UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TRANSCEND INFORMATION INC.,

Petitioner,

v.

TRUESIGHT COMMUNICATIONS LLC,

Patent Owner.

Case: IPR2025-00723
U.S. Patent No. 8,977,783

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 8,977,783

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

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Rules and Regulations

EXHIBIT LIST

Exhibit No.	***Description***
1001	U.S. Patent No. 8,977,783 B2 to Hahn et al.
1002	File History for U.S. Patent No. 8,977,783 B2 to Hahn et al.
1003	Declaration of Dr. Jacob Baker
1004	*Curriculum Vitae* of Dr. Jacob Baker
1005	U.S. Patent Publication No. 2009/0113116 (Thompson)
1006	U.S. Patent Publication No. 2010/0205023 (Wagner)
1007	U.S. Patent Publication No. 2007/0116268 (Kasahara)
1008	Enabling Secure Distribution of Digital Media to SD Cards (Ponceleon)
1009	Secure MultiMediaCard for Content Protection (Ishihara)
1010	Scheduling Order in the Texas Action
1011	Complaint in Texas Action
1012	Declaration of Dr. Sylvia Hall-Ellis
1013	*Curriculum Vitae* of Dr. Sylvia Hall-Ellis
1014	MARC record Auraria Library – *Proceedings of the 14th Annual ACM International Conference on Multimedia*
1015	MARC record OCLC – *Proceedings of the 14th Annual ACM International Conference on Multimedia*
1016	Library of Congress Subject Heading (sh89003285)
1017	Library of Congress Subject Heading (sh85042288)
1018	MARC record King Library – *ECN: Electronic Component News*
1019	MARC record OCLC – *ECN: Electronic Component News*

I. MANDATORY NOTICES

A. Real Party-In-Interest (37 C.F.R. §42.8(b)(1))

Petitioner Transcend Information Inc. ("Petitioner" or "Transcend") is a real party-in-interest.

B. Identification of Related Matters (37 C.F.R. §42.8(b)(2))

Patent Owner has asserted U.S. Patent No. 8,977,783 (the "'783 Patent") against Petitioner in co-pending civil litigation, *Truesight Communications LLC v. Transcend Information Inc.*, No. 2:24-cv-00186-JRG (E.D. Tex.) ("Texas Action"). Petitioner was served with the Complaint in that action on May 21, 2024. Ex[1011].

C. Counsel and Service Information (37 C.F.R. §§42.8(b)(3) & (b)(4))

Petitioner designates the following Lead and Backup Counsel. Concurrently filed with this Petition is a Power of Attorney for appointing the following Lead and Backup Counsel, per 37 C.F.R. § 42.10(b). Service via hand-delivery may be made at the postal mailing addresses below. Petitioner consents to electronic service by email at the following address: Case-TranscendIPRMembers@pillsburylaw.com.

Lead Counsel	**Back-Up Counsel**
Robert C.F. Pérez (Reg. No. 39,328) PILLSBURY WINTHROP SHAW PITTMAN LLP 7900 Tysons One Place, Suite 500 Tysons, VA 22102 Telephone: 703.770.7759 Facsimile: 703.770.7901 Email: robert.perez@pillsburylaw.com	**Christopher Kao** (*Pro Hac Vice* to be requested) **Brock S. Weber** (*Pro Hac Vice* to be requested) PILLSBURY WINTHROP SHAW PITTMAN LLP Four Embarcadero Center, 22nd Floor San Francisco, CA 94111 Telephone: 415.983.1000 Facsimile: 415.983.1200 christopher.kao@pillsburylaw.com brock.weber@pillsburylaw.com

D. Payment of Fees (37 C.F.R. §42.103)

Petitioner authorizes the Patent and Trademark Office to charge Deposit Account No. 033975 for the petition fee and for any other required fees.

II. INTRODUCTION

Petitioner Transcend hereby requests *inter partes* review ("IPR") of Claims 1-18 of U.S. Patent No. 8,977,783, and the cancellation of those claims as unpatentable.

The claims of the '783 Patent are unpatentable under 35 U.S.C. § 103 as rendered obvious by multiple prior art references. The '783 Patent discloses and claims the basic and well-known process of downloading media files to a Secure Digital ("SD") card through a kiosk. This technology substantially predates the '783 Patent, and the specific combination of this old technology in the claims would have been entirely obvious to a person of ordinary skill in the art at the time of earliest priority date in October 2009. Specifically, Claims 1-18 are rendered obvious by the following prior art references presented herein:

- U.S. Patent Publication No. 2009/0113116 ("Thompson") (Ex[1005])
- U.S. Patent Publication No. 2010/0205023 ("Wagner") (Ex[1006])
- U.S. Patent Publication No. 2007/0116268 ("Kasahara") (Ex[1007])
- Enabling Secure Distribution of Digital Media to SD Cards ("Ponceleon") (Ex[1008])
- Secure MultiMediaCard for Content Protection ("Ishihara") (Ex[1009])

These references were not discussed or cited during prosecution of the '783 Patent and they render Claims 1-18 obvious as described in detail below.

III. REQUIREMENTS FOR INTER PARTES REVIEW

This petition complies with all statutory requirements and requirements 37 C.F.R. §§ 42.103-105 and 42.15 and thus should be accorded a filing date pursuant to § 42.106.

IV. GROUNDS FOR STANDING UNDER § 42.104(A).

Pursuant to 37 C.F.R. 42.104(a), Petitioner certifies that the '783 Patent is available for IPR and that Petitioner is not barred or estopped from challenging its claims.

V. IDENTIFICATION OF CHALLENGE UNDER § 42.04(B)

A. Challenged claims under § 42.104(b)(1)

Pursuant to 37 C.F.R. §§ 42.104(b) and 42.22, Petitioner requests that the Board institute an IPR trial on Claims 1–18 of the '783 Patent and cancel all of those claims as unpatentable.

Prior art: The prior art references relied upon are Thompson (Ex. 1005), Wagner (Ex. 1006), Kasahara (Ex. 1007), Ponceleon (Ex. 1008), and Ishihara (Ex. 1009), as set forth in the Grounds, below.

Ground 1: Claims 1-3, 5-8, 10-13, 15, and 16 are unpatentable under 35 U.S.C. § 103(a) as obvious over Thompson and Kasahara.

Ground 2: Claim 4 is unpatentable under 35 U.S.C. § 103(a) as obvious over Thompson and Kasahara in view of Wagner.

Ground 3: Claims 9 and 14 are unpatentable under 35 U.S.C. § 103(a) as obvious over Thompson and Kasahara in view of Ishihara.

Ground 4: Claims 17 and 18 are unpatentable under 35 U.S.C. § 103(a) as obvious over Thompson and Kasahara in view of Ponceleon.

Ground	**Claims**	**Invalidating Art**
1	1-3, 5-8, 10-13, 15, 16	Thompson, Kasahara

Ground	**Claims**	**Invalidating Art**
2	4	Thompson, Kasahara, Wagner
3	9, 14	Thompson, Kasahara, Ishihara
4	17 and 18	Thompson, Kasahara, Ponceleon

VI. SUPPORTING EVIDENCE

The evidence includes the Declaration of Dr. Jacob Baker (Ex[1003]) and other supporting evidence in the Evidence List.

VII. STATUTORY GROUNDS

Pursuant to 37 C.F.R. § 42.104(b)(2), the review of patentability of Claims 1–18 is governed by AIA 35 U.S.C. §§ 102 and 103. Further, statutory provisions of 35 U.S.C. §§ 311 to 319 and 325(d) govern this IPR.

VIII. CLAIM CONSTRUCTION

For the purposes of this Petition, Petitioner contends that, unless otherwise specifically noted herein, the claim terms in the ’783 Patent are accorded their ordinary and customary meaning that they would have to a person of ordinary skill in the art at the time of the alleged invention (“POSITA”). Petitioner’s interpretation of the claim terms is further explained for each limitation in relation to the prior art discussed in Grounds 1-4, below.[1]

IX. A PERSON HAVING ORDINARY SKILL IN THE ART

As opined by Dr. R. Jacob Baker, an ordinarily skilled artisan at the time of the alleged invention would have at least a bachelor's degree in computer science, computer engineering, electrical engineering, or a related field and two to three years of experience in the field of data management. Ex[1003], Declaration of R. Jacob Baker, Ph.D, P.E. ("Baker Decl.") at ¶ 27.

X. OVERVIEW OF THE '783 PATENT

A. Purported Invention of the '783 Patent

U.S. Patent No. 8,977,783 [Ex. 1001], titled "High-Speed Secure Content Transfer to SD Card from Kiosk," was filed on October 18, 2010, and issued on March 10, 2015. The '783 Patent is directed to securely transferring digital media content to a Secure Digital (SD) card via a kiosk-based distribution system. Ex[1001] at Abstract.

[1] Petitioner reserves the right to address any claim construction positions taken by the Patent Owner in its Preliminary Response, including under 37 C.F.R. § 42.108(c).

In particular, the ‘783 Patent discloses a kiosk that enables customers to select and purchase media files, which are then securely transferred to an SD card. The ’783 Patent acknowledges, as it must, that this is nothing new, as the prior art included a “method of distributing digital media content [] through kiosk systems.” Ex[1001] at 1:18-21. The ’783 Patent purports to disclose that its system includes a customer interface module, a transaction module for processing payments, and an SD card writer that writes data to both the secure and unsecure areas of the SD card. Ex[1001] at Abstract; *see also* Claim 1. These basic components are illustrated in Figure 1 of the patent (reproduced to the right).

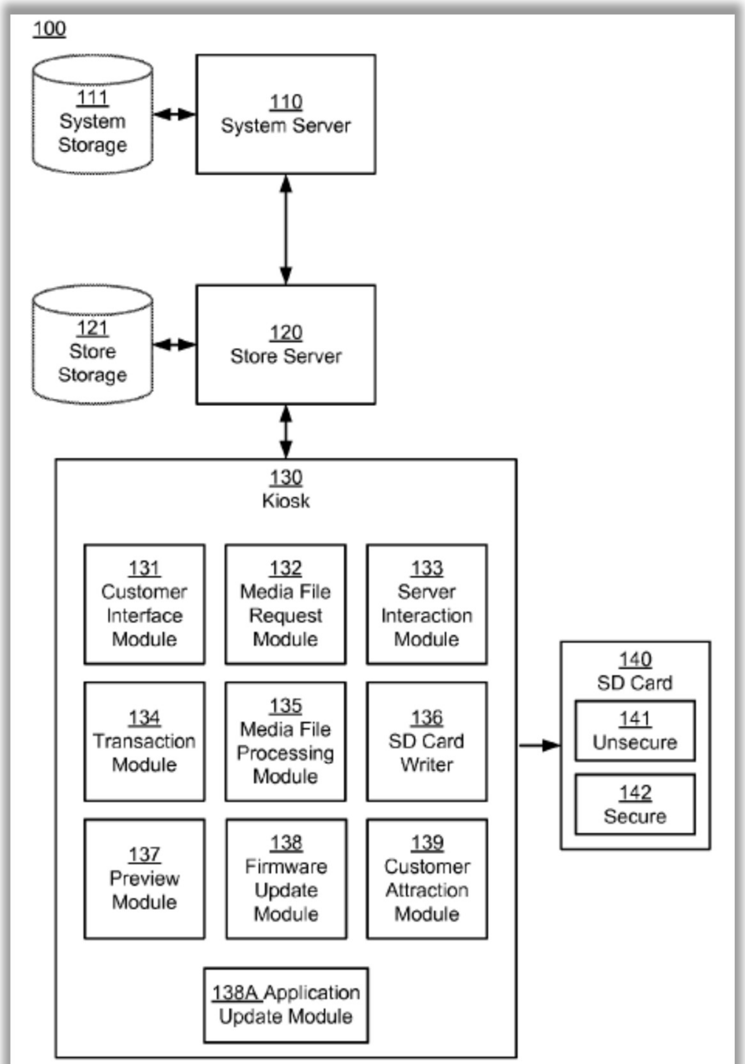

100
111 System Storage
110 System Server
121 Store Storage
120 Store Server
130 Kiosk
131 Customer Interface Module
132 Media File Request Module
133 Server Interaction Module
134 Transaction Module
135 Media File Processing Module
136 SD Card Writer
137 Preview Module
138 Firmware Update Module
139 Customer Attraction Module
138A Application Update Module
140 SD Card
141 Unsecure
142 Secure

FIG. 1

However, this is a conventional and well-known arrangement for the downloading of media content to a storage medium, according to the ’783 Patent itself in its “Description of [Prior] Art”:

> The kiosk is connected via a network to one or more servers having access to storage of digital media content. Customers can interact with the kiosk, for example through a touch screen interface, to select desired digital media content for purchase. The desired digital media content is located either in a storage local to the kiosk or in a remote storage and served to the kiosk. Then, the desired digital media content is downloaded to a storage medium, for example the memory in a customer’s digital playback device that has been connected to the kiosk, or another computer-readable medium such as a CD or DVD.

Ex[1001] at 1:22-32.

Further, the ’783 Patent does not purport to have invented SD cards or their fundamental architecture, including the well-known distinction between the secure and unsecure areas of an SD card. Rather, the patent explicitly describes SD cards as pre-existing technology, explaining that an “SD card comprises a media device having computer readable and writable storage areas with a secure area and an unsecure area thereon” and that “one embodiment of the system includes a configuration for high-speed secure writing to an SD card.” Ex[1001] at 2:10, 2:22-23. The patent further acknowledges that writing data to both secure and unsecure areas of SD cards follows established standards, specifically referencing Content

Protection for Recordable Media ("CPRM") for managing digital rights (Ex[1001] at 4:55-61). These statements confirm that an SD card having secure and unsecure areas, as well as the process of writing to these areas in compliance with existing security protocols, was known in the art and not an invention of the '783 Patent.

B. Priority Date

The earliest possible priority for the '783 Patent is October 21, 2009, the date U.S. Provisional Application No. 61/253,789 was filed. Ex[1001] at 1:7-10. Petitioner does not concede that the claims of the '783 Patent are entitled to that date but will use it for this Petition.

XI. OVERVIEW OF THE STATE OF THE ART

Petitioner presents the references below, none of which were cited or discussed during prosecution of the '783 Patent. Ex[1002].

A. U.S. Patent Publication No. 2009/0113116 ("Thompson") (Ex[1005])

Thompson is a publication of a U.S. patent application filed by SanDisk on October 30, 2007, and published on April 30, 2009. Thompson is prior art to the '783 Patent under at least 35 U.S.C. §§ 102(e).[2]

[2] Pre-AIA 35 U.S.C. §§ 102 and 103 apply to the '783 Patent, as it was filed on October 18, 2010.

Thompson discloses a digital content kiosk for writing digital media onto removable solid-state memory devices. Ex[1005] at [0031]. As with the ’783 Patent, Thompson discloses a kiosk distribution system that includes a customer interface module, a transaction module for processing payments, and programming circuitry for writing content to a solid state storage medium, such as a SD card. Ex[1005] at [0042], [0044], [0105]. For example, Thompson’s kiosk is depicted in Figure 1a, and the logical connections to a content server and the removable memory device is shown, e.g., in Figure 22a.

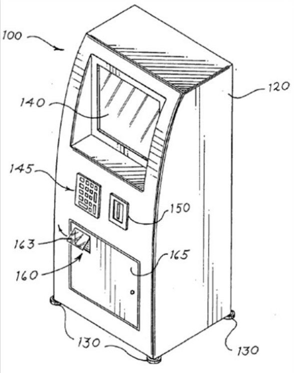


Fig. 1a

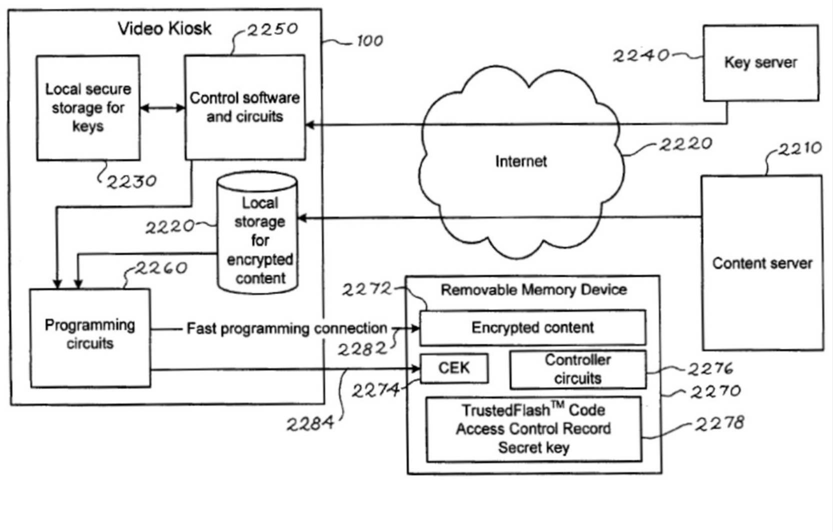


Fig. 22 a

Thompson also discloses methods for efficiently storing encrypted media content onto memory cards and ensuring secure access. For instance, Thompson states that its “video kiosk establishes communication with a removable solid-state memory device . . . and then programs the selected video content into a solid-state memory array in the memory device." Ex[1005] at [0044]. Thompson discloses that this memory device can be an SD card. *See* Ex[1005] at [0047] ("For example, in one embodiment, the user port 320 takes the form of an SD port with a data transfer rate in the range of 5 MB/sec to 20 MB/sec").

Additionally, Thompson teaches mechanisms for encrypting digital content and using transaction-based authorization to determine user rights before granting access. Specifically, Thompson describes that "[p]ayment can be made either through the payment device on the video kiosk, or the cost of the video content can be deducted from the user's account or automatically charged to a credit card on file." Ex[1005] at [0117].

B. U.S. Patent Publication No. 2010/0205023 ("Wagner") (Ex[1006])

Wagner is a publication of a U.S. patent application filed on October 8, 2009, and published on August 12, 2010. Wagner is prior art to the '783 Patent under at least 35 U.S.C. § 102(e).

Wagner discloses a system for high-speed digital media distribution, focusing on optimizing data transfers to secure and portable storage devices. *See* Ex[1006] at [0020]. One embodiment of the system disclosed by Wagner includes a "customer point of content delivery," comprising "a user-interface," and an "output configured to interface with and communicate with a portable digital content storage device. . . .” *Id.* at [0025]. This embodiment can take the form of kiosks. *See id.* at [0001]; Fig. 2.

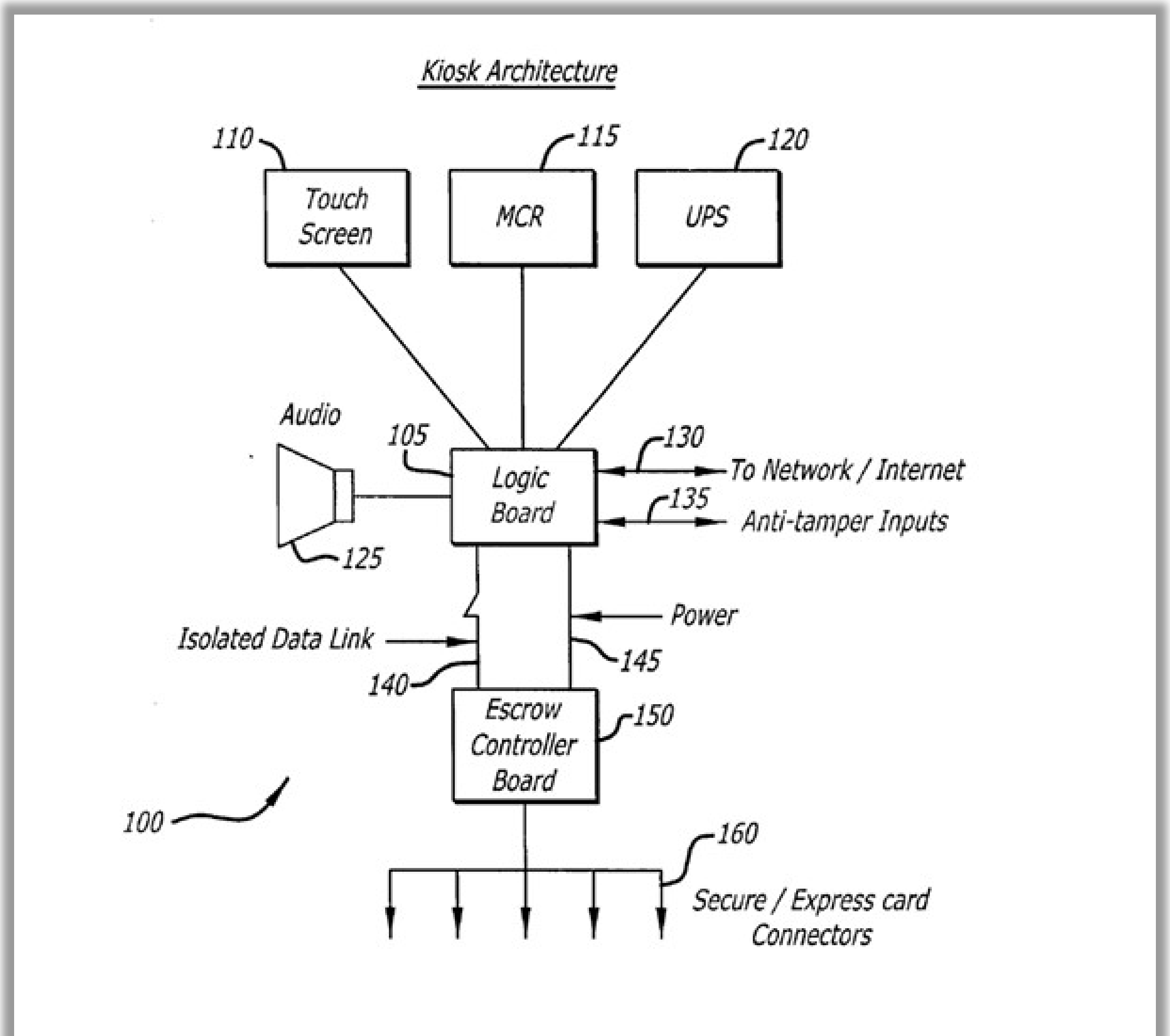


FIG. 2

Additionally, Wagner discloses that the media content purchased or rented from the kiosk could be encrypted with appropriate digital rights management information. *Id.* at [0043]. The user would then need to the right to access the encrypted content, which would be provided in the form of a content key which can be downloaded from the kiosk after purchase. *Id.* at [0055].

Wagner explains that the well-known architecture of secure flash cards makes this encryption process simple and easy, noting that "the system can be used to encrypt the customers own content in an exceptionally secure manner because the encryption key can be tied to the secure flashcard **200** itself." *Id.* at [0062].

C. U.S. Patent Publication No. 2007/0116268 (Kasahara) (Ex[1007])

Kasahara is a publication of a U.S. patent application filed on November 14, 2006, and published on May 24, 2007. Kasahara is prior art to the '783 Patent under at least 35 U.S.C. §§ 102(b).

Kasahara describes a method for delivering encrypted content data to portable storage media such as SD cards. The disclosed system utilizes a server-client model where users can download protected digital content from a remote server onto an SD card. The encryption framework is based on CPRM, ensuring that content can only be played back on authorized devices. Notably, Kasahara discloses user keys which are stored in an SD card "in such a way that the user key data is unable to be read out of the internal memory[.]" Ex[1007] at [0010]; *see also id.* at [0040].

A key aspect of Kasahara's disclosure is this encryption structure, wherein encrypted content data (encrypted by a content key) is stored in an SD card along with a user key, which is stored in the protected area of the SD card. *Id.* at [0040]. An encrypted content key is thereafter downloaded into internal memory. *Id.* at [0044]. The encrypted content key is then decrypted by the user key, and the decrypted content key in turn can be used to decrypt the encrypted content data, thus allowing the user to access it. *Id.* at Abstract.

D. Enabling Secure Distribution of Digital Media to SD Cards (Ponceleon) (Ex[1008])

Ponceleon is a publication of a conference paper first published in October 2006. Ex[1012], Declaration of Sylvia Hall-Ellis, Ph.D, ("Hall-Ellis Decl.") at ¶ 58. Ponceleon is prior art to the '783 Patent under at least 35 U.S.C. § 102(b).

Ponceleon provides a comprehensive discussion on secure digital media distribution, emphasizing high-speed downloads and DRM enforcement through the use of SD cards. The reference highlights a kiosk-based system where users can insert their SD cards, select content, and securely download encrypted media files. The system leverages CPRM to enforce digital rights, ensuring that playback is only possible on compliant devices. This system is shown in Figure 1:

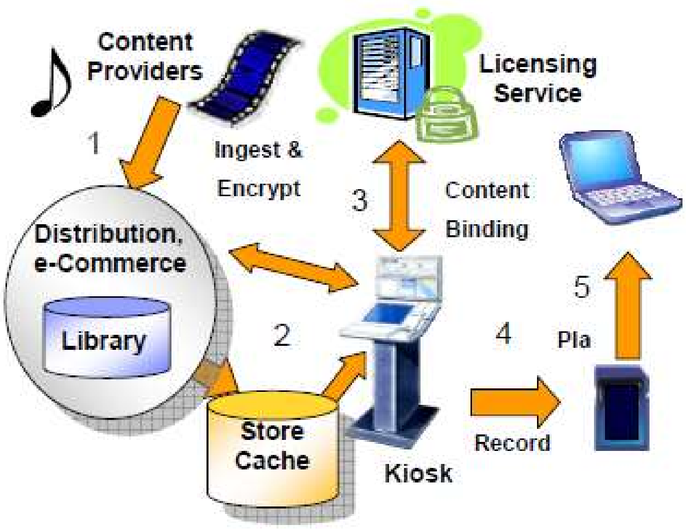


Figure 1: Secure Multimedia Distribution Architecture

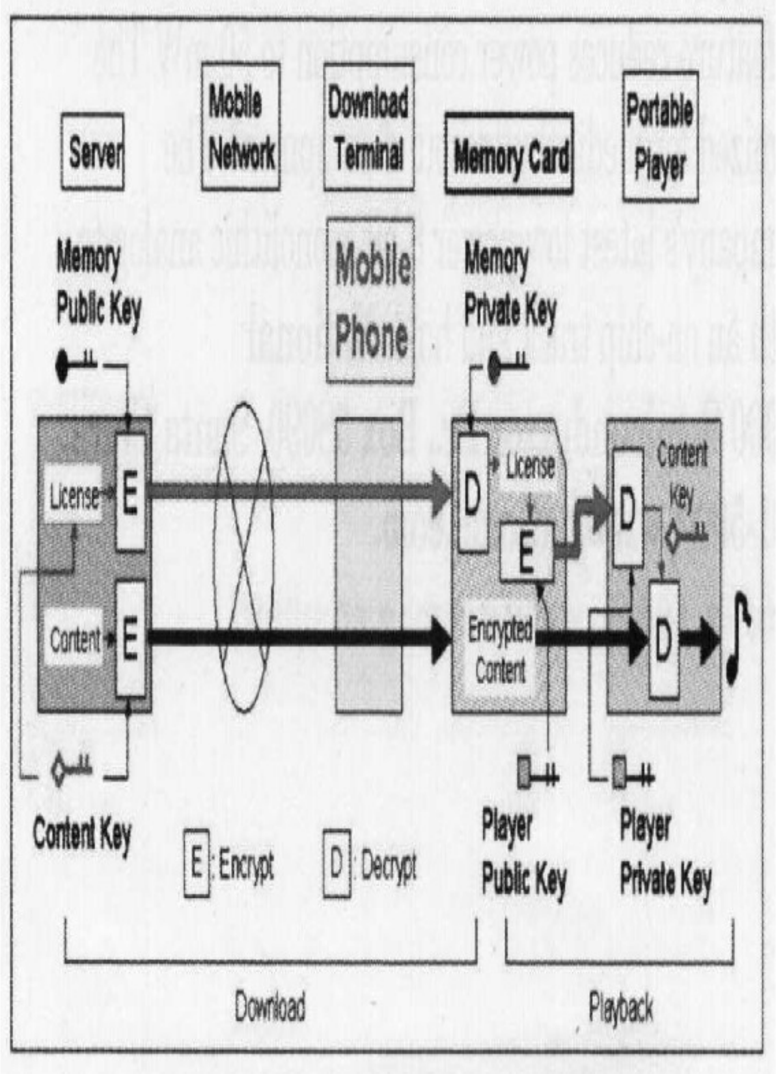
Ponceleon further discloses the implementation of a subscription-based rental model. The paper describes a process where a licensing server validates user entitlements before allowing content downloads. Ex[1008] at 496. Upon successful verification, the kiosk writes the encrypted content to the SD card and then securely stores a decryption key in the protected area of the card. Ex[1008] at 496.

Moreover, Ponceleon discusses the use of pre-cached encrypted content at kiosks to enable high-speed downloads, significantly reducing the time required to transfer full-length media files. Ex[1008] at 496.

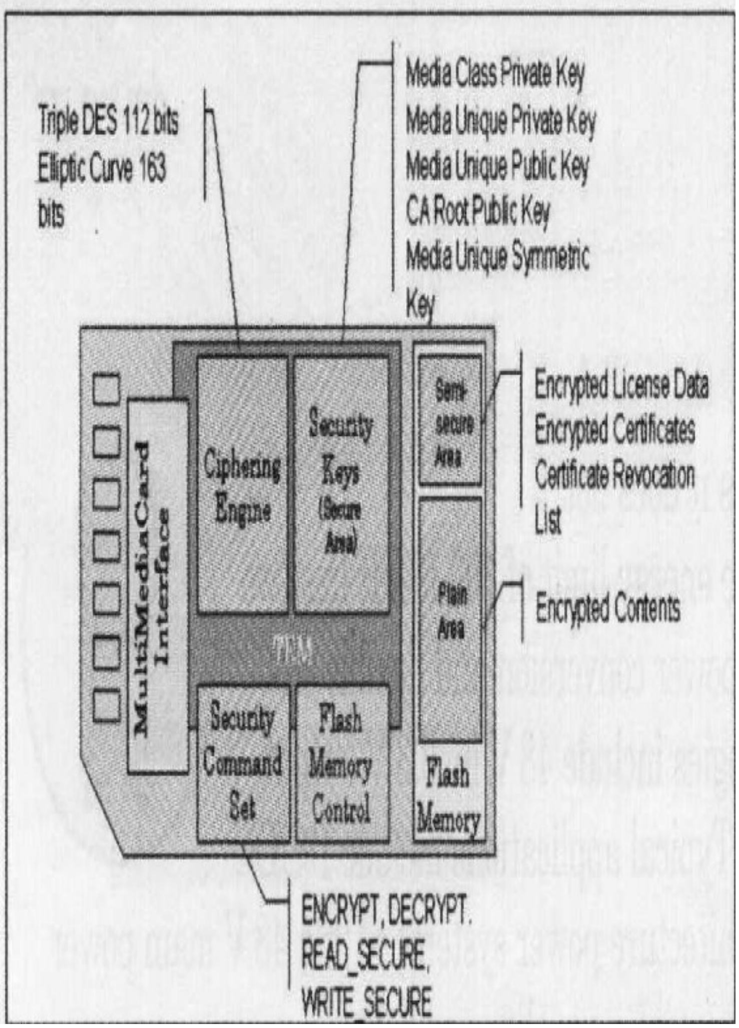
E. Secure MultiMediaCard for Content Protection (Ishihara) (Ex[1009])

Ishihara is a publication of an article published on December 15, 2001. Ex[1012] at ¶ 58. Ishihara is prior art to the ’783 Patent under at least 35 U.S.C. § 102(b).

Ishihara presents a content protection system for digital media distribution using Secure MultiMediaCards (“SMMC”). The reference describes a framework where encrypted content is stored on an SMMC, and access is controlled through a licensing server that issues decryption keys upon successful transaction validation. Ex[1009] at p. 23, 26. This system is illustrated in the figure below:



Ishihara further discloses a Public Key Infrastructure (PKI)-based approach to digital rights management. Ex[1009] at p. 23, 26. The system ensures that encrypted media remains secure by storing decryption keys in a tamper-resistant module, preventing unauthorized access. Ex[1009] at p. 23, 26. An example of this type of secure storage device is depicted in the following figure:



XII. GROUND 1: CLAIMS 1-3, 5-8, 10-13, 15, and 16 ARE OBVIOUS OVER THOMPSON IN VIEW OF KASAHARA

A. Motivation to Combine

A POSITA would have been motivated to combine Thompson (Ex[1005]) and Kasahara (Ex[1007]) because both references are directed toward efficient and digital media distribution. Ex[1005] at [0031]-[0034]; Ex[1007] at [0032]. Thompson teaches a kiosk-based system for transferring digital content to portable storage media (Ex[1005] at [0032]), while Kasahara describes an encryption and secure content management system for digital content distribution via SD cards (Ex[1007] at [0009]). Combining these teachings would have been an obvious improvement to enhance security and efficiency in media distribution kiosks. Ex[1003], ¶ 69. A POSITA would have been motivated to combine Thompson and Kasahara. Thompson and Kasahara are analogous to one another and both disclose a physical terminal-based system for delivery content in encrypted form to a memory device, just as in the '783 Patent. Ex[1003], ¶ 70. Like the '783 Patent, both references are in the same field of endeavor of secure content delivery to memory devices. Ex[1003], ¶ 70. Both references solve similar problems and complement each other in addressing content security, structured writing, and transaction validation. Ex[1003], ¶ 70.

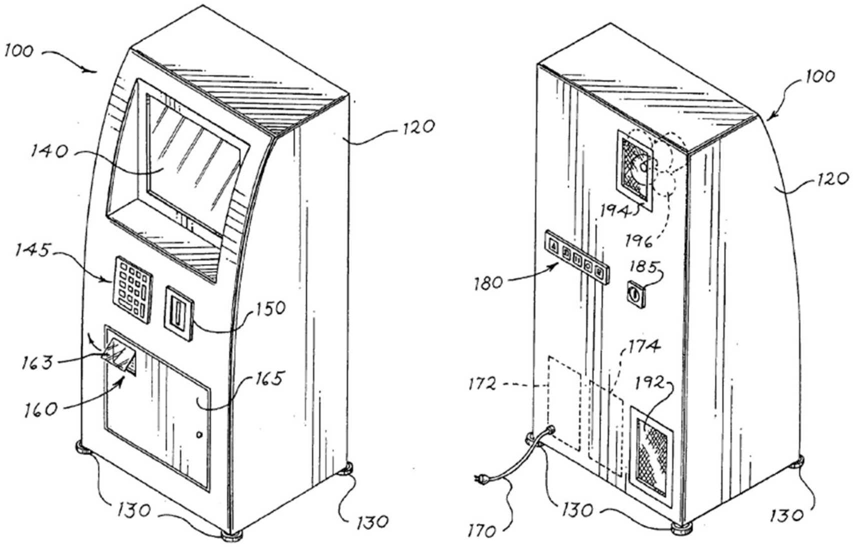
A POSITA would have recognized that integrating Kasahara's encryption techniques into Thompson's kiosk system would provide a robust solution for secure digital content transfers. Ex[1003], ¶ 72. Kasahara's encryption system is highly compatible with Thompson's kiosk-based media distribution platform. Thompson discloses a kiosk that transfers digital content to removable media (Ex[1005] at [0032]), but it does not focus on a detailed encryption scheme for securing that content. Kasahara provides such an encryption mechanism, which ensures that content transferred to SD cards remains secure and protected from unauthorized use (Ex[1007] at [0061]).

Given the increasing need for **s**ecure and efficient media transactions, a POSITA would have been motivated to combine these references to enhance both security and reliability in digital content distribution systems. Ex[1003], ¶ 73.

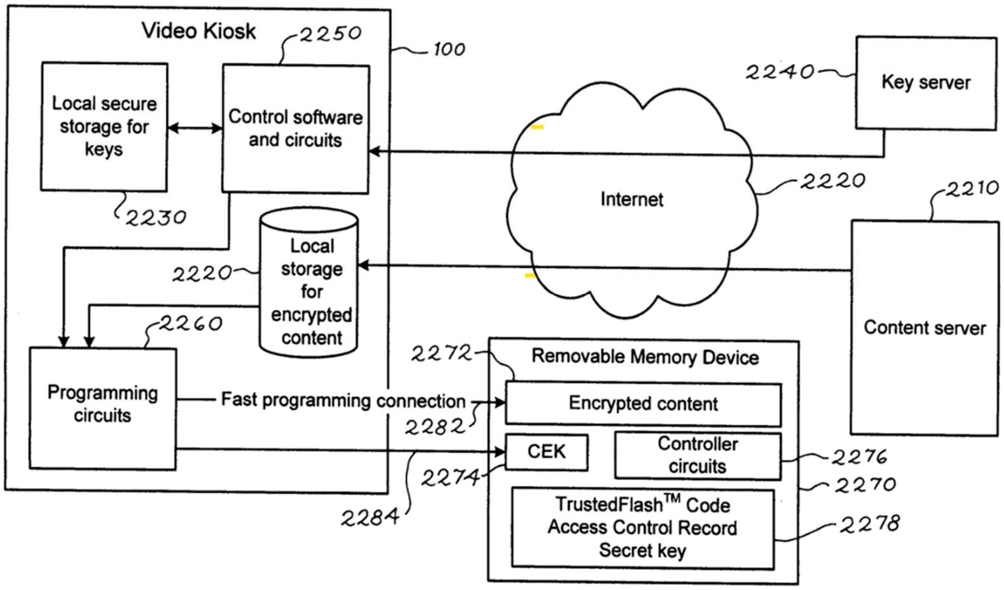
B. Independent Claim 1

1. 1[pre]: A kiosk for transferring content to a secure digital (SD) card, the kiosk comprising:

To the extent the preamble is a limitation, Thompson in view of Kasahara renders obvious limitation 1[pre]. Ex[1003], ¶ 74. Thompson discloses "a digital content kiosk for on-the-fly programming of digital content onto a removable solid-state memory device." Ex[1005] at [0031].



Ex[1005], Figs. 1a-1b.



Id., Fig. 22a.

Thus, Thompson discloses a "kiosk" that "transfer[s] content." Additionally, Thompson discloses transferring content to a "removable solid-state memory device," defined as "a memory device that uses a solid-state memory array to store data," which a POSITA would have understood necessarily to include an SD card. Ex[1005] at [0036]; Ex[1003], ¶ 75.

To the extent that Thompson's "removable solid-state memory device" does not disclose an "SD card," it would have been obvious to a POSITA to modify Thompson's kiosk system to use an SD card as an output medium. Thompson explicitly states that a "kiosk can be altered to use other types of devices," which can be "any type of media." Ex[1005] at [0033], [0037]. And, as the '783 Patent concedes, SD cards were already well-known and adapted for this use case. Ex[1001] at 2:8-12; Ex[1003], ¶ 76.

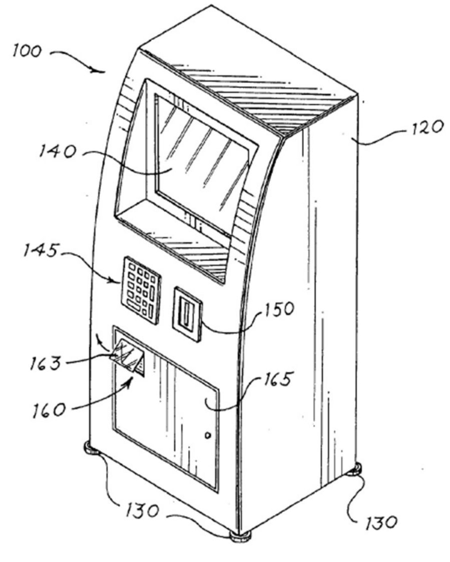
Additionally, Kasahara is a prior patent publication that discloses a content delivery system for delivering content to an SD card. Ex[1003], ¶ 77. For example, Kasahara discloses that "a user may have a personal computer (PC) 10, an SD memory card (SD card) 20, and a handheld terminal 30 (user terminal)" (Ex[1007] at [0032]), and "[t]he user connects the SD card 20 to the PC 10 to access the server 50, and downloads... encrypted content data Ci[.]" *Id.* at [0033]. Kasahara's content delivery system is intended for use in "stores, such as a conveneince store, [where] a store terminal 40 that is [] connected via the Internet or a leased (dedicated) line to the server [that provides the content]." *Id.* Therefore, a POSITA would have understood that Kasahara's content delivery system may be adapted to a physical store terminal such as a kiosk. Ex[1003], ¶ 78.

2. 1[a]: a customer interface module for receiving a customer's selection of a plurality of media files to transfer to the SD card;

Thompson discloses this limitation. Ex[1003], ¶ 79.

As explained by the '783 Patent, the "customer interface module" "manages a graphical user interface presented to a customer, through which, the customer can select media to preview at the kiosk 130 or download to the customer's SD card." Ex[1001] at 4:5-8.

Thompson discloses a video kiosk 100 that "receives a selection of video content either manually from a user using the touch-screen display 140 and/or the key pad 145" Ex[1005] at [0044]. Further the touch-screen display 140 and the key pad 145 constitute a "customer interface module" because they present a user interface through which a customer can select media to download to a memory device. *Id.* at [0038], [0044]. Because the kiosk disclosed by Thompson "manages a graphical user interface presented to a customer, through which, the customer can select media to. . . download to the customer's [memory device]" a POSITA would understand that Thompson discloses a "customer interface module." Ex[1003], ¶ 79.



Ex[1005], Fig. 1a.

To the extent that Thompson's "memory device" does not disclose an "SD card," it would have been obvious to a POSITA to modify Thompson's kiosk system to use an SD card as an output medium. Thompson explicitly states that a "kiosk can be altered to use other types of devices," which can be "any type of media." Ex[1005] at [0033], [0037]. And, as the '783 Patent concedes, SD cards were already well-known and adapted for this use case. Ex[1001] at 2:8-12; Ex[1003], ¶ 81.

3. 1[b]: a media file request module for requesting the plurality of media files and corresponding metadata file for each media file from a server communicatively coupled to the kiosk;

Thompson discloses this limitation. Ex[1003], ¶ 82.

As explained by the '783 Patent, the "media file request module" "receives the user's selections of media from the customer interface module 131 and prepares a request for the corresponding media files, for example, by performing a lookup of the selected media file." Ex[1001] at 4:16-21.

Thompson discloses requesting media files based on a user's selection. Ex[1005] at [0042] ("the video kiosk 100 can connect to an external network location to retrieve video content on-the-fly when requested by a user or to retrieve video content for local storage on one or more mass storage devices in the video kiosk 100.)." Thus, because the kiosk disclosed by Thompson includes functionality for requesting media files in response to user input, a POSITA would have understood that Thompson's kiosk includes a "media file request module" for requesting media files from a server communicatively coupled to the kiosk. Ex[1003], ¶ 83.

To the extent that Thompson's retrieval of "video content" does not disclose a "corresponding metadata file," it would have been obvious to a POSITA that a download of a video file could and would include a metadata file. Ex[1003], ¶ 84. As the '783 Patent explains, "[m]etadata includes the title of the playable content, and expanded descriptive information about the content, such as the actors, the director, and/or other information that may appear on or inside a DVD box, for example." Ex[1001] at 3:36-39. Thompson discloses that the control program and electronics 2300 can load "extra features" or "additional video". Ex[1005] at [0123]. Including such information with the download of a video file would have been obvious to a POSITA, as such information is useful to display to the user during playback of the video content. Ex[1003], ¶ 85. Further, providing such information with video rentals was common practice. Ex[1003], ¶ 85.

4. 1[c]: a server interaction module for receiving the requested plurality of media files and the corresponding metadata files from the server;

Thompson discloses this limitation. Ex[1003], ¶ 86.

As explained by the ’783 Patent, the “server interaction module” “manages communications between the kiosk 130 and the store server 120” and “receives media files from the store server 120 that are distributed to the kiosk 130.” Ex[1001] at 4:22-24 and 4:27-29.

Thompson discloses a kiosk that receives a media file from a server. Ex[1005] at [0101] (“if the local mass storage device 2200 does not have a video title desired by a user, the video kiosk 100 can contact the content server 2210 on-the-fly to download the desired video content**.**”). Thus, because the kiosk disclosed by Thompson includes functionality for “communicat[ing] with a store server” and “receiv[ing] media files from the store server” a POSITA would have understood that Thompson’s kiosk includes a “server interaction module” of the type claimed in the ’783 Patent. Ex[1003], ¶ 87.

To the extent that Thompson’s retrieval of “video content” does not disclose a “corresponding metadata file,” it would have been obvious to a POSITA that a download of a video file could and would include a metadata file. Ex[1003], ¶ 88. Again, as the ’783 Patent explains, “[m]etadata includes the title of the playable content, and expanded descriptive information about the content, such as the actors, the director, and/or other information that may appear on or inside a DVD box, for example.” Ex[1001] at 3:36-39. Thompson discloses that the control program and electronics 2300 can load "extra features" or "additional video." Ex[1005] at [0123]. Including such information with the download of a video file would have been obvious to a POSITA, as such information is useful to display to the user during playback of the video content. Ex[1003], ¶ 85. Further, providing such information with video rentals was common practice. Ex[1003], ¶ 85.

5. 1[d]: a transaction module for accepting payment from a customer for the customer's selection of the plurality of media files to transfer to the SD card;

Thompson discloses this limitation. Ex[1003], ¶ 89.

As explained by the '783 Patent, the "transaction module" "manages the payment detail of the customer's purchase form the kiosk 130. The transaction module 134 receives the customer's payment information, for example from information read from the swipe of a card through a card reader. . ." Ex[1001] at 4:30-34.

Thompson discloses a payment input device which allows a user to purchase video content from the video kiosk. Ex[1005] at [0040]. Thompson specifically states that "[t]he control program and electronics 2300 can then present a payment screen to facilitate the purchase of the video content and removable memory device." *Id.* at [0117]. A POSITA would have understood that Thompson's "control program" is used to "accept[] payment from a customer," as Thompson explains that the "control program and electronics 2300 can then present a payment screen to facilitate the purchase of the video content," thus a POSITA would have understood that Thompson's control device performs the same functions as the "transaction module" claimed in the '783 Patent. [Ex1005] at [0117]; Ex[1003], ¶ 91.

6. 1[e]: an SD card writer for writing data to an unsecure user area of the SD card and a protected secure area of the SD card; and

Thompson and Kasahara, alone or in combination, teach this limitation. Ex[1003], ¶ 92.

Thompson discloses programming circuits to program encrypted video content and associated keys into a solid-state memory device. Ex[1005] at [0105]. Thompson goes on to explain that, "[a]s the data is transferred to the device, it is encrypted by the encryption engine and stored in an encrypted format in a restricted region of the memory device." *Id.* at [0112]. Thompson further states that the content "is encrypted and decrypted using a secure key (CEK) contained within the memory device and not accessible outside of it." *Id.* at [0111]. Thompson's memory device also contains a user area that is not secured for storing certain data including, for example, "content identification" information "assigned by the kiosk when loading the content" that is subsequently used for user authentication. *Id.* at [0113]. Thompson thus discloses writing encrypted content to a protected secure area of the

SD card and an unsecure region that may contain data like content identification information. Ex[1003], ¶¶ 93, 94.

A POSITA reading Thompson would have understood that Thompson's "programing circuits" function as a writer for writing data into an unsecure user area and a protected secure area. Ex[1003], ¶ 94.

To the extent that Thompson's "removable solid-state memory device" does not disclose an "SD card," it would have been obvious to a POSITA to modify Thompson's kiosk system to use an SD card as an output medium. Thompson explicitly states that a "kiosk can be altered to use other types of devices," which can be "any type of media." Ex[1005] at [0033], [0037]. And, as the '783 Patent concedes, SD cards were already well-known and adapted for this use case. Ex[1001] at 2:8-12.

Kasahara also discloses this limitation. Ex[1003], ¶ 92. Kasahara differentiates between writing to secure and unsecure areas of an SD card. Specifically, Kasahara's SD card 20 includes a user area and a protection area. Ex[1007] at [0061]. Kasahara discloses writing content in the user area of the SD card and key data in the protected area of the SD card 20. *Id.* ("The handheld terminal 30 stores the encrypted content data Enc (Kcib:Ci) in the user area of the SD card 20. The SDSD content key data Kcib is encrypted with the SDSD user key data Kub to be an Enc (Kub:Kcib**)** and then also stored in the user area of the SD card 20. The SDSD user key data Kub itself is stored in the protection area of the SDSD card 20 in such a way that the SDSD user key data Kub may be inaccessible from outside.").

A POSITA reading Kasahara would have understood that Kasahara's system includes an SD card writer for writing data into an unsecure user area and a protected secure area, as Kasahara explicitly discloses writing content to a secure area (Ex[1007] at [0061]) and an unsecure area (*id.*) of an SD card. Ex[1003], ¶ 97.

7. 1[f]: a media file processing module for preparing the plurality of media files and the corresponding metadata files to be written to the SD card in cooperation with the SD card writer,

The Thompson-Kasahara combination teaches this limitation. Ex[1003], ¶ 98. As explained by the '783 Patent, "[t]he media file processing module 135 processes media files in preparation for writing the files to SD cards 140. The media file processing module 135 receives the requested media files from the store server 120 via the server interaction module 133. The media file processing module 135 then queues the media file for download to the SD card 140." Ex[1001] at 4:42-47.

Thompson's kiosk comprises control program and electronics 2300 which constitutes a media file processing module. Like the "media file processing module" disclosed by the '783 Patent, Thompson's control program and electronics 2300 "retrieve[s] the selected video content from the video content servers, and "initiate[s] the media programming process." Ex[1005] at [0117]-[0118]. Thus, because Thompson's kiosk discloses a control program which provides the same functionality as the '783 Patent's "media file processing module", a POSITA would have understood that Thompson discloses this limitation. Ex[1003], ¶¶ 99, 100.

Kasahara likewise discloses a system of controlled content retrieval, encryption, and storage, which involves the process of "download[ing] from a content-data download site provided by the server 50 content data[.]" Ex[1007] at [0033]. Thus, because Kasahara's system provides the same functionality as the '783 Patent's "media file processing module", a POSITA would have understood that Kasahara likewise discloses a "media file processing module" of the type claimed by the '783 Patent. Ex[1003], ¶ 101.

8. 1[g]: wherein space is pre-allocated on the SD card for writing an encrypted playable content portion of each media file to an unsecure area of the SD card, and

The Thompson-Kasahara combination teaches this limitation. Ex[1003], ¶ 102. The control program and electronics 2300 of Thompson optimizes the use of available memory space when programming the media content onto the SD card. Ex[1005] at [0120] ("The control program and electronics 2300 can also contain sales delivery optimization algorithms to calculate available space on a to-be- (or already-) programmed memory device and can provide flexible on-the-fly-delivery of video content based on that calculation."). Thompson's system is also designed to analyze available space before writing. *Id.* at [0121] ("The control program and electronics 2300 can also determine that programming a memory device with the selected video content will result in unused space in the memory device."). A POSITA reading Thompson would therefore have found pre-allocating space on the memory device for encrypted playable content to be inherently taught in Thompson or obvious, because Thompson's discloses optimization and memory scanning functionality would have necessarily allocated the optimal space for the encrypted content that was to be programmed and, in any event, would allow for the pre-allocation, as a design choice (e.g., the designer would know that encrypted content was to be written/programmed, such that space would need to be allocated before the writing operation). Ex[1003], ¶ 103.

Further, Thompson discloses writing an encrypted playable content portion of each media file to an unsecure portion of a memory device. Ex[1003], ¶ 104. Thompson states that "as shown in FIG. 22a, it is preferred that the encrypted video content 2272 be programmed in the removable memory device 2200 using a fast programming connection because of the relatively-large file size of the encrypted video content 2272." Ex[1005] at [0105]. A POSTIA would have understood that this "encrypted video content" is stored in the "unsecure area" of the memory device, as the secure area is reserved for the encrypted key, as shown in the figure below. Ex[1003], ¶ 104; Ex[1005] at [0106] ("The programming circuits 2260 also program the associated content encryption key ("CEK")").

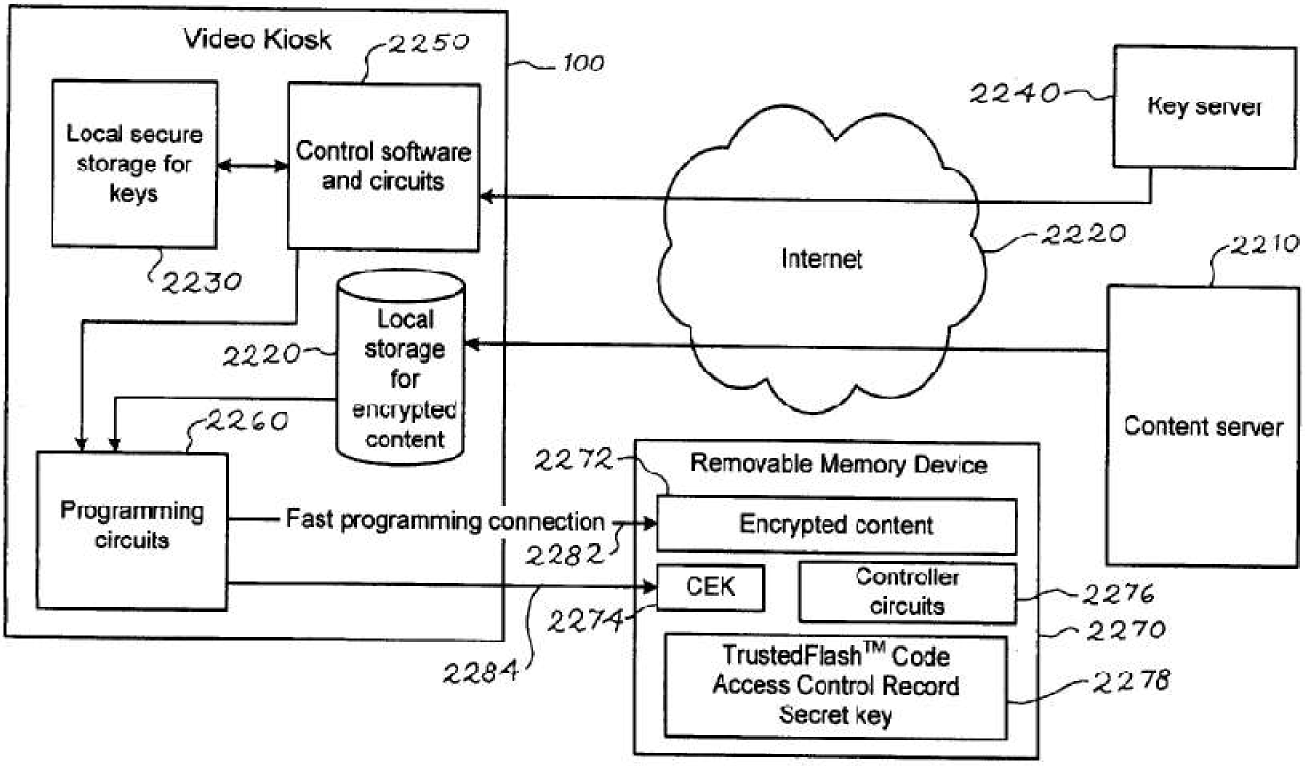


Fig. 22 a

Further, as discussed above, Kasahara expressly distinguishes between a user area ("unsecure area") and a protection area of the SD card. Kasahara discloses that, while the "SDSD content key data Kub" used to encrypt the content is stored in the protection area ("secure area"), the encrypted content is stored in the user area ("unsecure area"). Ex[1007] at [0061]. Thus, in view of Thompson and Kasahara, the benefits of storing video content data to the unsecure portion of an SD card, while storing relatively small-file size data, such as keys, to the secure portion of an SD card, would have been obvious to a POSITA. Ex[1003], ¶ 106.

9. 1[h]: wherein, except for a user key, data to be written to the unsecure area of the SD card is queued for writing in advance of data to be written to a secure area of the SD card, such that the data to be written to the unsecure area is written in time before the data to be written to the secure area is written, and

The Thompson-Kasahara combination teaches this limitation. Ex[1003], ¶ 107.

The '783 Patent explains the benefit of writing media content to an unsecure area of the SD card before writing data to a secure area of the SD card was to avoid "delay" as writing to a secure portion of the SD card is slower than writing to the unsecured portion. Ex[1001] at 9:57-64.

Thompson discloses writing content data to an unsecure portion of a memory device (Ex[1005] at [0105]) and encrypted content keys to a secure portion of a memory device (Ex[1005] at [0106]). Further, Thompson discloses that writing to the secure portion of the memory device could cause delays. Ex[1005] at [0106] ("Since the CEK 2272 comprises only a relatively limited amount of data, the delay caused by using a secure transfer mechanism should not be that noticeable to the user.").

To the extent that Thompson does not disclose writing media content to the unsecure area of an SD card before writing data to the secure area of an SD card, it would have been obvious to a POSITA to do so, given the known delays caused by writing to a secure portion of an SD card, as discussed by Thompson. Ex[1003], ¶ 109.

Further, to the extent that Thompson's "removable solid-state memory device" does not disclose an "SD card," it would have been obvious to a POSITA to modify Thompson's kiosk system to use an SD card as an output medium, as explained above. Again, Thompson explicitly states that a "kiosk can be altered to use other types of devices," which can be "any type of media." Ex[1005] at [0033], [0037].

Kasahara discloses the process of storing encrypted content data in the user area ("unsecure area") of the SD card 20 before key data is written to the secure area. Ex[1007] at [0033]. As Kasahara explains, after downloading this content to an unsecure area, "[a]t this point, the user does not have the content key data Kcis". Ex[1006] at [0033]. Only later does Kasahara disclose saving content key data in the secure area of the SD card. Ex[1007] at [0061] ("The SDSD content key data

Kcib is encrypted with the SDSD user key data Kub and then also stored in the user area of the SD card 20"). Then the SDSD user key data Kub is stored in the protection area ("secure area") of the SD card 20. *Id.*

10. 1[i]: wherein the playable media files are encrypted by a content key that is encrypted by the user key.

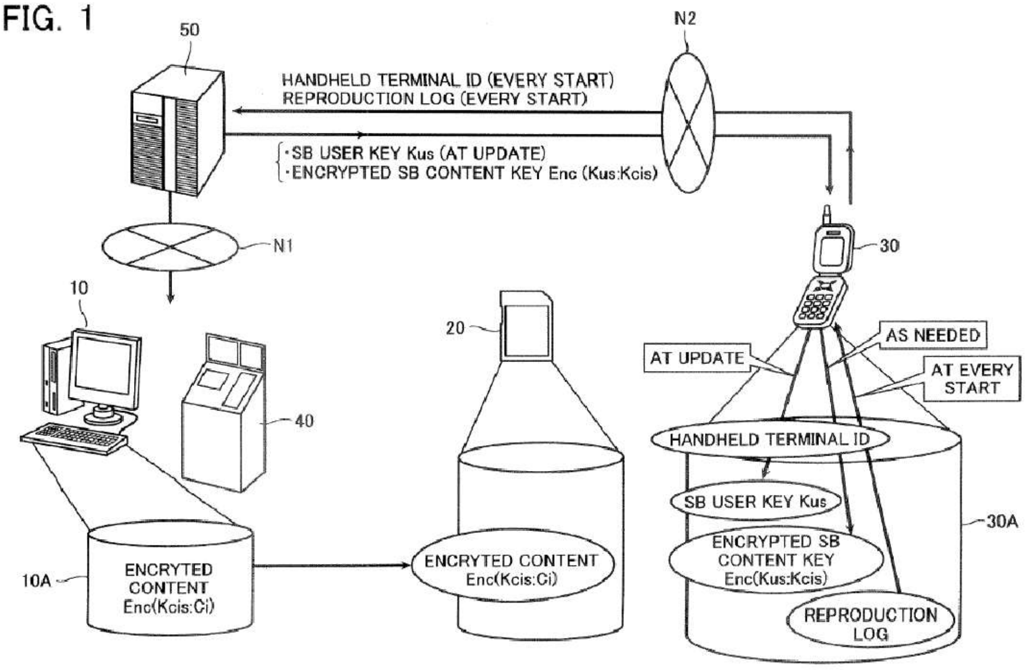
The Thompson-Kasahara combination teaches this limitation. Ex[1003], ¶ 111.

As the '783 Patent explains, "[t]he user key is encrypted with the SD cards 'media key' in an operation which can only be performed on the SD card through special interactions with the SD card's secured area." Ex[1001] at 7:50-53.

Thompson discloses that "video content is encrypted using a secure key (CEK) contained within the memory device and not accessible outside of it." Ex[1005] at [0111].

As discussed above, Kasahara discloses that the content key data is encrypted with user key data. Ex[1007] at [0061] ("The SDSD content key data Kcib is encrypted with the SDSD user key data Kub and then also stored in the user area of the SD card 20"). Kasahara further discloses that the content data itself (i.e., the "playable media files") are "encrypted with the content key data." Ex[1007] at [0009]. Thus, a POSITA would have understood that Kasahara discloses playable media files encrypted by a content key that is encrypted by the user key. Ex[1003], ¶¶ 113, 114.

FIG. 1


50
N2
HANDHELD TERMINAL ID (EVERY START)
REPRODUCTION LOG (EVERY START)
·SB USER KEY Kus (AT UPDATE)
·ENCRYPTED SB CONTENT KEY Enc (Kus:Kcis)
N1
10
40
20
30
AT UPDATE
AS NEEDED
AT EVERY START
HANDHELD TERMINAL ID
SB USER KEY Kus
ENCRYPTED SB CONTENT KEY Enc(Kus:Kcis)
REPRODUCTION LOG
30A
10A
ENCRYTED CONTENT Enc(Kcis:Ci)
ENCRYTED CONTENT Enc(Kcis:Ci)

It would have been obvious to a POSITA to combine Kasahara's encryption method (using a user key to encrypt a content key which encrypts content data) with the system disclosed by Thompson. Ex[1003], ¶ 114.

For the above reasons, Thompson in combination with Kasahara disclose all limitations of Claim 1. Ex[1003], 115.

C. Dependent Claim 2

1. 2[pre]: The kiosk of claim 1,

As explained above for Claim 1, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 1.

2. 2[a]: further comprising a preview module for playing a preview of content of selected [sic] by the customer through the kiosk while the SD card writer writes the plurality of media files to the SD card, wherein the preview of content selected by the customer includes content from the plurality of media files being written to the SD card.

Thompson discloses this limitation. Ex[1003], ¶ 117.

As explained by the '783 Patent, the "preview module" "manages the playback of preview of media files that are available for purchase. The preview module 137 can operate in parallel with the SD card writer". Ex[1001] at 5:1-6.

Thompson discloses a "control program and electronics" that "display movie trailers or advertisements on the video touch screen. . . ." Ex[1005] at [0115]. Thompson further states that these previews can be viewed while the SD card writer writes the plurality of media files to the SD card. Specifically, Thompson states that, "[a]s the memory device is being programmed, the control program and electronics 2300 can display trailers of related video titles, advertisements, options to search and purchase other video content, and options to provide other services." *Id.* at [0117].

Thus, a POSITA would have understood that Thompson's control program performs the same functions as the "preview module" claimed in the '783 Patent. Ex[1003], ¶ 119.

D. Dependent Claim 3

1. 3[pre]: The kiosk of claim 1,

As explained above for Claim 1, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 1.

2. 3[a]: further comprising a firmware update module for transferring a firmware update to the SD card.

Thompson discloses this limitation. Ex[1003], ¶ 122.

The '783 Patent explains that "[t]he firmware update module 138 receives firmware updates (e.g., firmware software updates). . . for use in updating firmware on the playback devices that use the SD cards 140." '783 Patent at 5:17-21.

Thompson discloses a video kiosk that can update firmware of a memory device. Ex[1005] at [0131]. Specifically, Thompson discloses that when the video kiosk 100 contacts the memory device 2600, firmware stored in the "memory array" 2610 (contained within the Memory Device) "can be updated". *Id.* Thus, because Thompson discloses a kiosk that provides the functionality of downloading firmware updates onto a flash card, a POSITA would have understood that Thompson's kiosk necessarily included the type of "firmware update module" claimed in the '783 Patent.

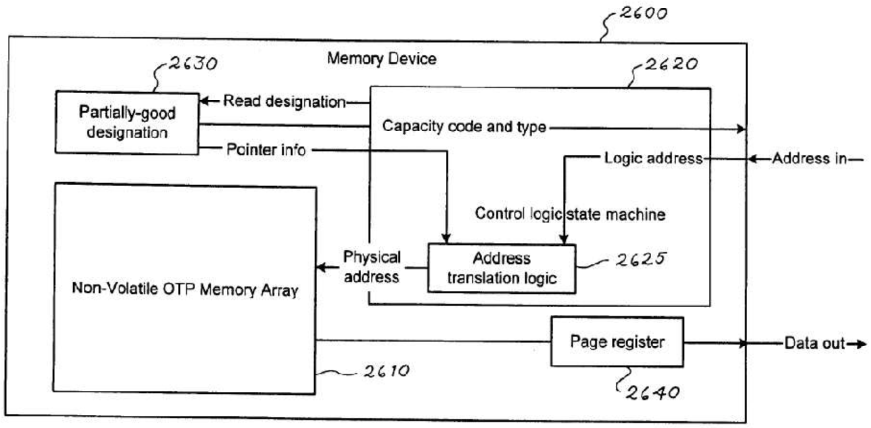


Fig. 26

To the extent that Thompson's "memory device" does not disclose an "SD card," it would have been obvious to a POSITA to modify Thompson's kiosk system to use an SD card as an output medium, as explained above. Again, Thompson explicitly states that a "kiosk can be altered to use other types of devices," which can be "any type of media." Ex[1005] at [0033], [0037].

E. Dependent Claim 5

1. 5[pre]: The kiosk of claim 1,

As explained above for Claim 1, Thompson and Kasahara, alone or in combination, disclose each and every limitation of Claim 1.

2. 5[a]: further comprising a customer attraction module for playing segments from media files currently available for download from the kiosk while the kiosk is not used for purchase of a media file.

Thompson discloses this limitation. Ex[1003], ¶ 127.

As the ’783 Patent explains that “The customer attraction module 139 plays preview, such as movie previews, short segments of media files, and/or advertisements to download particular media files, in order to entice customers to make a purchase.” ’783 Patent at 5:45-48.

Thompson’s kiosk comprises control program and electronics 2300, storage devices 2310 and a video touch screen 140. Ex[1005] at [0114]. Thompson discloses that the control program and electronics 2300 “display movie trailers or advertisements on the video touchscreen 140 while waiting for an active user.” *Id.* at [0115]. The trailers or advertisements are “stored in the storage device 2310” of the kiosk. *Id.* The control program and electronics 2300, storage devices 2310 and video touch screen 140 constitute a customer attraction module for playing media files available on the kiosk when the kiosk is not used for an active purchase. Ex[1003], ¶ 129.

F. Dependent Claim 6

1. 6[pre]: The kiosk of claim 1,

As explained above for Claim 1, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 1.

2. 6[a]: further comprising a USB port to allow connection of the SD card with a USB adapter to the kiosk.

Thompson discloses that the kiosk "comprises a plurality of ports 180 to connect a PC-based control system of the video kiosk 100 to external … peripherals" and the ports 180 specifically include "a USB port." Ex[1005] at [0042]. Thompson thus explicitly discloses that its kiosk comprises a USB port provided for peripheral connectivity. A POSITA would have recognized that a common use for a USB port is to interface with storage devices, including an SD card via a USB adapter. Ex[1003], ¶¶ 133, 134. At the time of the '783 Patent and Thompson's disclosure, USB-to-SD adapters were widely available and commonly used to allow electronic devices with USB ports to access SD cards. *Id.* Thus, this claim would have been obvious in view of Thompson. Ex[1003], ¶ 135.

G. Independent Claim 7

1. 7[pre]: A method of quickly and securely transferring media files from a kiosk to a secure digital (SD) card, the method comprising:

To the extent the preamble is limiting, for the same reasons described for Claim 1[Preamble] in Ground 1, Thompson and Kasahara, alone or in combination, teach a method of quickly and securely transferring media files from a kiosk to a secure digital (SD) card. Ex[1003], ¶ 136.

2. 7[a]: identifying a media file for download to the SD card;

Thompson discloses this limitation. Ex[1003], ¶ 137. Thompson discloses requesting media files and corresponding metadata file from a server communicatively coupled to the video kiosk. Ex[1005] at [0042] ("the video kiosk 100 can connect to an external network location to retrieve video content on-the-fly when requested by a user or to retrieve video content for local storage on one or more mass storage devices in the video kiosk 100.)"; *id.* at [0101] ("if the local mass storage device 2200 does not have a video title desired by a user, the video kiosk 100 can contact the content server 2210 on-the-fly to download the desired video content. Preferably, the connection between the video kiosk 100 and the content server 2210 is suitably fast"). Thus, a POSITA would have understood that Thompson discloses identifying a media file for download to the SD card. Ex[1003], ¶ 138.

3. 7[b]: pre-allocating space on the SD card for a playable content portion of the media file, wherein the playable content portion of the media file is encrypted by a content key that is encrypted by a user key;

The Thompson-Kasahara combination teaches this limitation. Ex[1003], ¶ 139. The control program and electronics 2300 of Thompson optimizes the use of available memory space when programming the media content onto the SD card. Ex[1005] at [0120] ("The control program and electronics 2300 can also contain sales delivery optimization algorithms to calculate available space on a to-be- (or already-) programmed memory device and can provide flexible on-the-fly-delivery of video content based on that calculation."). Thompson's system is also designed to analyze available space before writing. *Id.* at [0121] ("The control program and electronics 2300 can also determine that programming a memory device with the selected video content will result in unused space in the memory device."). A POSITA reading Thompson would therefore have found pre-allocating space on the memory device for encrypted playable content to be inherently taught in Thompson or obvious, because Thompson's discloses optimization and memory scanning functionality would have necessarily allocated the optimal space for the encrypted content that was to be programmed and, in any event, would allow for the pre-allocation, as a design choice (e.g., the designer would know that encrypted content was to be written/programmed, such that space would need to be allocated before the writing operation). Ex[1003], ¶ 103.

Further, Thompson discloses writing an encrypted playable content portion of each media file to an unsecure portion of a memory device. Ex[1003], ¶ 104. Thompson states that "as shown in FIG. 22a, it is preferred that the encrypted video content 2272 be programmed in the removable memory device 2200 using a fast programming connection because of the relatively-large file size of the encrypted video content 2272." Ex[1005] at [0105]. A POSTIA would have understood that this "encrypted video content" is stored in the "unsecure area" of the memory device, as the secure area is reserved for the encrypted key, as shown in the figure below. Ex[1003], ¶ 104; Ex[1005] at [0106] ("The programming circuits 2260 also program the associated content encryption key ("CEK")").

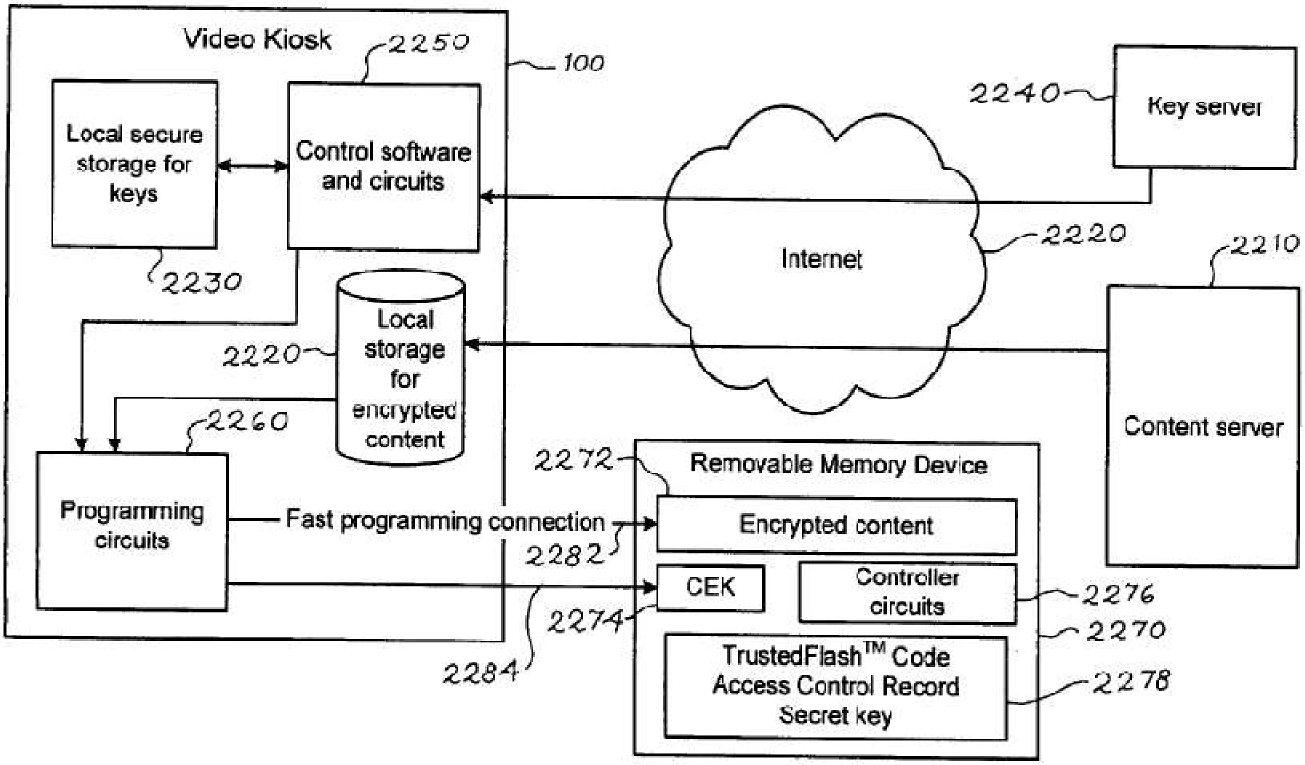


Fig. 22 a

Further, as discussed above, Kasahara expressly distinguishes between a user area ("unsecure area") and a protection area of the SD card. Kasahara discloses that while the "SDSD content key data Kub" used to encrypt the content is stored in the protection area ("secure area"), the encrypted content is stored in the user area ("unsecure area"). Ex[1007] at [0061]. Thus, in view of Thompson and Kasahara, the benefits of storing video content data to the unsecure portion of an SD card, while storing relatively small-file size data, such as keys, to the secure portion of an SD card would have been obvious to a POSITA. Ex[1003], ¶ 106.

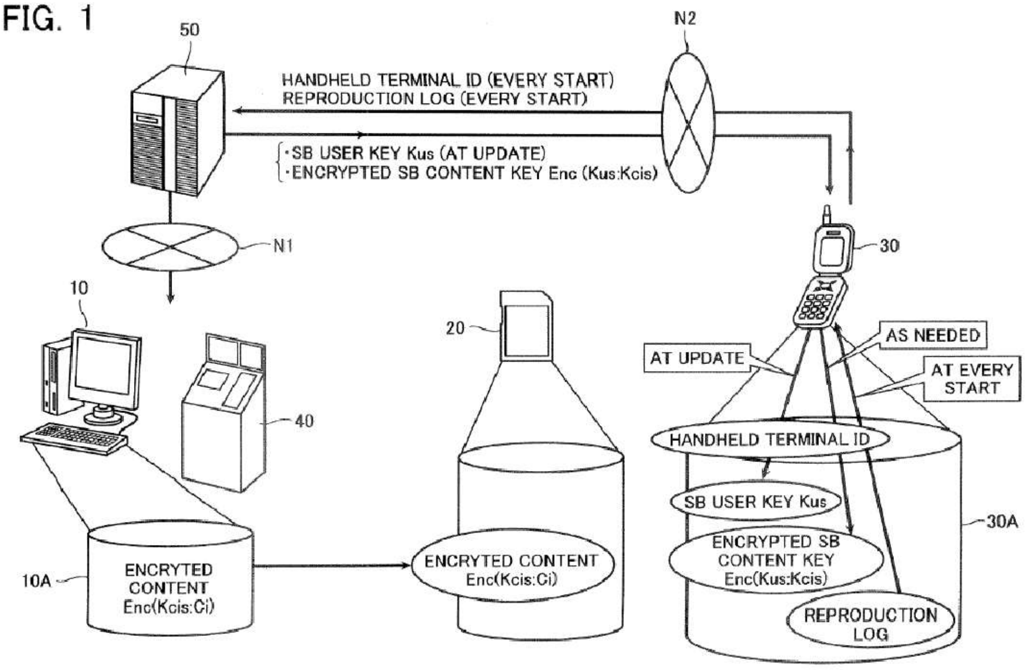
Further, the Thompson-Kasahara system discloses that the playable content portion of the media file is encrypted by a content key that is encrypted by a user key. Ex[1003], ¶ 111.

As the '783 Patent explains, "[t]he user key is encrypted with the SD card's "media key" in an operation which can only be performed on the SD card through special interactions with the SD card's secured area." Ex[1001] at 7:50-53.

Thompson discloses "video content is encrypted using a secure key (CEK) contained within the memory device and not accessible outside of it." Ex[1005] at [0111].

As discussed above, Kasahara discloses that the content key data is encrypted with user key data. Ex[1007] at [0061] ("The SDSD content key data Kcib is encrypted with the SDSD user key data Kub and then also stored in the user area of the SD card 20"). Kasahara further discloses that the content data itself (i.e., the "playable media files") are "encrypted with the content key data." Ex[1007] at [0009]. Thus, a POSITA would have understood that Kasahara discloses playable media files encrypted by a content key that is encrypted by the user key. Ex[1003], ¶¶ 113, 114.

FIG. 1


50
N2
HANDHELD TERMINAL ID (EVERY START)
REPRODUCTION LOG (EVERY START)
·SB USER KEY Kus (AT UPDATE)
·ENCRYPTED SB CONTENT KEY Enc (Kus:Kcis)
N1
30
10
20
AT UPDATE
AS NEEDED
AT EVERY START
40
HANDHELD TERMINAL ID
SB USER KEY Kus
30A
ENCRYPTED SB CONTENT KEY Enc(Kus:Kcis)
10A
ENCRYTED CONTENT Enc(Kcis:Ci)
ENCRYTED CONTENT Enc(Kcis:Ci)
REPRODUCTION LOG

It would have been obvious to a POSITA to combine Kasahara's encryption method (using a user key to encrypt a content key which encrypts content data) with the system disclosed by Thompson. Ex[1003], ¶ 114.

4. 7[c]: writing all directory blocks of the playable content portion of the media file together and, thereafter in time, writing all data blocks sequentially of the playable content portion of the media file; and

Thompson teaches this limitation. Ex[1003], ¶ 140.

Thompson discloses pre-allocating space on the SD card for media file storage before writing, ensuring efficient content transfer. Ex[1005] at [0105] ("The video kiosk 100 also comprises programming circuits 2260 to program encrypted video content and associated keys into a removable solid-state memory device 2270.").

Further, it would have been obvious to a POSITA to write directory blocks of a media file prior to writing data blocks. Ex[1003], ¶ 142. A POSITA would recognize that directory blocks store metadata such as file names, sizes and locations of data blocks, and data blocks store the actual media content. *Id.* Writing directory blocks first followed by sequential data blocks is a well-known technique in file system design, which ensures that the file system can properly reference the data before it is fully written. *Id.* Modern file systems inherently use this approach for storage on removable media. *Id.*

5. 7[d]: writing all data that is to be written to an unsecure area of the SD card, including the encrypted playable content, prior in time to writing any data to a secure area of the SD card, except for the user key.

The Thompson-Kasahara combination teaches this limitation. Ex[1003], ¶ 143.

The '783 Patent explains the benefit of writing media content to an unsecure area of the SD card before writing data to a secure area of the SD card was to avoid "delay" as writing to a secure portion of the SD card is slower than writing to the unsecured portion. Ex[1001] at 9:57-64.

Thompson discloses writing content data to an unsecure portion of a memory device (Ex[1005] at [0105]) and encrypted content keys to a secure portion of a memory device (Ex[1005] at [0106]). Further, Thompson discloses that writing to the secure portion of the memory device could cause delays. Ex[1005] at [0106] ("Since the CEK 2272 comprises only a relatively limited amount of data, the delay caused by using a secure transfer mechanism should not be that noticeable to the user.").

To the extent that Thompson does not disclose writing media content to the unsecure area of an SD card before writing data to the secure area of an SD card, it would have been obvious to a POSITA to do so, given the known delays caused by writing to a secure portion of an SD card, as discussed by Thompson. Ex[1003], ¶ 109.

Further, to the extent that Thompson's "removable solid-state memory device" does not disclose an "SD card," it would have been obvious to a POSITA to modify Thompson's kiosk system to use an SD card as an output medium, as explained above. Again, Thompson explicitly states that a "kiosk can be altered to use other types of devices," which can be "any type of media." Ex[1005] at [0033], [0037].

Kasahara also renders this limitation obvious. Ex[1003] at ¶ 143. Kasahara discloses the process of storing encrypted content data in the user area ("unsecure area") of the SD card 20. Ex[1007] at [0033]. As Kasahara explains, after downloading this content to an unsecure area "[a]t this point, the user does not have the content key data Kcis." Ex[1006] at [0033]. Only later does Kasahara disclose saving content key data in the secure area of the SD card. Ex[1007] at [0061] ("The SDSD content key data Kcib is encrypted with the SDSD user key data Kub and then also stored in the user area of the SD card 20"). Then the SDSD user key data Kub is stored in the protection area ("secure area") of the SD card 20. *Id.*

H. Dependent Claim 8

1. 8[pre]: The method of claim 7,

As explained above for Claim 7, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 7.

2. 8[a]: wherein, except for a user key, data is only written to the secure area of the SD card if a transaction for the media file successfully completes.

Thompson discloses this limitation. Ex[1003], ¶ 146. The '783 Patent explains that the purpose for writing data to the secure area of the SD card is to permit the user to decrypt and therefore view the downloaded media file.

Specifically, the ’783 Patent states that one of the reasons that content key data is written to the secure area of an SD card *after* the transfer of the media file successfully completes is so “if there is any kind of problem with the payment for the transaction through the transaction module 134 or with the transfer of the media file to the SD card 140, the kiosk 130 can abort the transfer without writing the data to the secure area 142 of the SD card 140. As a result, no matter what portion of the media file has been downloaded to the SD card 140 prior to the transfer process being aborted, the customer will not be able to playback any playable content that was downloaded to the SD card.” Ex[1001] at 9:65-10:7.

Thompson likewise discloses that the programming process will only initiate after the user has confirmed the purchase. Ex[1005] at [0117] (noting that data is only written to the memory device *after* the user confirms the purchase).

I. Dependent Claim 10

1. 10[pre]: The method of claim 7, further comprising:

As explained above for Claim 7, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 7.

2. 10[a]: writing the user key to the secure area of the SD card prior in time to writing all data to the unsecure area of the SD card; and

Thompson and Kasahara, alone or in combination, teach this limitation. Ex[1003], ¶ 151. Specifically, Kasahara discloses that the SDSD user key data Kub ("user key") is written to the protection area ("secure area") of the SD card 20 before completion of initiation of the data transfer. Ex[1007] at [0066]. After initiation, the SDSD content key data Kcib is encrypted with the user key and both are saved in the user area ("unsecure area") of the SD card 20. *Id.* at [0067].

It would have been obvious to a POSITA to combine Kasahara's encryption method (using a user key to encrypt a content key which encrypts content data), and writing the user key to the secure area of the SD card prior in time to writing all data to the unsecure area, with the system disclosed by Thompson. Ex[1003], ¶ 152.

3. 10[b]: writing other data to the secure area of the SD card after in time writing all data to the unsecure area of the SD card.

The Thompson-Kasahara combination discloses this limitation. Ex[1003], ¶ 153.

The '783 Patent explains the benefit of writing media content to an unsecure area of the SD card before writing data to a secure area of the SD card was to avoid "delay" as writing to a secure portion of the SD card is slower than writing to the unsecured portion. Ex[1001] at 9:57-64.

Thompson discloses writing content data to an unsecure portion of a memory device (Ex[1005] at [0105]) and encrypted content keys to a secure portion of a memory device (Ex[1005] at [0106]). Further, Thompson discloses that writing to the secure portion of the memory device could cause delays. Ex[1005] at [0106] ("Since the CEK 2272 comprises only a relatively limited amount of data, the delay caused by using a secure transfer mechanism should not be that noticeable to the user.").

To the extent that Thompson does not disclose writing media content to the unsecure area of an SD card before writing data to the secure area of an SD card, it would have been obvious to a POSITA to do so, given the known delays caused by writing to a secure portion of an SD card, as discussed by Thompson. Ex[1003], ¶ 109.

Further, to the extent that Thompson's "removable solid-state memory device" does not disclose an "SD card," it would have been obvious to a POSITA to modify Thompson's kiosk system to use an SD card as an output medium. Thompson explicitly states that a "kiosk can be altered to use other types of devices," which can be "any type of media." Ex[1005] at [0033], [0037].

Kasahara discloses the process of storing encrypted content data in the user area ("unsecure area") of the SD card 20. Ex[1007] at [0033]. As Kasahara explains, after downloading this content to an unsecure area "[a]t this point, the user does not have the content key data Kcis." Ex[1006] at [0033]. Only later does Kasahara disclose saving content key data in the secure area of the SD card. Ex[1007] at

[0061] ("The SDSD content key data Kcib is encrypted with the SDSD user key data Kub and then also stored in the user area of the SD card 20"). Then the SDSD user key data Kub is stored in the protection area ("secure area") of the SD card 20. *Id.*

J. Dependent Claim 11

1. 11[pre]: The method of claim 7,

As explained above for Claim 7, Thompson and Kasahara, alone or in combination, disclose each and every limitation of Claim 7.

2. 11[a]: where the directory blocks are optionally written at once.

Thompson discloses this limitation. Ex[1003], ¶ 156. Thompson discloses that the data to be written may be divided into many portions, whereafter these portions are stored in sub-arrays, thus allowing for parallel writing of all information so stored. Ex[1005] at [0072]. Further, it would have been obvious to a POSITA to write directory blocks of a media file all at once because writing directory blocks all at once ensures that file system metadata remains contiguous and consistent, reducing fragmentation and increasing read/write performance. Ex[1003], ¶ 157.

K. Independent Claim 12

1. 12[pre]: A non-transitory computer readable storage medium storing instructions thereon, the instructions when executed cause at least one processor to:

To the extent the preamble is a limitation, Thompson discloses a computable readable storage medium that stores computer-readable program code. Ex[1003],

¶ 159. Specifically, Thompson discloses that the video kiosk comprises circuitry to control its operation, and the circuitry can comprise a computer-readable medium that stores computer-readable code. Ex[1005] at [0043].

2. 12[a]: identify a media file for download to an SD card;

For the same reasons described for Claim 1[b] and Claim 7[a] in Ground 1, Thompson teaches this limitation.

3. 12[b]: pre-allocate space on the SD card for a playable content portion of the media file, wherein the playable content portion of the media file is encrypted by a content key that is encrypted by a user key;

For the same reasons described for Claim 1[g] and Claim 7[b] in Ground 1, Thompson teaches this limitation.

4. 12[c]: write all directory blocks together of the playable content portion of the media file and, thereafter in time, write all data blocks sequentially of the playable content portion of the media file; and

For the same reasons described for Claim 7[c] in Ground 1, Thompson and Kasahara, either alone or in combination, teach this limitation.

5. 12[d]: write all data that is to be written to an unsecure area of the SD card, including the encrypted playable content, prior in time to writing any data to a secure area of the SD card, except for the user key.

For the same reasons described for Claim 1[h] in Ground 1, Thompson teaches this limitation.

L. Dependent Claim 13

1. 13[pre]: The computer readable storage medium of claim 12,

As explained above for Claim 12, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 12.

2. 13[a]: wherein, except for a user key, data is only written to the secure area of the SD card if a transaction for the media file successfully completes.

For the same reasons described for Claim 8[a] in Ground 1, Thompson teaches this limitation.

M. Dependent Claim 15

1. 15[pre]: The computer readable storage medium of claim 12, further comprising instructions that when executed cause the at least one processor to:

As explained above for Claim 12, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 12.

2. 15[a]: write the user key to the secure area of the SD card prior in time to a write of all data to the unsecure area of the SD card; and

For the same reasons described for Claim 10[a] in Ground 1, Thompson and Kasahara, either alone or in combination, teach this limitation.

3. 15[b]: write other data to the secure area of the SD card after in time a write of all data to the unsecure area of the SD card.

For the same reasons described for Claim 10[b] in Ground 1, Kasahara teaches this limitation.

N. Dependent Claim 16

1. 16[pre]: The computer readable storage medium of claim 12,

As explained above for Claim 12, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 12.

2. 16[a]: where the directory blocks are optionally written at once.

For the same reasons described for Claim 11[a] in Ground 1, Thompson teaches this limitation.

XIII. GROUND 2: CLAIM 4 IS OBVIOUS OVER THOMPSON AND KASAHARA IN VIEW OF WAGNER

A. Motivation to Combine

A POSITA would have been motivated to combine Wagner (Ex[1006]) with Thompson (Ex[1005]) and Kasahara (Ex[1007]) because all three references are directed toward improving the efficiency, security, and reliability of digital media transfer and distribution. Each reference addresses key aspects of content delivery through kiosks or similar systems that store and transmit digital media files to removable storage devices. Ex[1003] at ¶¶ 175, 176. A POSITA would have recognized that integrating Wagner's techniques into the combined Thompson-Kasahara system would lead to a predictable and desirable improvement in digital media distribution. Ex[1003] at ¶ 177. Wagner, like Thompson and Kasahara, is in the same field of endeavor of secure content delivery via automated kiosks and other media distribution terminals. Ex[1003] at ¶ 176. Wagner specifically teaches advancements in content management that enhance the protection of the media content. Ex[1006] at [0055]. Given that Wagner's methods align with the objectives of Thompson and Kasahara, a POSITA would have understood that incorporating these features would have improved the overall performance of a kiosk-based content delivery system. Ex[1003] at ¶ 177.

B. Dependent Claim 4

1. 4[pre]: The kiosk of claim 1,

As explained above for Claim 1 in Ground 1, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 1.

2. 4[a]: further comprising a software player update module for transferring a software player update to the SD card.

Wagner discloses this limitation. Ex[1003], ¶ 179.

The specification of the '783 Patent does not mention a "software player update module", however it explains that "[t]he firmware update module 138 receives firmware updates (e.g., firmware software updates). . . for use in updating firmware on the playback devices that use the SD cards 140." '783 Patent at 5:17-21.

Wagner discloses a kiosk that downloads required software onto a flash card. Ex[1006] at [0044]. Wagner further describes a mechanism for updating at least the programming of RAM memory 230, which can be used to update the functionality of an adapter or to add or remove digital rights management functionality. *Id.* at [0072]. Thus, because Wagner discloses a kiosk that provides the functionality of downloading software onto a flash card, a POSITA would have understood that Wagner necessarily included the type of "software player update module" claimed in the '783 Patent.

The Thompson-Kasahara system already provides a secure and efficient method for transferring encrypted media content to SD cards using a kiosk. However, it does not explicitly disclose the ability to update software players on the SD card. Wagner's teaching of software updates on flash storage would have been a natural extension of the Thompson-Kasahara system's functionality, as it would allow kiosks to maintain compatibility with evolving content protection and playback requirements. Ex[1003], ¶ 175. A POSITA would have recognized that integrating Wagner's software update module with Thompson-Kasahara would not require substantial modifications to the existing system. Ex[1003], ¶ 177. Wagner describes a standard approach to software updates using flash memory storage, which aligns well with the secure media distribution framework of the Thompson-Kasahara kiosk. Ex[1003], ¶ 177.

XIV. GROUND 3: CLAIMS 9 AND 14 ARE OBVIOUS OVER THOMPSON AND KASAHARA IN VIEW OF ISHIHARA

A. Motivation to Combine

A POSITA would have been motivated to combine Ishihara (Ex[1009]) with Thompson (Ex[1005]) and Kasahara (Ex[1007]) because all three references address key challenges in secure digital content distribution. Ex[1003], ¶ 184. Ishihara discloses a content protection mechanism specifically tailored for digital media, including encryption techniques, key management, and authentication protocols that prevent unauthorized access and copying. Ex[1009] at 23. Thompson teaches a kiosk-based system for transferring digital content to portable storage media (Ex[1005] at [0032]), while Kasahara provides an encryption and secure content management framework for content delivery to SD cards Ex[1007] at [0061]. The combination of Ishihara's encryption methodologies with Thompson and Kasahara's content delivery model would have been an obvious improvement, ensuring enhanced data protection and controlled access to digital content. Ex[1003], ¶ 186.

A POSITA would have understood that integrating Ishihara's security framework into the Thompson-Kasahara system would provide multiple advantages.

Ex[1003], ¶ 185. Ishihara describes a hierarchical encryption system where a memory public key is used to encrypt licenses, and a memory private key is required for decryption before playback. Ex[1009] at 23, 26. This model ensures that only authorized users with valid licenses can access digital content, preventing unauthorized duplication. *Id.* Applying this encryption system to Thompson's kiosk model would have further strengthened its security, ensuring that purchased or rented digital media files could not be accessed without authentication. Kasahara's structured content encryption methods already complement Thompson's approach to digital media delivery, and adding Ishihara's licensing and key management framework would create a more comprehensive DRM system. Ex[1003], ¶ 187.

B. Dependent Claim 9

1. 9[pre]: The method of claim 7,

As explained above for Claim 7 in Ground 7, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 7.

2. 9[a]: wherein the SD card is pre-configured with the user key stored in the secure area of the SD card.

Ishihara discloses this limitation. Ex[1003], ¶ 189.

Ishihara discloses that certain keys can come pre-programmed in the secure portion of the memory storage device. Ex[1009].

Incorporating Ishihara's pre-configuration of user keys into the Thompson-Kasahara system to streamline the authentication and decryption process for media files would have been obvious to a POSITA. Ex[1003], ¶ 190. In the Thompson-Kasahara system, encryption keys are essential for content playback, and ensuring that a user key is pre-installed in the secure area of an SD card would simplify and enhance the user experience by eliminating the need for additional key transfers at the time of media download. Ex[1003], ¶ 190.

C. Dependent Claim 14

1. 14[pre]: The computer readable storage medium of claim 12,

As explained above for Claim 12 in Ground 12, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 12.

2. 14[a]: wherein the SD card is pre-configured with the user key stored in the secure area of the SD card.

For the same reasons described for Claim 9 [a] in Ground 3, Ishihara teaches this limitation.

XV. GROUND 4: CLAIMS 17 AND 18 ARE OBVIOUS OVER THOMPSON AND KASAHARA IN VIEW OF PONCELEON

A. Motivation to Combine

A POSITA would have been motivated to combine Ponceleon (Ex[1008]) with Thompson (Ex[1005]) and Kasahara (Ex[1007]) because Ponceleon provides additional details on secure digital media distribution models, including subscription and licensing mechanisms. Ex[1008] at p. 496; Ex[1003], ¶ 195. Thompson and Kasahara already describe a secure digital content transfer system, but Ponceleon introduces sophisticated DRM frameworks that facilitate controlled access and rental-based digital media distribution. Ex[1008] at p. 496; Ex[1003], ¶ 195. Integrating Ponceleon's licensing and DRM structures with Thompson and Kasahara's secure kiosk-based delivery system would have been a natural extension of existing methods, providing an improved and commercially viable approach to digital media transactions. Ex[1003], ¶ 196. A POSITA would have recognized that incorporating Ponceleon's user authentication and access control techniques would yield a predictable and beneficial enhancement to the secure digital kiosk environment of Thompson and Kasahara. Ex[1003], ¶ 197.

B. Dependent Claim 17

1. 17[pre]: The computer readable storage medium of claim 12

As explained above for Claim 12 in Ground 1, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 12.

2. 17[a]: wherein the instructions cause the media file to be downloaded to the SD card in substantially 2 minutes.

Thompson and Ponceleon, either alone or in combination, teach this limitation.

Thompson discloses a "high-speed programming port" that has a data transfer rate of between 65 MB/sec to 500 MB/sec. Ex[10005] at [0047]. This rate would allow for the download of a 20 GB video file in between 40 seconds to 5 minutes. *Id.*

Ponceleon discloses using SD cards to achieve the download of a 120-minute movie in less than 20 seconds. Ex[1008].

C. Dependent Claim 18

1. 18[pre]: The method of claim 7

As explained above for Claim 12 in Ground 1, Thompson and Kasahara, alone or in combination, teach each and every limitation of Claim 12.

2. 18[a]: wherein the media file is downloaded to the SD card in substantially 2 minutes.

For the same reasons described for Claim 17[a] in Ground 1, Thompson and Ponceleon, alone or in combination, teach this limitation.

XVI. DISCRETIONARY DENIAL IS NOT APPROPRIATE

The Board should decline to exercise its discretion to deny institution based on the co-pending Texas Action. The factors set forth in *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential) ("*Fintiv* factors") favor institution.

The first *Fintiv* factor favors institution, or is at a minimum neutral, because the potential of a stay exists in the Texas Action if this proceeding is instituted, especially as this Petition challenges all asserted claims. *See, e.g.*, *Pers. Audio LLC v. Google, Inc.*, 230 F. Supp. 3d 623, 626 (E.D. Tex. 2017). Further, Petitioner intends to request a stay if the IPR is instituted.

Regarding the second factor, the District Court tentatively set trial in the Texas Litigation for January 2026, however in light of the Board's holistic analysis, the litigation trial date is not determinative. *See, e.g., NetNut Ltd. v. Bright Data Ltd.*, IPR2021-01492, Paper 12 at 9-16 (PTAB Mar. 21, 2022) (instituting review with related litigation trial date six months before a final written decision); *CoolIT Sys., Inc. v. Asetek Danmark A/S*, IPR2021-01195, Paper 10, at 11-14 (PTAB Dec. 28, 2021) (same by five months); *Align Tech., Inc. v. 3Shape A/S*, IPR2021-01313, Paper 11, at 16-19 (PTAB Feb. 10, 2022) (same by four months). Thus, in view of the other factors, particularly given that the Parties have not engaged in any claim construction or any expert discovery, Factor 2 does not warrant denial.

The third *Fintiv* factor weighs in favor of institution. The Texas Action is in its early stages. The parties have not yet briefed claim construction or engaged in meaningful discovery. No depositions have taken place, and expert discovery is far off.

The fourth *Fintiv* factor weighs in favor of institution or is, at a minimum, neutral. Petitioner will file in the parallel district court litigation a stipulation that, if IPR is instituted, it will not pursue in the parallel litigation any ground that is raised or that could have reasonably been raised in an IPR. This favors institution. *Sotera, Wireless, Inc. v. Masimo Corp*., IPR2020-01019, Paper 12 at 19 (PTAB Dec. 1, 2020) (precedential).

Also, despite Petitioner being the defendant in the Texas Action (*Fintiv* factor five)—something out of Petitioner's control—other circumstances weigh against discretionary denial (*Fintiv* factor six). For one, the strength of the merits in the proposed invalidity grounds favors institution. *Fintiv*, 14-15. Furthermore, this IPR is the sole IPR challenging the '783 Patent before the Board, which favors institution. *Google LLC v. Uniloc 2017 LLC*, IPR2020-00115, Paper 10 at 6 (PTAB May 12, 2020).

XVII. CONCLUSION

Each of the challenged claims is invalid, and Petitioner has shown a substantial likelihood of invalidation of each. Petitioner seeks institution of *inter partes* review of the challenged claims.

Dated: March 12, 2025

Respectfully submitted,

/Robert C.F. Pérez/

Robert C.F. Pérez
(Reg. No. 39,328)
PILLSBURY WINTHROP SHAW
PITTMAN LLP
7900 Tysons One Place, Suite 500
Tysons, VA 22102
Telephone: 703.770.7759
Facsimile: 703.770.7901
Email: robert.perez@pillsburylaw.com

Christopher Kao (*pro hac vice* to be filed)
Brock S. Weber (*pro hac vice* to be filed)
PILLSBURY WINTHROP SHAW
PITTMAN LLP
Four Embarcadero Center, 22nd Floor
San Francisco, CA 94111
Telephone: 415.983.1000
Email: christopher.kao@pillsburylaw.com
Email: brock.weber@pillsburylaw.com

Counsel for Petitioner

CERTIFICATE OF COMPLIANCE

1. The undersigned certifies that this brief complies with the type volume limitations of 37 CFR § 42.24(a)(1)(i). This brief contains 12,069 words (excluding the table of contents, the table of authorities, mandatory notices under 37 CFR § 42.8, the certificate of service, certificate of compliance, and appendix of exhibits), as calculated by the "Word Count" feature of Microsoft Word 360, the word processing program used to create it.

2. The undersigned further certifies that this brief complies with the typeface requirements of 37 CFR § 42.6(a)(2)(ii) and typestyle requirements of 37 CFR § 42.6(a)(2)(iii). This brief has been prepared in a proportionally spaced typeface using Microsoft Word in Times New Roman 14-point font.

Dated: March 12, 2025

Respectfully submitted,

/Robert C.F. Pérez/

Robert C.F. Pérez (Reg. No. 39,328)
PILLSBURY WINTHROP SHAW
PITTMAN LLP
7900 Tysons One Place, Suite 500
Tysons, VA 22102
Telephone: 703.770.7759
Facsimile: 703.770.7901
Email: robert.perez@pillsburylaw.com

Counsel for Petitioner

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true copy of the foregoing **PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 8,977,783** and supporting materials have been served in its entirety by electronic mail this 12th day of March, 2025, and to be served by FedEx on March 13, 2025 on Patent Owner at the correspondence address for the attorney of record for U.S. Patent No. 8,977,783 shown in USPTO Patent Center, as well as on counsel for Patent Owner in the co-pending litigation:

Patent Owner in Patent Center:

Peter Lambrianakos, Esq.
Fabricant LLP
411 Theodore Fremd Road, Suite 206 South
Rye, NY 10580
plambrianakos@fabricantllp.com

Counsel for Patent Owner in co-pending litigation:

Alfred R. Fabricant
Peter Lambrianakos
Vincent J. Rubino, III
Enrique W. Iturralde
FABRICANT LLP
411 Theodore Fremd Avenue
Suite 206 South
Rye, NY 10580

John Andrew Rubino
Michael Mondelli III
RUBINO IP
51 J.F.K. Parkway
Short Hills, NJ 07078

Samuel F. Baxter
Jennifer L. Truelove
MCKOOL SMITH, P.C.
104 E. Houston Street, Suite 300
Marshall, TX 75670

/Robert C.F. Pérez/
Robert C.F. Pérez (Reg. No. 39,328)