

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETFLIX, INC.

Petitioner,

v.

LAURI VALJAKKA,

Patent Owner.

IPR2023-00423

Patent No. 10,726,102

**PRELIMINARY RESPONSE TO PETITION FOR *INTER PARTES*
REVIEW OF U.S. PATENT NO. 10,726,102**

TABLE OF CONTENTS

I. <u>INTRODUCTION</u>	1
II. <u>OVERVIEW OF THE '102 PATENT</u>	2
A. <u>Brief Description</u>	2
B. <u>The '102 Patent Prosecution History</u>	5
C. <u>Claim Construction</u>	6
IV. <u>THE ASSERTED PRIOR ART</u>	7
A. <u>Downs (EXH1005)</u>	7
B. <u>DeMello (EXH1006)</u>	13
C. <u>Schwartz (EXH1007)</u>	15
D. <u>Walmsley (EXH1008)</u>	17
V. <u>PETITIONER HAS NOT DEMONSTRATED A REASONABLE</u> <u>LIKELIHOOD OF SUCCESS FOR THE GROUNDS ADVANCED IN THE</u> <u>PETITION, AND THE PETITION SHOULD BE DENIED</u>	18
A. <u>Requirements for Showing Obviousness Under 35 U.S.C. § 103</u>	18
B. <u>Petitioner Fails to Establish in Ground 1 that Challenged Claim 10 is Obvious</u> <u>Over Downs</u>	20
<u>Claim 10</u>	20
a. <u>Downs does not teach the limitations [10B] and [10C]</u>	21
b. <u>Downs does not teach the limitations [10D]</u>	24
C. <u>Petitioner Fails to Establish in Ground 2 that Challenged Claims 10-11 are</u> <u>Obvious Over DeMello in View of Schwartz and Walmsley</u>	28
1. <u>Claim 10</u>	28
a. <u>DeMello in View of Schwartz and Walmsley does not teach the limitations</u> <u>[10B] and [10C]</u>	28
b. <u>DeMello in View of Schwartz and Walmsley does not teach the limitation</u> <u>[10D]</u>	33
2. <u>Claim 11</u>	35
VI. <u>CONCLUSION</u>	36

TABLE OF AUTHORITIES

Cases

<i>Graham v. John Deere Co.</i> , 383 U.S. 1 (1966)	18
<i>Pers. Web Techs., LLC v. Apple, Inc.</i> , 848 F.3d 987 (Fed. Cir. 2017)	19
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	19
<i>Los Angeles Biomedical Res. Inst. at Harbor-UCLA Med. Ctr. v. Eli Lilly Co.</i> , 849 F.3d 1049 (Fed. Cir. 2017)	19
<i>Broadcom Corp. v. Emulex Corp.</i> , 732 F.3d 1325 (Fed. Cir. 2013).	19
<i>In re Van Os</i> , 844 F.3d 1359 (Fed. Cir. 2017).....	20
<i>Innogenetics, N.V. v. Abbott Labs.</i> , 512 F.3d 1363 (Fed. Cir. 2008).	20
<i>CFMT, Inc. v. Yieldup Intern. Corp.</i> , 349 F.3d 1333, 1342 (Fed. Cir. 2003).....	28

PTAB Cases

<i>Apple, Inc. v. Contentguard Holdings, Inc.</i> , IPR2015-00355, Paper 9 (P.T.A.B. June 26, 2015)	18
--	----

Statutes

35 U.S.C. §103.....	10
---------------------	----

Rules

37 C.F.R. § 42.107	1
--------------------------	---

I. INTRODUCTION

On January 2, 2023, Netflix, INC. (“Petitioner”) submitted a Petition for *Inter Partes* Review (“Petition”) of U.S. Patent No. 10,726,102 (“the ’102 Patent”, “EXH1001”), challenging Claims 10-11 (“Challenged Claims”). Pursuant to 37 C.F.R. § 42.107, Patent Owner Lauri Valjakka, (“Patent Owner”) files this Preliminary Response to the Petition, setting forth reasons the Board should deny institution.

Petitioner challenges the patentability of Claims 10-11 of the ’102 Patent based on the following references:

U.S. Pat. No. 6,226,618 (“Downs”);

U.S. Pat. No. 6,891,953, (“DeMello”);

U.S. Pat. No. 8,112,444 (“Schwartz”); and

U.S. Pat. No. 7,685,424 (“Walmsley”).

Petitioner requests institution of the IPR proceeding on the following grounds.

Ground	Claims	Basis
1	10	§103 – Downs
2	10-11	§103 – DeMello, Schwartz, and Walmsley

Petitioner fails to establish a reasonable likelihood that the Challenged Claims are unpatentable. Patent Owner will specifically address each of Petitioner's arguments in the following sections.

II. OVERVIEW OF THE '102 PATENT

A. Brief Description

The application issued as the '102 Patent was filed on January 8, 2015. EXH1001, 1:7-15. The '102 Patent claims foreign priority of FI application Ser. No. 20145013, filed on Jan. 08, 2014. EXH1001, 1:7-24.

The '102 Patent generally discloses a system for providing access to access restricted content to a user. EXH1001, at Abstract.

The architecture of the system is shown in Figure 1 (reproduced below).

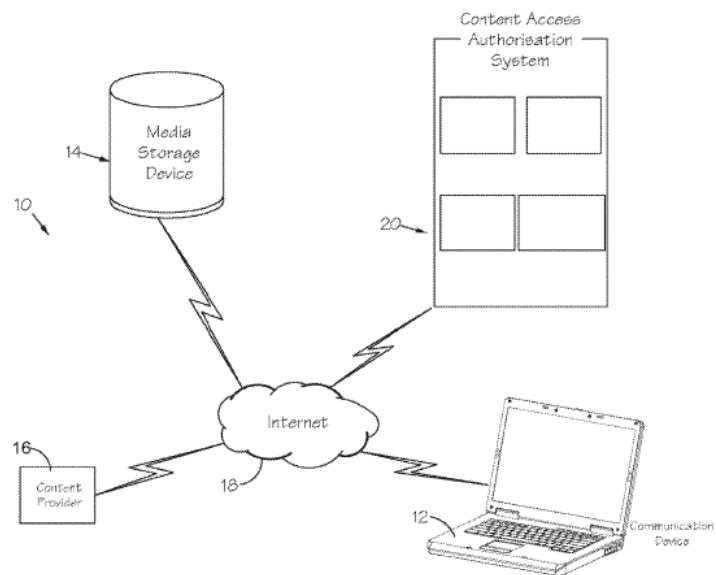


FIG 1

'102 Patent, Figure 1

The system 20 includes a communication device 12 used by a user who intends to obtain access to access restricted content which may be stored in a media storage device 14, a content provider 16 and a content access authorization server 22. EXH1001, 5:13-62.

The content access authorization server 22 includes an interrogation module 26, a validation module 28, a calculation module 30, a decryption module 32 and a communication arrangement 34. EXH1001, 6:1-17. The media storage device 14 stores therein a plurality of content identifiers and associated content, digital rights management keys and/or user identifiers. EXH1001, 6:20-22.

In the illustrated embodiment, the communication arrangement 34 receives a content request message from the personal computer 12 of the user. The content request message includes a unique identifier associated with the user and a content identifier. The interrogation module 26 interrogates the media storage device 14 whether or not the received content identifier and user identifier matches with any combination of the stored user identifiers and content identifiers. EXH1001, 6:55-7:15.

The validation module 28 retrieves a first digital rights management key (Key #1) and a header associated with the user identifier in response to a determination that the received content identifier and user identifier matches with at least one combination of the stored user identifiers and content identifiers. The interrogation

module further interrogates the media storage device 14 in order to determine whether or not the content identifier and the Key # 1 matches with any combination of content identifier and Key # 1 stored in the media storage device 14 and associated with the user identifier. If the answer is affirmative, the validation module provides the access-restricted media content to the user. EXH1001, 7:16-32.

To protect integrity of the access restricted media content, “the client may obtain, in phase 4120, a fingerprint of the content wherein the obtaining may be based at least in part on the first DRM key. In phase 4130, the client may transmit the fingerprint to the content server, optionally with the content identifier and in phase 4140, the content server may query the content database for the content fingerprint. The query may comprise the content identifier. In phase 4150, the content database may responsively provide the fingerprint to the content server. In phase 4160, the server may compare the fingerprints received in phases 4150 and 4130. In case of mismatch, the processing advances to phase 4170 and ends. In case the fingerprints match, processing advances to phase 4180 where the client is provided with a positive validation result.” EXH1001,10:33-47.

Once the user has access to the access restricted media content, the user may need to use the media content. In that instance, the communication arrangement 34 may receive a content usage request message from the personal computer 12 of the user. The content usage request message includes the user identifier, Key # 1, and

the content identifier. The validation module 28 analyses the header associated with Key #1 and prepares a second digital rights management key (Key #2). The preparation of Key #2 may comprise, for example, performing a cryptographic operation on at least part of the access restricted content, wherein the cryptographic operation may employ Key #1. The cryptographic operation may comprise decrypting Key #2 by using Key #1. A decryption module may be configured to use Key # 1 and Key # 2 to decode the media content, thereby allowing the user use of media content. EXH1001,7:64-8:20.

The validation module may further use Key # 1 in order to prepare a third digital rights management key (Key #3). Key # 3 may be obtained from the access restricted content using Key # 1 in a similar was as described above in connection with obtaining Key # 2. EXH1001,8:21-34.

B. The '102 Patent Prosecution History

The application that issued as the '102 Patent was filed on January 8, 2015. EXH1001, 1:7-15. The '102 Patent claims foreign priority of FI application Ser. No. 20145013, filed on Jan. 08, 2014. EXH1001, 1:7-24.

References cited by the applicant and considered by the Examiner include U.S. Patent No. 6,236,365 (LeBlanc, EXH1015), U.S. Patent App. Publ. Nos. 2002/0168986 (Lau, EXH1016), On January 9, 2018, "A Notice of Allowance" was mailed allowing claims 1-30. (EXH1002 at 1345).

During prosecution of the '102 Patent, the examiner issued a restriction requirement to the original claim set, holding that claims 1-5 were directed to receiving a content request message, while claims 6-9 were directed to obtain an access restricted content from at least of a content database and a content providing server. *File History*, EX1002, at 83. The applicant elected claims 6-9, which were rejected as judicial exception, anticipated or obvious. References cited by the applicant and considered by the Examiner include U.S. Patent App. Publ. No. 2012/0308008 (Kondareddy), *File History*, EX1002, at 104. The '102 patent went through a lengthy prosecution, involving three nonfinal rejections, two final rejections, and two requests for continued examination. On August 14, 2019, "A Notice of Allowance" was mailed allowing claims 6,8-15 and 17-18. (EXH1002 at 411).

C. Claim Construction

According to 37 C.F.R. §42.100(b), in an inter partes review, claim terms are construed using the same standard used in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.

The ordinary and customary meaning of a term may be evidenced by a variety of sources, including the words of the claims themselves, the specification,

drawings, and prior art. However, the best source for determining the meaning of a claim term is the specification – the greatest clarity is obtained when the specification serves as a glossary for the claim terms. The words of the claim must be given their plain meaning unless the plain meaning is inconsistent with the specification. *In re Zletz*, 893 F.2d 319, 321, 13 USPQ2d 1320, 1322 (Fed. Cir. 1989); *Chef America, Inc. v. Lamb-Weston, Inc.*, 358 F.3d 1371, 1372, 69 USPQ2d 1857 (Fed. Cir. 2004).

Patent owner adopts Court’s construction of “fingerprint” and “Order of Steps” (Ex. 1013) proposed by petitioner. Pet., 15-19.

III. LEVEL OF ORDINARY SKILL IN THE ART

For purposes of this Response, PO adopt Petitioner’s proffered level of ordinary skill in the art because it comports with the technology and claims of the ’102 Patent as well as the asserted prior art.

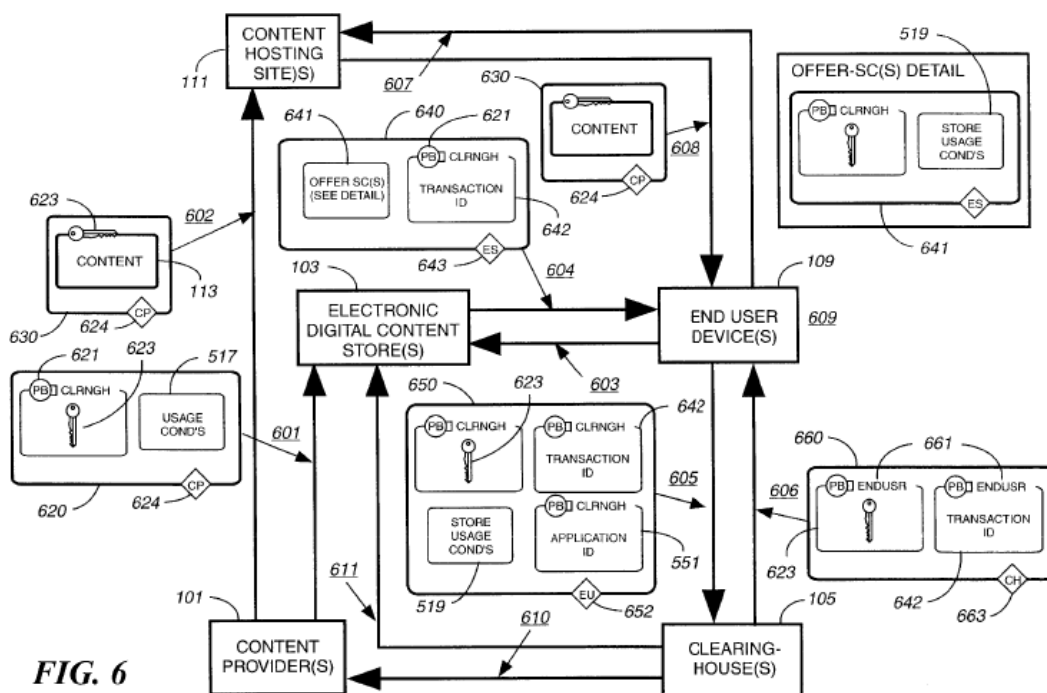
IV. THE ASSERTED PRIOR ART

A. Downs (EXH1005)

Downs describes a method and system for “Securely providing data to a user’s system” EXH1005, Abstract.

Downs’s Secure Digital Content Electronic Distribution system, illustrated in

Figure 6 below, “encompasses several business elements that comprise an end-to-end solution, including: Content Provider(s) 101 or the proprietors of the Digital Content, Electronic Digital Content Store(s) 103, Intermediate Market Partners (not shown), Clearinghouse(s) 105, Content Hosting Site 111, Transmission Infrastructures 107, and End-User Device(s) 109.” EXH1005, 8:55-65.



Downs, Figure 6

In the specification, Downs explains “Symmetric Algorithms,” “Public Key Algorithms” and “Digital Signature” as follows:

Symmetric Algorithms

In the Secure Digital Content Electronic Distribution System 100 the Content Provider(s) 101 encrypts the content using symmetric algorithms. They are called

symmetric algorithms because the same key is used to encrypt and decrypt data. The data sender and the message recipient must share the key. The shared key is referred to here as the symmetric key. EXH1005, 12:44-49.

Public Key Algorithms

In the Secure Digital Content Electronic Distribution System 100, symmetric keys and other small data pieces are encrypted using public keys. Public key algorithms use two keys. The two keys are mathematically related so that data encrypted with one key can only be decrypted with the other key. The owner of the keys keeps one key private (private key) and publicly distributes the second key (public key).

To secure the transmission of a confidential message using a public key algorithm, one must use the recipient's public key to encrypt the message. Only the recipient, who has the associated private key, can decrypt the message. **Public key algorithms are also used to generate digital signatures. The private key is used for that purpose.** The following section provides information on digital signatures. EXH1005, 13:20-33.

Digital Signature

In the Secure Digital Content Electronic Distribution System 100, the issuer of SC(s) protects the integrity of SC(s) by digitally signing it. In general, **to create a digital signature of a message, a message owner first computes the message**

digest (defined below) and then encrypts the message digest using the owner's private key. The message is distributed with its signature. **Any recipient of the message can verify the digital signature first by decrypting the signature using the public key of the message owner to recover the message digest.** Then, the recipient computes the digest of the received message and compares it with the recovered one. If the message has not being altered during distribution, the calculated digest and recovered digest must be equal.

A one-way hash algorithm is used to calculate a message digest. A hash algorithm takes a variable-length-input message and converts it into a fixed length string, the message digest. A one-way hash algorithm operates only in one direction. That is, it is easy to calculate the digest for an input message, but it is very difficult (computationally infeasible) to generate the input message from its digest. Because of the properties of the one-way hash functions, **one can think of a message digest as a fingerprint of the message.** EXH1005, 13:49-14:14.

Downs provides an overview of the encryption and decryption process as follows:

Process Flow for Encryption Process of FIG. 3

301 Sender generates a random symmetric key and uses it to encrypt the content.

302 Sender runs the encrypted content through a hash algorithm to produce the content digest.

303 Sender encrypts the symmetric key using the recipient's public key.

304 Sender runs the encrypted symmetric key through the same hash algorithm used in step 2 to produce the symmetric key digest.

305 Sender runs the concatenation of the content digest and symmetric key digest through the same hash algorithm used in step 2 to produce the SC(s) digest.

306 Sender encrypts the SC(s) digest with the sender's private key to produce the digital signature for the SC(s). PV SENDER refers to the sender's private key.

307B Sender creates a SC(s) file that includes the encrypted content, encrypted symmetric key, content digest, symmetric key digest, sender's certificate, and SC(s) signature.

307A Sender must have obtained the certificate from a certification authority prior to initiating secure communications. The certification authority includes in the certificate the sender's public key, the sender's name, and signs it. Sender transmits the SC(s) to the recipient. EXH1005, Col. 15-16.

Process Flow for Decryption Process of FIG. 4

408 Recipient receives the SC(s) and separates its parts.

409 Recipient verifies the digital signature in the sender's certificate by decrypting it with the public key of the certification authority. If the certificate's digital signature is valid, the recipient acquires the sender's public key from the certificate.

410 Recipient decrypts the SC(s) digital signature using the sender's public key. This recovers the SC(s) digest.

411 Recipient runs the concatenation of the received content digest and encrypted key digest through the same hash algorithm used by the sender to compute the SC(s) digest.

412 Recipient compares the computed SC(s) digest with the one recovered from the sender's digital signature. If they are the same, the recipient confirms that the received digests have not been altered and continues with the decryption process.

413 Recipient runs the encrypted symmetric key through the same hash algorithm used in step 411 to compute the symmetric key digest.

414 Recipient compares the computed symmetric key digest with the one received in the SC(s). If it is the same, the recipient knows that the encrypted symmetric key has not been altered.

415 Recipient runs the encrypted content through the same hash algorithm used in step 411 to compute the content digest.

416 Recipient compares the computed content digest with the one received
in the SC(s). If it is the same, the recipient knows that the encrypted content has not
been altered.

417 Recipient decrypts the encrypted symmetric key using the recipient's
private key. This recovers the symmetric key.

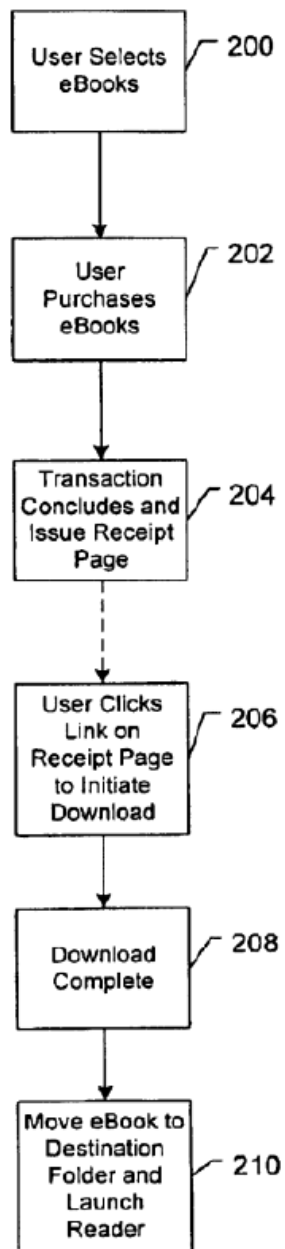
418 Recipient uses the symmetric key to decrypt the encrypted content. This
recovers the content. EXH1005, Col. 15-16.

B. DeMello (EXH1006)

DeMello discloses a system for processing and delivery of electronic content
wherein the content may be protected at multiple levels. EXH1006, 4:41-43.
DeMello provides an infrastructure "which supports the distribution of protected
content in a digital rights management ('DRM') system." EXH1006, 1:60-62.

DeMello describes a server architecture includes "a retail site which sells
content items to consumers, a fulfillment site which provides to consumers the
content items sold by the retail site, and an activation site which enables consumer
reading devices to use content items having an enhanced level of copy protection."
EXH1006, Abstract.

DeMello's "process by which eBook titles are acquired and delivered online,"
illustrated in Figure 9 below, begins in step 200 when a "user chooses book(s) via
mechanism that the retail site implements." EXH1006, 25:66-67, 26:2-3.



DeMello - Figure 9

In step 204, when the transaction completes, the retail site generates “a receipt page (i.e., an order confirmation or ‘thank you’ page) that contains links (POST

requests) for downloading each title purchased (i.e., the URLs containing the address of content server 76, plus the encrypted information created by URL encryption object 74).” For level 5 content, a client-side script executing at the user device “populate[s] the body of the POST with the activation certificate, preferably using COM object implemented by the reader which obtains the necessary activation certificate or relevant information therefrom.” EXH1006, 26:4-15.

When the user clicks on the links in the POST message, the browser at the user’s device initiates a “download from content servers 76 (via the download server ISAPI DLL 78).” For level 3 content, “the download server 76 adds the consumer’s name to the title meta-data and re-seal the symmetric key 14A using a new cryptographic hash resulting from the new metadata, which now includes the users name.” For level 5 content, “a license is generated and embedded in the LIT file, in addition to the Bookplate being created.” The license “contains the symmetric key 14A that encrypted the LIT file ‘sealed’ with the public key in the activation certificate[,] [w]hen the download is complete (step 208), the download server 76 logs the transaction and, on the client, the reader is launched automatically (step 210).” EXH1006, 26:16-30.

C. Schwartz (EXH1007)

Schwartz describes a method “for facilitating the validation of content over a network.” EXH1007, 4:62-64. In Schwartz, a content registration authority is

provided which registers the content disseminated by one or more content providers to one or more client devices. A client device which receives content that has been registered can securely consume the content, based on an assumption that a content provider which furnishes the content is entrusted by the content registration authority to provide the content, and without prompting a user of the client device to expressly approve the content provider. In a first solution, the content registration authority registers the content by issuing a certification stamp; in a second solution, the content registration authority registers the content by storing registration information in a central repository. EXH1007, Abstract.

Schwartz describes two approaches for improving content security. According to the second solution ('solution B'), "registration may comprise storing the content identifier in a registration store maintained by the content registration authority." "In this case, validation at the client device may comprise determining whether received content has a corresponding registered content identifier stored at the content registration authority." EXH1007, 5:67-6:5.

In this solution, content registration authority 332 "receives a content identifier from the content publisher." The content publisher "forms the content identifier by computing a digest of the content 330, such as a hash of the content." Upon receipt of the content identifier, the content registration authority 332 "store[s] the content

identifier in a registration data store, thereby effectively registering the content identifier.” EXH1007, 10:64-11:4.

The content publisher 328 then “transfer[s] the content 330 to the client device A.” To verify the integrity of the content 330, the client device A 302 independently “compute[s] the content identifier of the received content 330, e.g., by forming a hash of the received content.” The client device A 302 then “use[s] the computed content identifier as a key to determine whether the content has been previously registered in the registration data store of the content registration authority 332.” If this test passes, “the client device A 302 assesses that the content 330 is trustworthy, regardless of the specific identity of the content publisher 328 used to furnish the content 330. The client device A302 can then safely consume the content 330 by storing (and possibly installing) it.” (EXH1007, Schwartz, 11:4-18.)

D. Walmsley (EXH1008)

Walmsley discloses a validation method for determining whether an untrusted chip is valid, or not. EXH1008, Abstract. Walmsley describes the use of hash functions. Specifically, Walmsley explains that a “one-way hash function is not sufficient protection for a message.” EXH1008, 11:43-44. Walmsley then provide a solution to this problem “the Message Authentication Code, or MAC.” EXH1008, 11:52-53.

Walmsley specifically discloses use of HMAC which was “gaining acceptance as a solution for Internet message authentication security protocols.” An HMAC uses a “secret key shared by the two parties” to compute the hash. EXH1008, 12:32-47.

Walmsley teaches that, to authenticate a consumable, “Two kinds of data must be stored within the authentication chip: Authentication data, such as secret keys, Consumable state data, such as serial numbers, and media remaining etc.” EXH1008, 26:47-52. Authentication data must remain confidential. It needs to be stored in the chip during a manufacturing/programming stage of the chip’s life, but from then on must not be permitted to leave the chip. EXH1008, 26:62-65.

V. PETITIONER HAS NOT DEMONSTRATED A REASONABLE LIKELIHOOD OF SUCCESS FOR THE GROUNDS ADVANCED IN THE PETITION, AND THE PETITION SHOULD BE DENIED

A. Requirements for Showing Obviousness Under 35 U.S.C. § 103

The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) where in evidence, so called secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). The Board has held that a failure to identify the differences between the claimed subject matter and the prior art is fatal to an obviousness challenge. *See, Apple, Inc. v. Contentguard Holdings, Inc.*,

IPR2015-00355, Decision Denying Institution of *Inter Partes* Review, Paper 9 at 9-10 (P.T.A.B. June 26, 2015) (denying institution for failure to identify the differences between the claimed subject matter and the prior art).

In arriving at an obviousness determination, the Board must sufficiently explain and support the conclusions that the prior art references disclose all the elements recited in the Challenged Claims and a relevant skilled artisan not only could have made, but would have been motivated to combine all the prior-art references in the way the patent claims. *Pers. Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 994 (Fed. Cir. 2017). That is, even if all the claim elements are found across a number of references, an obviousness determination must consider whether a person of ordinary skill in the art would have been motivated to combine those references. *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1368 (Fed. Cir. 2016); *Los Angeles Biomedical Res. Inst. at Harbor-UCLA Med. Ctr. v. Eli Lilly Co.*, 849 F.3d 1049, 1067 (Fed. Cir. 2017) (vacating and remanding an obviousness determination, in part, because the Board did not make factual findings as to whether there was an apparent reason to combine all three prior art references to achieve the claimed invention and whether a POSITA would have had a reasonable expectation of success from such a combination). This combination determination, as supported by an articulated motivation to combine, requires a plausible rationale as to why those prior art references would have worked together.

Broadcom Corp. v. Emulex Corp., 732 F.3d 1325, 1335 (Fed. Cir. 2013). Absent some articulated rationale, a “common sense” finding is no different than the conclusory statement “would have been obvious.” *In re Van Os*, 844 F.3d 1359, 1361 (Fed. Cir. 2017). Of additional importance, “knowledge of a problem and motivation to solve it are entirely different from motivation to combine particular references.” *Innogenetics, N.V. v. Abbott Labs.*, 512 F.3d 1363, 1373 (Fed. Cir. 2008).

B. Petitioner Fails to Establish in Ground 1 that Challenged Claim 10 is Obvious Over Downs

Claim 10

Independent claim 10 has been broken into elements for consideration by Petitioner as follows:

[10P]. A method, comprising:

[10A]. obtaining an access restricted content from at least one of a content database and a content providing server;

[10B] obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query, the query comprising the content identifier and an identifier associated with the user;

[10C] deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content wherein the obtaining is based at least in part on the first digital rights management key,

[10D] causing the content providing server to validate the fingerprint; and, if the validation is successful, accessing the access restricted content and information describing encryption properties of the access restricted content, and

[10E] deriving, using the digital rights management header of the access restricted content, from the access restricted content a second and third digital rights management key,

[10F] wherein the second and third digital rights management keys are applied to retrieve the payload of the access restricted content and

[10G] wherein at least one of the second or third digital rights management key is used to encrypt the other key of the second or third digital rights management key,

[10H] wherein the content is usable without being in an unprotected state.

a. Downs does not teach the limitations [10B] and [10C]

First, as to the limitation “first digital rights management key.” Petitioner asserts that “the Content Provider’s public key and its associated private key (the Content Provider’s asymmetric key pair) are the “first digital rights management key.” Pet. At 30-31.

Petitioner proffers that Downs discloses “End-User device 109 “initiates the request for a Content SC(s) 630 by sending the License SC(s) 660 to the Content Hosting Site(s) 111.” Pet. At 29. “A POSITA would understand that the primary

content site (Content Hosting Site 111) retrieves the requested Content SC from the appropriate secondary content site for delivery to the End User.” “The Content SC, illustrated below, includes the Certificate for the Content Provider. **The certificate “includes the public key**, the name of the person or entity, an expiration date, the name of the certification authority, and other information.” Pet. At 30. **The Content SC digest is encrypted with the Content Provider’s private key** [the recited “first digital rights management key”] to produce the digital signature for the SC (306). Pet. At 32.

According to Petitioner, on the one hand, client obtains a public key of a Content Provider from a content database, thus the public key is identical to “the first digital rights management key”, on the other hand, the Content Provider derives a fingerprint of the access restricted content using Content Provider’s private key, thus, the private key is identical to “the first digital rights management key.”

Although Content Provider’s private key and public key are the Content Provider’s asymmetric key pair, there are different keys, since Downs employed Public Key Algorithms (using different private key and public key) in Digital Signature system which encrypts and decrypts the digital signature for the SC using the private key by the Content Provider and public key by the client respectively. EXH1005, 13:49-14:14. Only in the Symmetric Algorithms which used by Downs

to encrypts and decrypts the content of the SC, encryption key and decryption key are identical. EXH1005, 12:44-49.

In the '102 Patent, both the specification and the language of claims show that “the first digital rights management key” obtained from a database and used to derive a fingerprint of the access restricted content is the same key, which is distinct from the Content Provider’s public key and its associated private key of Downs.

Second, regarding the limitation “deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content.” On the one hand, Petitioner concedes that “deriving a fingerprint” is conducted by the client, since Petitioner proffers that “This interpretation is consistent with the first method described in the specification. (EXH1003, ¶60.) In this method, the client first obtains a fingerprint using the first DRM key and “transmit[s] the fingerprint to the content server, optionally with the content identifier.” (EXH1001, 10:35-37.) Pet, at 18.

On the other hand, in arguing that Downs teaches “deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content,” Petitioner proffers that “Because of the properties of the one-way hash functions, one can think of a message digest as a fingerprint of the message.” (EXH1005, 14:13-14.) and Downs discloses “**The Content Provider creates a digest for the Content SC** by concatenating the individual digests

associated with Content SC (encrypted content digest, encrypted metadata digest, and metadata digest). (EXH1005, 16:8-10.) **The Content SC digest is encrypted with the Content Provider's private key** [the recited “first digital rights management key” to produce the digital signature for the SC (306). (EXH1005, 16:11-13.) The digital signature is “a fingerprint of the access restricted content” that is “derived, using the first digital rights management key, from the access restricted content. Pet, at 18.

The cited portions of the Petition shows that “deriving a fingerprint” is conducted by the Content Provider, not by the client, which conflicts with Petitioner's position that “deriving a fingerprint” is conducted by the client as depicted both in the specification and the language of claims. Therefore, Downs does not teach that “deriving a fingerprint” is conducted by the client as required by claim 10.

b. Downs does not teach the limitations [10D]

Regarding the limitation “causing the content providing server to validate the fingerprint; and, if the validation is successful, accessing the access restricted content.”

To arguing that Downs teaches the limitation, Petitioner proffers that Upon receipt of the Content SC, the Content Hosting Site (primary content site) verifies

the integrity of the Content SC. As explained by Downs, “recipients of SC(s) can verify the integrity of the SC(s) and its parts by means of the received digital signature and part digests.” (EXH1005, 14:3-5; see also, EXH1005, 25:14-18 (“Parties receiving the SC(s) can use the digital signature to verify all of the digests and thus validate the integrity and completeness of the SC(s) and all of its parts”). Specifically, the Content Hosting Site “decrypts the SC(s) digital signature” using the Content Provider’s public key. (EXH1005, col. 16 (step 410).) The Content Hosting Site then compares the computed Content SC digest with the one recovered from the Content Provider’s digital signature. (EXH1005, col. 16 (step 412).) “If they are the same, recipient confirms that the received digests have not been altered.” (EXH1005, col. 16 (step 412).) Thus, the system “caus[es] the content providing server to validate the fingerprint” [10D] to verify the integrity of the received Content SC. (EXH1003, ¶85.) Pet, at 33.

It is clear that Petitioner equates “Content Hosting Site” to “content providing server” of the ’102 Patent. The cited portion of the Petition shows:

First, validating the fingerprint is performed by recipients of SC(s), not by the “Content Hosting Site.” Although the “Content Hosting Site” is a kind of recipient when it receives content from Content Provider(s), In the case of claim 10, “content providing server” is a sender to send content to the user, not a recipient, thus the “Content Hosting Site” should also be a sender, not a recipient.

Second, the purpose of validation the fingerprint **of Content SC** is to verifies the integrity of the Content SC, not to determine accessing the access restricted content. Downs does not disclose using the fingerprint **of Content SC** to determine “if the validation is successful, accessing the access restricted content.”

In fact, Downs discloses the “Content Hosting Site” validates the fingerprint **of License SC(s) not Content SC(s)** (corresponding to fingerprint of the access restricted content of the ’102 Patent) in order to determine accessing the access restricted content as follows:

The End-User Device(s) 109 initiates the request for a Content SC(s) 630 by sending the License SC(s) 660 to the Content Hosting Site(s) 111. This is the same License SC(s) 660 returned by the Clearinghouse(s) 105. **The Digital Signature of the License SC(s) 660 can be verified to determine if it is a valid License SC(s) 660. If it is a valid License SC(s) 660 either the download is initiated,** or the download request may be redirected to another Content Hosting Site(s) 111. EXH1005, 69:40-48.

Downs also describes the License SC(s) 660 as follows:

The following information is typically logged by the Clearinghouse(s) 105 for a License SC(s) 660:

Date and time of the request

Date and time of the purchase transaction

Content ID of the item being purchased

Identification of the Content Provider(s) 101

Store Usage Conditions 519

Watermarking instruction modifications

Transaction ID 535 that was added by the Electronic Digital Content Store(s)

103

Identification of the Electronic Digital Content Store(s) 103

Identification of the End-User Device(s) 109

End-User(s) credit card information

Authorization number received from the clearer of the credit card. EXH1005,
46:8-41.

The cited portion of the Petition shows that License SC(s) are different from Content SC(s). Therefore, Downs does not teach the limitation “causing the content providing server to validate the fingerprint; and, if the validation is successful, accessing the access restricted content.”

C. Downs Does Not Render Claim 1 Obvious

Petitioner fails to undertake a proper Graham analysis, because Downs lacks evidence of crucial limitations of claim 1, such as the elements [10B], [10C]. and [10D]. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Therefore, Downs does not render claim 10 obvious. Petition has failed to establish a prima facie case, since “obviousness requires a suggestion of all limitations in a claim.” *CFMT, Inc. v. Yieldup Intern. Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003).

C. Petitioner Fails to Establish in Ground 2 that Challenged Claims 10-11 are Obvious Over DeMello in View of Schwartz and Walmsley

1. Claim 10

a. DeMello in View of Schwartz and Walmsley does not teach the limitations [10B] and [10C]

The limitations [10B] and [10C] recite “obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query, the query comprising the content identifier and an identifier associated with the user; deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content wherein the obtaining is based at least in part on the first digital rights management key.”

The language of limitations [10B] and [10C] shows that, to verify the integrity of the access restricted content, client (user) obtains the first digital rights management key from content database during the period of querying and use the first digital rights management key to form a fingerprint of the access restricted content.

First, Petitioner admits that “While DeMello discloses the transmission of a content file having content encrypted using an encrypted symmetric key, **DeMello does not provide a technique to authenticate that the received content is the actual content** stored in the content database by the content provider.” Pet, at 54-55.

The function of limitations [10B] and [10C] is to authenticate that the received content is the actual content stored in the content database, since DeMello does not provide a technique to authenticate that the received content is the actual content stored in the content database, DeMello does not disclose the limitations [10B] and [10C].

Second, Petitioner proffers that Schwartz discloses the use of a one-way hash function to calculate a content ID for content and admits that Schwartz does not disclose any details regarding the hash function used with its technique. Pet, at 56. That is, Petitioner admits that Schwartz does not disclose “deriving, **using the first digital rights management key**, from the access restricted content a fingerprint of

the access restricted content wherein **the obtaining is based at least in part on the first digital rights management key.**” Thus, Schwartz does not teach the first digital rights management key.

Third, Petitioner argues that, “In the proposed combination, a POSITA would have been motivated to use a keyed hash for computing the Content ID (e.g., Book ID) in the combination of DeMello and Schwartz as disclosed by Walmsley. (Citing EXH1003, ¶138.) Specifically, a POSITA would have been motivated to use Walmsley’s message authentication code which is a “key-dependent one-way hash function.” (Citing EXH1003, 455.) As described by Walmsley, “[t]he simplest method of constructing a MAC from a hash function is to encrypt the hash value with a symmetric algorithm.” (EXH1008, 11:61-63.) Walmsley further describes a known MAC algorithm HMAC, which uses a hash function and a shared secret key. (EXH1008, 12:41-67.) **The shared secret hash key is the “first digital rights management key.”** (Citing EXH1003, ¶138.) Pet. At 65-66.

Petitioner further argues that Walmsley does not disclose that the symmetric hash key is shared by the content provider. However, a POSITA would have understood that in the combined system the shared symmetric hash key for the content would have been included in the content file with the shared encryption key (content key) for the content because it is a cryptographic key used to process the content stored in the content store (database) of DeMello. Like the content key, the

shared hash key would have been sealed with the public key of the user's activation certificate. Thus, the client device "obtain[s] a first digital rights management key from a content database" [10B] in the content file received by the user device. (Citing EXH1003, ¶139). Pet. At 66.

The cited portion of the Petition demonstrates Petitioner's tacit admission that Walmsley teaches the "first digital rights management key" and does not teach "obtain[s] a first digital rights management key from a content database."

Although the shared hash key is a kind of cryptographic key like the content key of DeMello, it should not be sealed with the public key of the user's activation certificate in the content file received by the user device just like the content key of DeMello. Since the content key and the shared hash key have different functions, the content key is used to encrypt the content while the shared hash key is used to authenticate content, they require different processing methods.

Walmsley teaches that the shared hash key is used to authenticate and stored within the authentication chip (corresponding to client's device of the '102 Patent) during a manufacturing/programming stage of the chip's life and must remain confidential. Walmsley describes the Authentication data (including the shared hash key) as follows,

“Although authentication protocols take care of ensuring data integrity in communicated messages, data storage integrity is also required. Two kinds of data must be stored within the authentication chip:

Authentication data, such as secret keys

Consumable state data, such as serial numbers, and media remaining etc.”

EXH1008,26:45-52.

“Authentication data must remain confidential. It needs to be stored in the chip during a manufacturing/programming stage of the chip’s life, but from then on must not be permitted to leave the chip.” EXH1008, 26:62-65.

Thus, there is no need for the authentication chip “obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query” since the shared hash key is already stored in the authentication chip. Walmsley teaches away from “obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query.”

Therefore, DeMello in View of Schwartz and Walmsley does not teach the limitations [10B] and [10C], particularly, DeMello in View of Schwartz and Walmsley does not teach the limitation “obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query” as required by claim 10 of the ’102 Patent.

b. DeMello in View of Schwartz and Walmsley does not teach the limitation [10D]

Regarding the limitation “causing the content providing server to validate the fingerprint; and, if the validation is successful, accessing the access restricted content.”

The language of limitations [10B] and [10C] shows validating the fingerprint is conducted by the content providing server, not by the user.

First, as set forth above, Petitioner admits that DeMello does not provide a technique to authenticate that the received content is the actual content, thus, DeMello does not disclose “causing the content providing server to validate the fingerprint; and, if the validation is successful, accessing the access restricted content.”

Second, Petitioner argues that “[Schwartz’s] client device “use[s] the computed content identifier as a key to determine whether the content has been previously registered in the registration data store of the content registration.” (EXH1007, 11:9-12.) That is, the user device transmits the keyed hash (“fingerprint”) to the content registration database at the Fulfillment site, DeMello’s content storage database (“content database”). As taught by Schwartz, the content database at the Fulfillment Site (“content providing server”) in the combined system validates the keyed hash by determining whether the keyed hash exists in the registration database of Content IDs. (Citing EXH1003, ¶141.) If the keyed hash

exists, the content received at the client device is authentic and has not been altered. (Id.) Thus, the combination teaches “causing the content providing server to validate the fingerprint.” Pet. At 67.

The cited portion of the petition shows that Petitioner admits that, as taught by Schwartz, validating the fingerprint is conducted by the client device, not by the content registration database (corresponding to the content providing server of the ’102 Patent). Petitioner does not argue that Walmsley teaches that validating the fingerprint is conducted by the content providing server, as required by the ’102 Patent either.

Therefore, DeMello in View of Schwartz and Walmsley does not teach the limitation [10D], particularly, DeMello in View of Schwartz and Walmsley does not teach the limitation “validating the fingerprint is conducted by the content providing server as required by the ’102 Patent” as required by claim 10 of the ’102 Patent.

C. DeMello in View of Schwartz and Walmsley Does Not Render Claim 10 Obvious

Petitioner asserts there is a motivation to combine DeMello, Schwartz and Walmsley to deduce a combined system as recited in claim 10. Pet. At 54-58. However, DeMello in View of Schwartz and Walmsley does not teach the limitations [10B], [10C] and [10D].

Petitioner has used hindsight to bridge the gaps in its argument. It is wrong to use the patent in suit as a guide through the maze of prior art references, combining the right references in the right way so as to achieve [a desired result]. *Orthopedic Equip. Co. v. United States*, 702 F.2d 1005, 1012, 217 USPQ 193, 199 (Fed. Cir. 1983).

2. Claim 11

Claim 11 contains all limitations of claim 1 and is not obvious over DeMello in View of Schwartz and Walmsley.

A. Schwarz and Walmsley would not have been combined with DeMello.

A POSITA would not have combined Schwarz and Walmsley with DeMello. Petitioner's arguments to combine miss the point of Schwarz and Walmsley, which are to authenticate malicious digital content in a chat program (Schwarz) or the identity of a malicious chip in a computer (Walmsley). DeMello, and the '102 Patent, on the other hand, relate to authenticating a user, not the digital content itself. The content in both DeMello and the '102 Patent is not questioned nor in need of authentication. Although the combination has related technology of authenticating something, the technology of the supporting references would not be used for authenticating the user, since neither of the supporting references use digital keys held or used by an end-user.

VI. CONCLUSION

For the foregoing reasons, Patent Owner respectfully requests that the Board deny institution of the Petition.

Dated: May 12, 2023

Respectfully submitted,



William P. Ramey, III
Ramey LLP
Registration No. 44,295
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
(713) 426-3923 (telephone)
(832) 900-4941 (fax)
uspto@rameyfirm.com
wramey@rameyfirm.com

Counsel for Patent Owner
LAURI VALJAKKA

CERTIFICATE OF SERVICE

I the undersigned, counsel with the law firm of Ramey LLP, hereby certify that the following statements are true and correct under penalty of perjury, pursuant to 28 U.S.C. § 1746:

On May 12, 2023, this PATENT OWNER LAURI VALJAKKA PRELIMINARY RESPONSE TO PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 10,726,102 were served via email to the addresses below:

Lead Counsel

Lori A. Gordon
Perkins Coie LLP
700 Thirteenth Street, N.W., Suite 800
Washington, DC 2005-3960
Ph: 202/654-6200
Email: gordon-ptab@perkinscoie.com

Back-up Counsel

Jassiem Moore
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
Email: moore-ptab@perkinscoie.com

Dated: May 12, 2023

Respectfully submitted,



William P. Ramey, III
Ramey LLP
Registration No. 44,295
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
(713) 426-3923 (telephone)
(832) 900-4941 (fax)
uspto@rameyfirm.com
wramey@rameyfirm.com

Counsel for Patent Owner
LAURI VALJAKKA

CERTIFICATION OF WORD NUMBER

Counsel for Patent Owner hereby certifies that this PATENT OWNER LAURI VALJAKKA PRELIMINARY RESPONSE TO PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 10,726,102 contains 6,979 words as calculated using the word count function of Microsoft Word, not including material excluded under 37 C.F.R. 42.24(a)(1).

Dated: May 12, 2023

Respectfully submitted,



William P. Ramey, III
Ramey LLP
Registration No. 44,295
5020 Montrose Blvd., Suite 800
Houston, Texas 77006
(713) 426-3923 (telephone)
(832) 900-4941 (fax)
uspto@rameyfirm.com
wramey@rameyfirm.com

Counsel for Patent Owner
LAURI VALJAKKA