, 2:67-3:2. POSITAs thus would have understood that *Hirota's* authentication area and *Maeda's* protected area (as well as the *AAPA's* secure area) are directed to essentially the same structure. *Zadok*, ¶¶372-375.

Hirota also discloses that its authentication area is encrypted. See *Hirota*, 2:41-45 (“.... the instruction to access the authentication area has been encrypted... to protect an unauthorized access of the authentication area.”);

11:58-12:4 (“The encryption/decryption circuit 327 is a circuit which **performs encryption** and decryption **using the master key 323a** stored in the master key storage unit 323... The encryption/decryption circuit 327 **encrypts data before writing the data to the flash memory 303**... These encryption and decryption are performed to prevent unauthorized acts such as an act of disassembling the memory card 109, analyzing the contents of the flash memory 303 directly, and **stealing the password from the authentication area 332**.”).

Thus, POSITAs would have understood that the when the SD cards described in *Maeda-AAPA-Hirota* are virtualized using *Hamann*’s teachings, the resulting file system (i.e., “storage area” of a virtual SD card) for secure data would be encrypted, just as claimed. *Zadok*, ¶¶376-377.

2. Motivation To Combine

POSITAs would have been motivated to combine *Hirota* with *Maeda-Hamann-AAPA*. *Zadok*, ¶¶379-382. POSITAs would have recognized that encrypting the file system for secure data created when virtualizing the *Maeda-AAPA* SD card would have increased the security of the information stored therein, particularly in view of *Hirota*’s teachings that encryption keys are stored therein. This is reinforced by *Hamann*, which teaches that its virtualized private area is also encrypted. *See Hamann*, ¶[0027]. *Zadok*, ¶¶380-381. Thus, adding *Hirota*’s encryption would be seen by POSITAs as not only providing a highly desirable

feature, but also nothing more than combining known techniques for enhancing security in a predictable manner, with a reasonable expectation of success. *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 416-417 (Fed. Cir. 2007). Indeed, as Dr. Zadok explains, data and file encryption techniques were well known and there were a wide variety of techniques available for POSITAs, meaning that POSITAs would have had a strong expectation of success in making such a combination. *Zadok*, ¶¶381-382.

3. Claim 6

Well before 2010, computers already supported multiple storage devices, and each device supported multiple partitions. Formatting different devices and/or partitions for different uses was routine and even encouraged. For example, a POSITA would have been motivated to place highly secure data in one partition and less sensitive data in another. This made it easier to apply different retention, backup, and reliability policies—and it also helped compartmentalize data of different security levels. *Zadok*, ¶383.

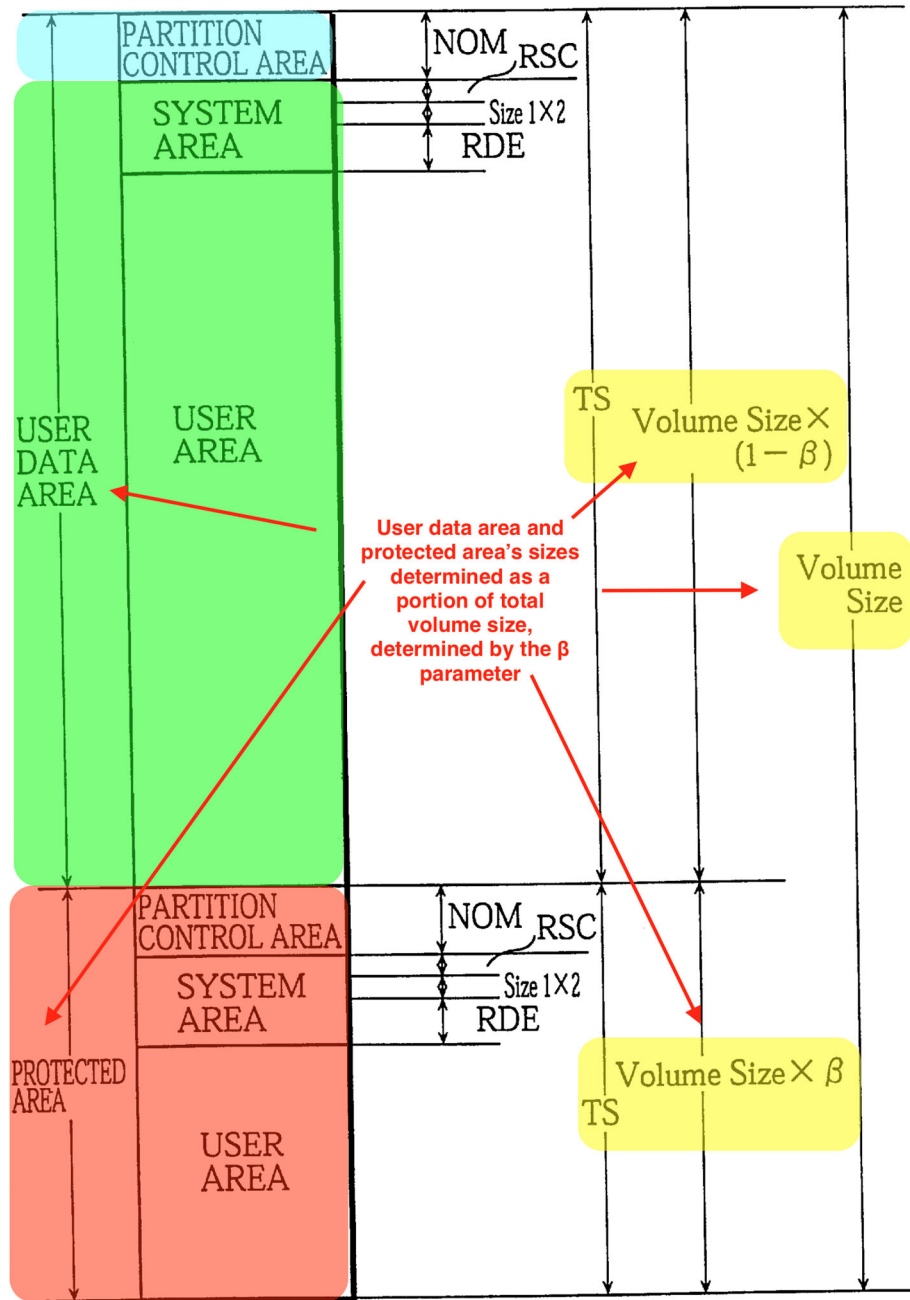
Nevertheless, *Maeda-Hamann-AAPA-Hirota* discloses/suggests this feature. *Zadok*, ¶¶384-388. As discussed in §VIII.C.1, *Hamann* teaches its “virtual smart card (VSC) [has] the same defined logical file structure ... as its assigned real smart card.” *Hamann*, ¶[0014]. POSITAs would have understood this file structure includes the hardware structure of the VSC’s architectural features, such as the

layout of sectors and erasable blocks described in *Meada's* SD card. *See Maeda*, 1:44-55, Figs. 1A, 1B. Thus, POSITAs would have recognized that *Hamann* was suggesting that the secure data and user data of its VSC reside on different physical partitions. *Zadok*, ¶384.

Despite this suggestion, *Hamann* does not disclose “the file system for secure data and the file system for user data are located on different physical partitions of the storage device.” However, the '749*Pat* states that in “typical” SD cards, “[t]he **secured area 260 may be implemented as a physical or logical device** within the SD card as chosen by the SD card's original equipment manufacturer (OEM)” (*id.* at 4:63-66) and “[t]he **user (or unsecured) area 265 also may be either physical or logical partitions** depending on implementation within the SD card” (*id.* at 5:4-6). Thus, the feature recited in claim 6 is *AAPA*. *Zadok*, ¶385.

Moreover, *Maeda's* Fig. 16 (annotated below) illustrates using partitions. *Maeda*, discloses using known FAT-based file systems, which use a partition table to determine the number and positions of the partitions. *See* “partition control area” annotated in blue in Fig. 16 below.

FIG. 16



A POSITA would have understood that FAT file systems include partitions that reside on the same device. *Zadok*, ¶386.

Accordingly, POSITAs would have understood that when *Hamann's*

teachings are used to virtualize an SD card as in *Maeda-AAPA-Hirota*, the resulting virtual SD card would have the same file structure as the original SD card, including the same physical partitions. *Zadok*, ¶387.

4. Claim 7

Maeda-Hamann-AAPA-Hirota discloses/suggests this feature. *Zadok*, ¶¶389-393. As discussed in §VIII.C.1, *Hamann* teaches its “virtual smart card (VSC) [has] the same defined logical file structure ... as its assigned real smart card.” *Hamann*, ¶[0014]. POSITAs would have understood this file structure includes the logical structure of the VSC, such as the file system layout (*e.g.*, FAT file system) of *Meada*’s SD card. *See Maeda*, 1:55-2:2, Figs. 1C, 1D. Thus, POSITAs would have recognized that *Hamann* was suggesting that the secure data and user data of its VSC to be on different logical partitions. *Zadok*, ¶390.

Despite this suggestion *Hamann* does not disclose “the file system for secure data and the file system for user data are located on different logical partitions of the storage device.” However, the ’749*Pat* states that in “typical” SD cards, “[t]he **secured area 260 may be implemented as a physical or logical device** within the SD card as chosen by the SD card’s original equipment manufacturer (OEM)” (*id.* at 4:63-66) and “[t]he **user (or unsecured) area 265 also may be either physical or logical partitions** depending on implementation within the SD card” (*id.* at 5:4-6). Thus, the feature recited in claim 7 is *AAPA*. *Zadok*, ¶391.

Accordingly, POSITAs would have understood that when *Hamann's* teachings are used to virtualize an SD card as in *Maeda-AAPA-Hirota*, the resulting virtual SD card would have the same file structure as the original SD card, including the same logical partitions. *Zadok*, ¶392.

5. Claim 8

Maeda-Hamann-AAPA-Hirota discloses/suggests this feature. *Zadok*, ¶¶394-397. The '749*Pat* discloses that its virtual SD card can be configured in either internal or external storage of a computer. '749*Pat*, 6:18-23. POSITAs would therefore have understood that the “existing file system” can be the file system of a computer on which the VSC operates. As discussed, *Hamann* discloses that its VSC “is a **software implemented** version of a real smart card providing the equivalent functionality of a real smart card,” that is “used by a VSC control program...” *Hamann*, ¶[0015].

POSITAs would therefore have understood that the *Maeda-Hamann-AAPA-Hirota* virtual SD card would have been implemented on the computer running *Hamann's* VSC control program. *Zadok*, ¶396. Thus, POSITAs would have also understood that the *Maeda-Hamann-AAPA-Hirota* virtual SD card's file systems for secure data and user data would be “within an existing file system,” i.e., an existing storage area on the computer running *Hamann's* VSC control program. *Id.*

6. Claim 19

See §VIII.B.1.

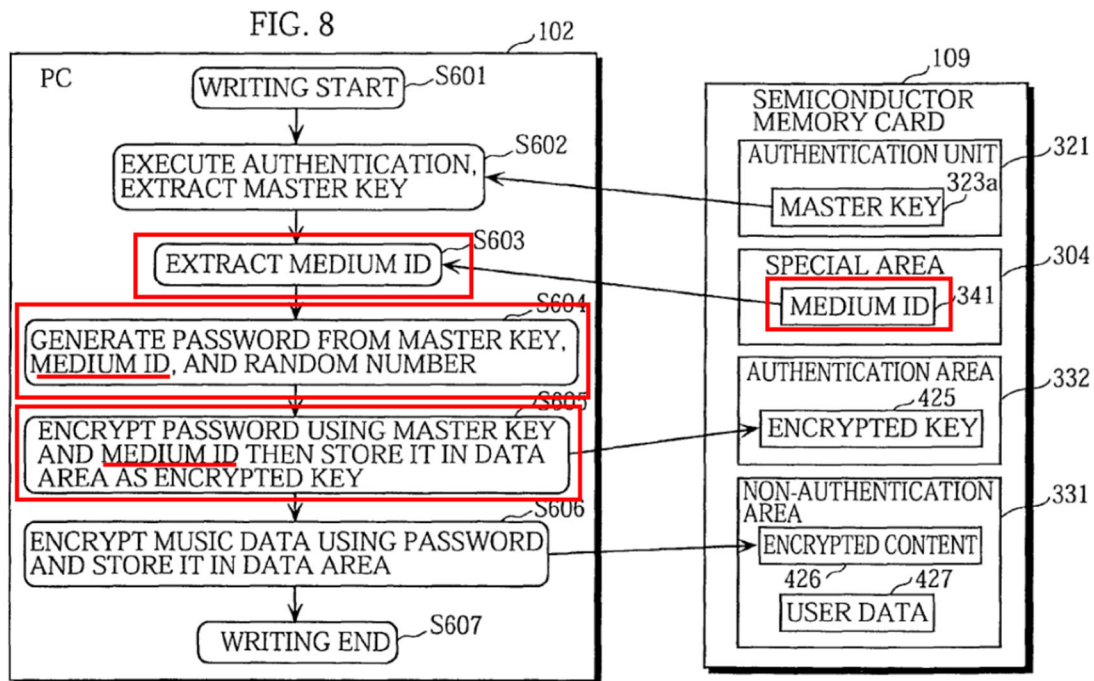
C. Ground 3: *Maeda-Hamann-Hirota-Lu* Renders Claims 3-5, 20-21 Obvious

1. Claim 3

Maeda-Hamann-AAPA-Hirota-Lu discloses/suggests this claim. *Zadok*, ¶¶399-407. Claim 3 first requires that the recited “file system” be encrypted with an encryption key. POSITAs would have understood that encryption is almost always performed with an encryption key. *Zadok*, ¶401. Regardless, *Hirota* discloses that its “authentication area,” i.e., the claimed “file system for secure data,” is encrypted with an encryption key. See e.g., *Hirota*, 2:41-45 (“.... the instruction to access the **authentication area has been encrypted**... such a semiconductor memory card has a reliable function to **protect an unauthorized access of the authentication area.**”); 11:58-12:4 (“The encryption/decryption circuit 327 is a circuit which **performs encryption** and decryption **using the master key 323a** stored in the master key storage unit 323... The encryption/decryption circuit 327 **encrypts data before writing the data to the flash memory 303**... These encryption and decryption are performed to prevent unauthorized acts such as an act of disassembling the memory card 109, analyzing the contents of the flash memory 303 directly, and **stealing the password from the authentication area 332.**”). *Zadok*,

¶402. See also *Hirota*, 23:31-57.

Claim 3 also requires that the encryption key be “derived from computer system information.” According to the ’749*Pat*, such “computer system information” can be, “e.g., processor serial number, bios serial number, device serial number.” ’749*Pat*, 7:2-6. *Hirota* suggests using device data for deriving encryption keys, as it discloses that encrypted key 425 stored in its authentication area uses a key that is derived, in part, from the “medium ID” of the SD card itself. This is shown in Fig. 8 (annotated):



Hirota discloses that the “medium ID” is an “identifier of the memory card 109.” *Hirota*, 10:41-42. To store encrypted key 425 in the authentication area, *Hirota* teaches that the card’s medium ID 341 is extracted by the PC in which the

card is inserted, that a password is generated using, inter alia, the card's medium ID, and encrypting this password, which then "is written to the authentication area 332 as the encryption key 425 (S605)." *Hirota*, 14:58-15:3. POSITAs would have understood *Hirota* to disclose a process whereby the actual key is derived from the medium ID, including additional steps. *Zadok*, ¶¶403-404.

Note that this encryption key is not the encryption key used to encrypt the authentication area (i.e., the claimed "file system for secure data"), but POSITAs would have understood these teachings to be a suggestion to use device data to derive encryption keys. *Zadok*, ¶405. POSITAs would have understood that instead of using data from an SD card to derive encryption keys, computer system information could be used to derive encryption keys, as described in *Lu*, which discloses associating encryption with a serial number for software/hardware binding and therefore discloses an encryption key derived from a computer system. *See Lu*, p. 1 (describing an "encryption and decryption methods for implementing hardware and software binding."⁹). *Lu* discloses a chip storing a unique serial number HW_UID "that represents the identity of the chip." *Lu*, p. 5. *Lu* uses a HASH to transform the HW_UID to a SW_UID, which in turn is used to create the encryption key. *Id.* Thus, POSITAs would have understood that *Lu* discloses deriving an encryption key

⁹ All *Lu* quotations are from the certified translation, *EX1009*.

using a serial number of the hardware system. *Zadok*, ¶405.

Thus, when virtualizing an SD card like that in *Maeda/AAPA/Hirota* using *Hamann*, POSITAs would have understood that whenever the encryption key was needed to access the authenticated area, it could be derived from a hardware feature in the computer system using *Lu*'s teachings. *Zadok*, ¶406. POSITAs would have recognized that this means that the encryption key need not be saved by the computer system on which the virtual SD card is stored since it could be derived using *Lu* whenever it was needed. Thus, in *Maeda-Hamann-AAPA-Hirota-Lu*, the encryption key derived from the computer system need not be “stored by the computer system,” just as claimed. *Id.*

2. Motivation To Combine

POSITAs would have been motivated to combine *Lu* with *Maeda-Hamann-AAPA-Hirota* because *Lu* would add additional security features to the system and allow tying the security to the hardware platform. *Lu* at 1. *Zadok*, ¶¶408-410. POSITAs would have understood that the when the SD cards described in *Maeda-AAPA-Hirota* are virtualized using *Hamann*'s teachings, binding the virtual SD card to a host computer (*e.g.*, by using a hardware serial number) would ensure that secure data on the virtual SD card cannot be transferred between computers, as only the host computer would have access to the secure area of the virtual SD card. *Zadok*, ¶¶409.

Indeed, POSITAs would have recognized that tying the secure area to the particular computer would make the backed up data even more secure than it otherwise would be, and prevent circumvention of copyrights because encrypted data could only be decrypted on the same authorized computer. POSITAs would also have understood that changing the source of information where keys are derived from is a simple change that requires little experimentation, can be accomplished without undue burden, and that POSITAs would have expected success in making such a small change. *Zadok*, ¶¶409-410.

3. Claim 4

The only difference between claim 4 and claim 3 is that claim 4 requires that encryption key is stored by the computer system, rather than “not stored by the computer system,” as in claim 3. *Maeda-Hamann-AAPA-Hirota-Lu* discloses this claim. As discussed in §VIII.C.1, *Maeda-Hamann-AAPA-Hirota-Lu* discloses that “the file system is encrypted with an encryption key, the encryption key derived from a computer system.” *Hirota* discloses that its master key 323a can be stored “by the computer,” just as claimed. *Hirota*, 16:1-2 (“... master key 323a may be embedded in ... the PC 102 beforehand.”). When *Hirota*’s SD card is virtualized using *Hamann*’s teachings, POSITAs would have understood the encryption key can be stored by the computer system. *Zadok*, ¶¶411-412. As such, only the computer used to create the virtual SD card would have the master key and therefore, access

to the authentication area.

Similarly, *Hamann* discloses that encryption keys can be stored in a “secret key area 16” of its VSC, which POSITAs would understand is necessarily stored by the computer system used to create the VSC. *See Hamann*, ¶[0028] and Fig. 1. Thus, *Maeda-Hamann-AAPA-Hirota-Lu* also discloses this claim. *Zadok*, ¶413.

4. Claim 5

The only difference between claim 5 and claim 4 is that claim 5 requires that the claimed “encryption key” be stored “within a trusted host” of the computer system. *Maeda-Hamann-AAPA-Hirota-Lu* discloses this claim. As discussed, *Hamann* discloses that its computer system uses a VSC control program. *Hamann* further discloses that its computer system uses logic and cryptographic routines for authentication. *Hamann*, ¶[0040]. POSITAs would have understood that this means that the computer is “authenticated” and therefore, a “trusted host.” As such, any key stored “by the computer system” would necessarily mean “within a trusted host.” *Zadok*, ¶¶415-416.

Moreover, as discussed in §VIII.C.3, *Hirota* also discloses that encryption keys can be stored “by the computer system.” *Hirota* teaches that only authenticated devices can get access to the authentication area since master key 323a is used by *Hirota*’s encryption/decryption circuit 327 to control access to the authentication area. *See Hirota*, 11:58-12:4. When *Hirota*’s SD card is virtualized using *Hamann*’s

teachings, and the encryption key is derived from the computer system using *Lu's* teachings (as discussed in §VIII.C.3), the virtual SD card is bound to the computer (to prevent other computers from accessing the SD card). POSITAs would have understood that if master key 323a is stored on the computer system, as *Hirota* teaches is an option, it must be stored in a trusted host (an authenticated device). *Zadok*, ¶¶417-418. This way, only the authenticated computer (the one used to create the virtual SD card) would have access to the master key and therefore, access to the authentication area, while other computers would not be able to access the authentication area of the virtual SD card. *Id.* Thus, claim 5 is obvious.

5. Claim 17

Maeda-Hamann-AAPA-Hirota-Lu discloses/suggests this claim. *Zadok*, ¶¶420-427. The '749*Pat* discloses that when writing data to the virtual SD card's secure area, its "process decrypts 555 data with the key derived during AKE, reads from storage, decrypts the with encryption key, updates data, encrypts with the encryption key, and writes data to the virtual secure area file system 315 of the virtual SD card 300." '749*Pat*, 8:22-27. Decrypting data "with the key derived during AKE" is recited in claim 16, and is rendered obvious by *Maeda-Hamann-AAPA*, as discussed in §VIII.A.5. Claim 17 is directed to the second part of this process, "encrypt[ing] with the encryption key, and writ[ing] data to the virtual secure area file system ..." *Zadok*, ¶¶420-423.

For this process, the *'749Pat* discloses “that there are two encryption keys.” *'749Pat*, 8:27-28. The first key “is for physical storage,” while “[t]he second key is calculated during AKE.” *Id.*, 8:28-29. Because claim 17 recites that “data received from an application program through Authenticated Key Encryption (AKE) is encrypted with another key before storing the data in the secure area of the provisioned virtual SD card,” POSITAs would understand that it is directed to the first key. *Zadok*, ¶424.

POSITAs would have understood that the *'749Pat* discloses that one possible “encryption key for storage” is an encryption key that is derived from unique information regarding the computer on which the virtual SD card is stored. *Zadok*, ¶425. The *'749Pat* discloses that secure area file system 315 is encrypted using an encryption key “derived from the computing device’s unique information...” *'749Pat*, 6:64-7:6. Indeed, the *'749Pat* discloses that during a read operation, “the process fetches and decrypts 560 data from the virtual secure area file system 315 using the key derived from the computing device unique information.” *Id.*, 8:32-35. POSITAs would have understood that if data read from the secure area is decrypted using the derived key, it would have been encrypted using that same derived key. *Zadok*, ¶425.

As discussed in §VIII.C.1 regarding claim 3, *Maeda-Hamann-AAPA-Hirota-Lu* discloses/suggests deriving an encryption key for encrypting data stored in the

“file system for secure data (*e.g.*, *Hamann’s* private area/*Hirota’s* authentication area).” Thus, claim 17 is rendered obvious for the same reasons as discussed regarding claim 3. *Zadok*, ¶426.

6. Claim 20

See §VIII.C.1.

7. Claim 21

See §VIII.C.3.¹⁰

8. Claim 25

See §VIII.C.5.

¹⁰ Note that claim 21 is a multiple dependent claim, depending from claims 18, 19 or 20. Petitioners note that certain of these dependencies have ambiguities. For example, claim 21 recites “the encryption key,” but claim 18 contains no such recitation, making it unclear what the encryption key is. Additionally, while claim 21 states that the encryption key is “stored by the computer system,” claim 20 recites that the encryption key is “not stored by the computer system.” Thus, claim 21’s dependency on claim 20 is nonsensical. Regardless, claim 21, when dependent on claim 19, is rendered obvious *Maeda-Hamann-AAPA-Hirota-Lu*. *Zadok*, ¶430.

D. Ground 4: *Maeda-Hamann-AAPA-Matsukawa* Renders Claim 13 Obvious

1. Claim 13

Maeda-Hamann-AAPA-Matsukawa discloses/suggests this claim. *Zadok*, ¶¶432-435. As discussed in §V.F, *Matsukawa* discloses an authentication method for use in memory devices, including SD cards. *Matsukawa*, ¶¶[0003], [0007]. *Matsukawa* states that SD cards and host computers “generate the same session key for each authentication process between the host computer and the recording medium (SD card).” *Id.*, ¶[0007]. To do so, *Matsukawa* discloses a “media ID generating module 130 [having] the function of generating the media ID in such a manner as not to duplicate a media ID generated in the past” by, for example, “collating with past media IDs after random number generation.” *Id.*, ¶[0051]. *Matsukawa*’s media ID generating module 130 is located in *Matsukawa*’s key generation center unit 100, which is separate from recording medium 300. *Id.*, ¶[0039]. *Matsukawa* states that an SD card is “an example of the recording medium.” *Id.*, ¶[0007]. Thus, POSITAs would have recognized that *Matsukawa* discloses that a media identification is “not allocated from the SD card,” and therefore, *Maeda-Hamann-AAPA-Hirota-Matsukawa* renders claim 13 obvious. *Zadok*, ¶¶433-434.

2. Motivation To Combine

POSITAs would have been motivated to combine *Matsukawa* with *Maeda-Hamann-AAPA*. First, POSITAs would have recognized that *Matsukawa*, like *Maeda* and the *AAPA*, is directed to SD cards. *See Matsukawa*, ¶[0007]. *Zadok*, ¶436.

POSITAs would have recognized that using a random media identification not allocated from an SD card, by adding *Matsukawa*'s random media identification using a media ID generating module 130, would require nothing more than combining known techniques for enhancing security in a predictable manner, with a reasonable expectation of success. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416-417 (Fed. Cir. 2007). Moreover, POSITAs would have recognized that a media identification that includes random data would make the virtual SD card more secure than it otherwise would be. Indeed, using random number generators is a long-established technique in cryptography, because random numbers' high entropy makes them less susceptible to guessing. Conversely, if, say, a vendor assigned sequential ID numbers to each device, it would be much easier to guess them. *Zadok*, ¶¶437-438.

3. The Board Should Not Exercise Its Discretion Under §325(d) To Deny Institution

During prosecution, the Examiner rejected claim 13, asserting that *Matsukawa*

discloses claim 13's subject matter. Patentee, however, never traversed this rejection, and as seen from the above, such a traversal would not have succeeded. In particular, as discussed in §IV.B, patentee overcame the prior art rejections by amending all the independent claims to recite that the "size of the file system for secure data" is determined "based on a lookup table..."

Even though *Matsukawa* was considered during prosecution, the Board should not deny institution under 35 U.S.C. §325(d). See *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8, 17-18 (PTAB Dec. 15, 2017) (precedential); *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6, 9-11 (PTAB Feb. 13, 2020) (precedential).

When a reference is cited during prosecution, *Becton, Dickinson* factors (c), (e), and (f) are evaluated. *Advanced Bionics*, Paper 6, 10–11. Factor (c) is "the extent to which the asserted art was evaluated during examination, including whether the prior art was the basis for rejection." As discussed, the Examiner rejected claim 13 under *Matsukawa*, and patentee never asserted that the Examiner's application to this claim was incorrect. Moreover, Petitioners rely on *Matsukawa* for only one of the fifteen challenged claims (and none of the independent claims). Petitioners respectfully submit that this weighs against discretionary denial of the entire petition, especially when the base references differ from those used by the Examiner. Moreover, the Examiner overlooked the fact that the *AAPA* disclosed the very

feature the Examiner thought distinguished all the claims over the prior art. According to *SolarEdge Techs. LTD v. SMA Solar*, IPR2020-00021, Paper 8, 12 (Apr. 10, 2020), when an Examiner fails to rely on “AAPA [or the other references petition relies on] to reject a claim, *Becton* Factor (c) weighs strongly against exercising our discretion to deny institution.”).

Factor (e) asks “whether Petitioner has pointed out sufficiently how the Examiner erred in its evaluation of the asserted prior art.” This factor is inapplicable since the Examiner correctly found that *Matsukawa* discloses the subject matter recited in claim 13, patentee did not assert otherwise, and the claim was allowed because it depended from other claims containing the “lookup table” limitation the Examiner incorrectly thought was not in the prior art. This weighs against discretionary denial.

Becton, Dickinson factor (f) considers “the extent to which additional evidence and facts presented in the Petition warrant reconsideration of the prior art or arguments.” In this Petition, the base references used to challenge the claims are completely different than those the Examiner relied on during prosecution, demonstrating that *Matsukawa* is presented in a different context than the Examiner viewed it during prosecution. Indeed, Petitioners’ challenges are based almost completely on prior art the Examiner did not consider. In sum, the Board should not exercise its discretion to deny this Petition.

Moreover, the expert evidence in this Petition shows how the references disclose or render obvious every limitation of the challenged claims and the reasons POSITAs would have made the combinations. Thus, Petitioners' challenges are based on additional evidence and arguments that the Examiner did not consider during prosecution, which weighs against exercising discretion under §325(d). *See Mylan Pharms. Inc. v. Merck Sharp & Dohme Corp.*, IPR2020-00040, Paper 21, 20 (PTAB May 12, 2020) (new expert testimony weighs against exercising discretion under §325(d)).

IX. SECONDARY CONSIDERATIONS

There is no evidence in the prosecution history or elsewhere supporting secondary considerations arguments, or evidence of nexus of such alleged evidence to the claims.

X. THE DISCRETIONARY FACTORS FAVOR INSTITUTING TRIAL

The 06/2022 discretionary denial guidance states that institution will not be denied when, as here, Petitioners present a *Sotera* stipulation. (*EX1020*).

XI. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

A. Real Parties-in-Interest

Petitioners identify themselves as the real parties-in-interest.

B. Related Matters

To the best of Petitioners' knowledge, the '749*Pat* has only been involved in

the following district court litigation:

- *Truesight Communications LLC. v. Samsung Electronics Co., Ltd. et al.*, 2-23-cv-00643 (E.D. Tex.), filed December 29, 2023;
- *Truesight Communications LLC. v. TCL Technology Group Corp.*, Case No. 2-24-cv-00032 (E.D. Tex.), filed January 22, 2024; and
- *Truesight Communications LLC. v. Lenovo Group Ltd.*, Case No. 2-24-cv-00031, filed January 22, 2024 (E.D. Tex.).

To the best of Petitioners' knowledge, the '749Pat has not been challenged in any other *inter partes* review or post-grant review prior to this proceeding.

On September 27, 2024, Petitioners filed a petition for inter partes review that challenged U.S. Patent No. 8,898,803 (IPR2024-01477).

C. Lead and Backup Counsel

Lead Counsel	Back-Up Counsel
Jeffrey A. Miller (Reg. No. 35,287) jeffrey.miller@apks.com Arnold & Porter Kaye Scholer LLP 5 Palo Alto Square, Suite 500 3000 El Camino Real Palo Alto, CA 94306 Tel: 650-319-4519	Ali R. Sharifahmadian (Reg. No. 48,202) ali.sharifahmadian@arnoldporter.com Arnold & Porter Kaye Scholer LLP 601 Massachusetts Ave., NW Washington, DC 20001-3743 Tel: 202-942-5000 Fax: 202-942-5999

D. Service Information

Please address all correspondence to lead and back-up counsel at the addresses shown above. Petitioners consent to electronic service by e-mail.

E. Power of Attorney

A power of attorney is filed herewith according to 37 C.F.R. §42.10(b).

XII. FEES

Petitioners concurrently electronically submit the required fees for this Petition. The Board is authorized to charge Arnold & Porter Kaye Scholer LLP's deposit account, No. 50-2387, for any fee deficiency.

Date: November 1, 2024

Respectfully submitted,

/Jeffrey A. Miller/

Jeffrey A. Miller, Lead Counsel
Reg. No. 35,287

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that the foregoing Petition for *Inter Partes* Review contains 13,989 words, excluding those portions identified in 37 C.F.R. §42.24(a), as measured by the word-processing system used to prepare this paper.

/Jeffrey A. Miller/
Jeffrey A. Miller, Lead Counsel
Reg. No. 35,287

CERTIFICATE OF SERVICE

I certify that on November 1, 2024, I caused a true and correct copy of the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 8,745,749 and supporting exhibits to be served via overnight delivery on the Patent Owner at the following correspondence address of record as listed on Patent Center:

Peter Lambrianakos
Fabricant LLP
411 Theodore Fremd Road
Suite 206 South
Rye, NY 10580

A courtesy copy was also sent via electronic mail to Patent Owner's litigation counsel listed below:

Alfred R. Fabricant (ffabricant@fabricantllp.com)
Peter Lambrianakos (plambrianakos@fabricantllp.com)
Vincent J. Rubino, III (vrubino@fabricantllp.com)
John Andrew Rubino (jarubino@rubinoip.com)
Michael Mondelli III (mmondelli@rubinoip.com)
Samuel F. Baxter (sbaxter@mckoolsmith.com)
Jennifer L. Truelove (jtruelove@mckoolsmith.com)

/Jeffrey A. Miller/
Jeffrey A. Miller, Lead Counsel
Reg. No. 35,287