

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

Case No. IPR2023-00458
U.S. Patent No. 9,280,678

PATENT OWNER'S NOTICE OF APPEAL

Office of the General Counsel
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450

Notice is hereby given, pursuant to 37 C.F.R. § 90.2(a) and 35 U.S.C. §§ 141(c), 142, and 319, that Patent Owner Fortinet, Inc. (“Patent Owner”) appeals to the United States Court of Appeals for the Federal Circuit from the Final Written Decision of the Patent Trial and Appeal Board in Case No. IPR2023-00458, entered August 12, 2024 (Paper No. 29) (attached as Exhibit A). This notice is timely filed within 63 days of the issuance of the Final Written Decision. For the limited purpose of providing the Director with the information specified in 37 C.F.R. § 90.2(a)(3)(ii), Patent Owner indicates that the issues on appeal may include, but are not limited to, the following:

1. Whether the PTAB erred in finding that Petitioner has shown by a preponderance of the evidence that claims 1-3, 6, 8-17, and 21-27 of U.S. Patent No. 9,280,678 (“the ’678 Patent”) are unpatentable;
2. Whether the PTAB erred in finding that Petitioner has shown by a preponderance of the evidence that claims 1-3, 8-14, 16-17, and 21-27 of the ’678 Patent are unpatentable under 35 U.S.C. § 103 as obvious in view of U.S. Pat. App. Pub. No. 2014/0013112 A2 (“Cidon”), U.S. Pat. App. Pub. No. 2014/0359282 A1 (“Shikfa”), and U.S. Pat. App. Pub. No. 2003/0055994 A1 (“Herrmann”);
3. Whether the PTAB erred in finding that Petitioner has shown by a preponderance of the evidence that claim 6 of the ’678 Patent is unpatentable under 35 U.S.C. § 103 as obvious in view of Cidon, Shikfa, Hermann, and U.S. Pat. App. Pub. No. 2005/0010593 A1 (“Fellenstein”);

4. Whether the PTAB erred in finding that Petitioner has shown by a preponderance of the evidence that claim 15 of the '678 Patent is unpatentable under 35 U.S.C. § 103 as obvious in view of Cidon, Shikfa, Hermann, and U.S. Pat. No. 6,622,248 B1 ("Hirai");
5. Whether the PTAB erred in finding that Petitioner has shown by a preponderance of the evidence that claims 1-3, 8-17, and 21-27 of the '678 Patent are unpatentable under 35 U.S.C. § 103 as obvious in view of U.S. Pat. App. Pub. No. 2011/0119481 A1 ("Auradkar"), U.S. Pat. App. Pub. No. 2013/0159694 A1 ("Chiueh"), and U.S. Pat. App. Pub. No. 2014/0068030 A1 ("Chambers");
6. Whether the PTAB erred in finding that Petitioner has shown by a preponderance of the evidence that claim 6 of the '678 Patent is unpatentable under 35 U.S.C. § 103 as obvious in view of Auradkar, Chiueh, Chambers, and U.S. Pat. App. Pub. No. 2003/0063321 ("Inoue");
7. Whether the PTAB erred in all other prior interlocutory and underlying orders, decisions, rulings, findings and opinions decided adversely to Patent Owner, including procedural orders, discovery orders, or other findings and determinations.

Simultaneous with this submission and in accordance with 37 C.F.R. § 90.2(a), a copy of this Notice of Appeal is being filed with the Director of the United States Patent and Trademark Office, filed with the Patent Trial and Appeal Board, and served upon Petitioner in accordance with 37 C.F.R. § 42.6(e). In addition, this Notice of Appeal, along with the required docketing fees, is being filed with the Clerk's Office for the United States Court of Appeal for the Federal Circuit in accordance with Fed. Cir. R. 15(a)(1).

Respectfully submitted,

Dated: October 14, 2024

By: /s/ James M. Glass

James M. Glass
jimglass@quinnemanuel.com
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
51 Madison Ave, 22nd Floor
New York, New York 10010
Tel: (212) 849-7000
Fax: (212) 849-7100

Counsel for Patent Owner

CERTIFICATE OF FILING

The undersigned hereby certifies that, in addition to being filed electronically via PTAB P-TACTS, the foregoing document was filed by Express Mail on October 14, 2024, with the Director of the United States Patent and Trademark Office, at the following address:

Director of the United States Patent and Trademark Office
c/o Office of the General Counsel
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450.

CERTIFICATE OF FILING

The undersigned hereby certifies that a true and correct copy of the foregoing document was filed electronically by CM/ECF on October 14, 2024, with the Clerk's Office of the United States Court of Appeals for the Federal Circuit.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a copy of the foregoing document was served on October 14, 2024, by email at the following addresses:

millikan-ptab@perkinscoie.com

tehranchi-ptab@perkinscoie.com

yuan-ptab@perkinscoie.com

Netskope-FortinetIPRTeam@perkinscoie.com

Dated: October 14, 2024

By: /s/ James M. Glass
James M. Glass
jimglass@quinnemanuel.com
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
51 Madison Ave, 22nd Floor
New York, New York 10010
Tel: (212) 849-7000
Fax: (212) 849-7100

Counsel for Patent Owner

EXHIBIT A

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

IPR2023-00458
Patent 9,280,678 B2

Before JAMES P. CALVE, THOMAS L. GIANNETTI, and
STEPHEN E. BELISLE, *Administrative Patent Judges*.

CALVE, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. BACKGROUND

Netskope, Inc. (“Petitioner”) filed a petition requesting *inter partes* review of claims 1–3, 6, 8–17, and 21–27 (the “challenged claims”) of U.S. Patent No. 9,280,678 B2 (“the ’678 patent”) (Ex. 1001). Paper 2 (“Pet.”), 1. Fortinet, Inc. (“Patent Owner”) timely filed a Preliminary Response. Paper 6. Applying the standard in 35 U.S.C. § 314(a), we instituted an *inter partes* review of all challenged claims on all grounds asserted in the Petition. Paper 10.

After we instituted trial, Patent Owner filed a Patent Owner Response. Paper 15 (“PO Resp.”). Petitioner filed a Reply to Patent Owner’s Response. Paper 19 (“Reply”). Patent Owner filed a Sur-reply to Petitioner’s Reply. Paper 24 (“Sur-reply”).

An oral hearing was held on June 21, 2024, and a copy of the transcript was entered in the record. Paper 28 (“Tr.”).

We have jurisdiction pursuant to 35 U.S.C. § 6. This Decision is a Final Written Decision under 35 U.S.C. § 318(a) (2018) and 37 C.F.R. § 42.73 (2020) as to the patentability of the claims on which we instituted trial. Petitioner bears the burden of proving unpatentability of the challenged claims. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). To prevail, Petitioner must prove unpatentability by a preponderance of the evidence. *See* 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d).

For reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–3, 6, 8–17, and 21–27 of the ’678 patent are unpatentable.

A. Related Proceedings

The parties identify the following proceeding involving the '678 patent: *Netskope, Inc. v. Fortinet, Inc.*, No. 3:22-cv-01852-TLT (N.D. Cal.). Pet. 5; Paper 3 (Patent Owner's Mandatory Notices), 2. Petitioner identifies the following *inter partes* reviews that challenge other patents of Patent Owner: IPR2022-01587, IPR2023-00030, IPR2023-00175, IPR2023-00456, IPR2023-00457, and IPR2023-00459. Pet. 5.

B. Real Parties in Interest

Petitioner identifies Netskope, Inc. as the real party in interest. Pet. 5. Patent Owner identifies Fortinet, Inc. as the real party in interest. Paper 3, 2.

C. The '678 Patent

The '678 patent describes systems that operatively couple users 102 with cloud service providers as shown in Figure 2, reproduced below.

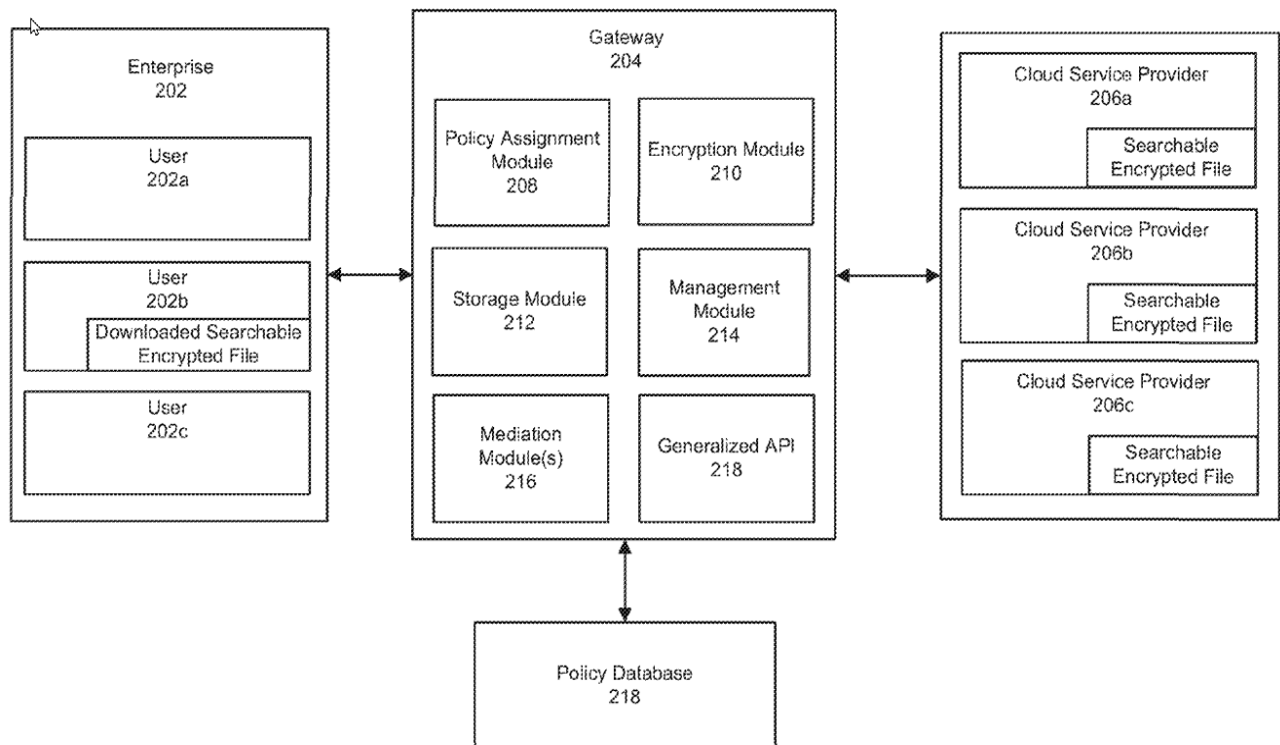


Fig. 2

Figure 2 depicts modules for encrypting, storing, accessing, and managing data on cloud platforms. Ex. 1001, 3:25–28, 8:27–41. Policy assignment module 208 assigns policies to users 202 based on roles, responsibilities, and enterprise practices. *Id.* at 9:11–19. A policy can define how files are uploaded, stored, downloaded, searched, and processed by a cloud platform and how users 202 access data stored on cloud platforms. *Id.* at 9:19–26. Encryption module 210 encrypts files uploaded to a cloud platform based on policies that are assigned by policy assignment module 208. *Id.* at 9:53–56. Gateway 204 shares encryption/decryption keys. *Id.* at 9:61–67.

D. Challenged Claims

Claims 1 and 16 are independent. Claims 2, 3, 6 and 8–15 depend from claim 1. Claims 17 and 21–27 depend from claim 16. Claim 1 is reproduced below with Petitioner’s annotations. Pet. 140 (claim listing).

1[pre] A method comprising:

1[a][i] assigning to one or more users, by a gateway device, a policy for managing access to and processing a file to be stored on one or more cloud platforms, *1[a][ii]* wherein the policy defines access rights of the one or more users;

1[b] encrypting, by the gateway device, using cryptographic key information defined by the policy, content of the file to produce a searchable encrypted file by:

1[b][i] dividing the file into a plurality of chunks;

1[b][ii] creating namespaces for one or more of the plurality of chunks; and

1[b][iii] configuring the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable;

1[c] storing, by the gateway device, the searchable encrypted file on the one or more cloud platforms based on the policy; and

1[d] managing access to the searchable encrypted file by the one or more users based on the policy.

E. Asserted Grounds of Unpatentability

Ground	Challenged Claim(s) ¹	35 U.S.C. §	Reference(s)
1	1–3, 8–14, 16, 17, 21–27	103 ²	Cidon ³ , Shikfa ⁴ , Herrmann ⁵
2	6	103	Cidon, Shikfa, Herrmann, Fellenstein ⁶
3	15	103	Cidon, Shikfa, Herrmann, Hirai ⁷
4	1–3, 8–17, 21–27	103	Auradkar ⁸ , Chiueh ⁹ , Chambers ¹⁰
5	6	103	Auradkar, Chiueh, Chambers, Inoue ¹¹

Petitioner relies on Declarations of Dr. Wenke Lee. Exs. 1002, 1026.
Patent Owner relies on Declarations of Dr. John Black Jr. Exs. 2001, 2003.

¹ Petitioner lists claims 18–20 in Ground 1 and claims 18 and 19 in Ground 4 but presents no argument for those claims. Pet. 7, 15–69, 72–135. We deem this to be an inadvertent error in listing the challenged claims, and we need not and do not herein address these claims.

² The Leahy-Smith America Invents Act (“AIA”) revised 35 U.S.C. § 103 effective on March 16, 2013. Because the ’678 patent has an effective filing date after March 16, 2013, we use the AIA version of 35 U.S.C. § 103.

³ US 2014/0013112 A1, published Jan. 9, 2014 (Ex. 1004, “Cidon”).

⁴ US 2014/0359282 A1, published Dec. 4, 2014 (Ex. 1006, “Shikfa”).

⁵ US 2003/0055994 A1, published Mar. 20, 2003 (Ex. 1005, “Herrmann”).

⁶ US 2005/0010593 A1, published Jan. 13, 2005 (Ex. 1007, “Fellenstein”).

⁷ US 6,622,248 B1, issued Sept. 16, 2003 (Ex. 1008, “Hirai”).

⁸ US 2011/0119481 A1, published May 19, 2011 (Ex. 1009, “Auradkar”).

⁹ US 2013/0159694 A1, published June 20, 2013 (Ex. 1011, “Chiueh”).

¹⁰ US 2014/0068030 A1, published Mar. 6, 2014 (Ex. 1010, “Chambers”).

¹¹ US 2003/0063321 A1, published Apr. 3, 2003 (Ex. 1012, “Inoue”).

II. DISCUSSION

A. Level of Ordinary Skill in the Art

Petitioner asserts that a skilled artisan “would have had a B.S. in computer science, computer engineering, or electrical engineering, with at least two years’ experience in computer networking/security.” Pet. 15. Patent Owner asserts that a skilled artisan “would have had a Bachelor of Science degree in electrical engineering and/or computer science, and two years of work or research experience in the fields of network and data security, or a Master’s degree in electrical engineering and/or computer science and one year of work or research experience in related fields.” PO Resp. 16–17 (the positions in the PO Response would be the same under either parties’ proposal). The parties’ proposals are substantially the same. Our decision and analysis would be the same under either party’s proposal.

B. Claim Interpretation

We interpret the claims “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b).” 37 C.F.R. § 42.100(b). Under that standard, words of a claim are generally given their ordinary and customary meaning as understood by a person of ordinary skill in the art at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc). We construe the claims only to the extent necessary to reach our final written decision. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). The parties assert that no claim constructions are necessary but dispute the meaning of “namespace.” Pet. 15; PO Resp. 17.

1. “creating namespaces for one or more . . . chunks”

a. Petitioner’s contentions

Petitioner asserts that “[t]he plain meaning of ‘namespace’ should be ‘the set of names available for naming things.’” Reply 1 (citing Ex. 1002 ¶ 101 (quoting Ex. 1014 (Dictionary of Computer and Internet Terms))).

b. Patent Owner’s arguments

Patent Owner asserts that a “namespace” is “a set of names available within a particular context,” and it “defines *the set of allowable identifiers* within a particular context.” PO Resp. 18, 19. Patent Owner asserts that policies that define keys for encrypting chunks “create a namespace that defines the naming convention for the file chunks (*e.g.* encryption based on a particular key)” and “storing the file chunks in a folder creates a namespace scope for the file chunks.” *Id.* at 20. Patent Owner asserts that identifiers are names within a namespace rather than a namespace. *Id.* at 21.

c. Analysis

The ’678 patent describes storage containers as “directories, directory structures, web directories, folders, . . . files and namespaces of the same.” *Id.* at 6:44–47; *id.* at 10:12–15. However, it discloses that data is “stored in the namespaces, directories, folders, files or other storage containers of one or more cloud platforms,” which seems to equate namespaces with storage containers. *Id.* at 9:23–25. In claim 6, “the step of configuring the namespaces comprises storing content of the file as filenames.” *Id.* at 20:20–22. One definition of “namespace” is a “grouping of one or more names that represent individual objects within the group in a shared computing environment, such as a network.” *Microsoft Computer Dictionary, Fifth Edition* 130 (Microsoft Press 2002) (Ex. 3001).

“The names within a namespace are unique, are created according to the same rules, and can be resolved into a particular identifying item of information, such as an IP address or a network device.” Ex. 3001.

Petitioner asserts, “[t]he plain meaning of ‘namespace’ should be ‘the set of names available for naming things.’” Reply 1 (citing Ex. 1002 ¶ 101; Ex. 1014 (Dictionary of Computer and Internet Terms)); Tr. 5:18–20, 7:21–8:1. This definition is consistent with the extrinsic evidence cited above.

Patent Owner largely agrees with this proposed definition. Dr. Black testifies that “to the extent a namespace is applied to object identifiers, it will define *the set of allowable identifiers* within a particular context.” Ex. 2003 ¶ 69 (cited in PO Resp. 19). Dr. Black agrees with Dr. Lee’s testimony “that a directory named ‘documents’ is a namespace for the files within that directory—within that ‘documents’ namespace, files can be identified by simply referring to the file name, such as ‘foo.’” *Id.* ¶ 68. Patent Owner however, asserts that “a name itself (such as an identifier that identifies an object) is *not* a namespace.” PO Resp. 19.

Patent Owner asserts that the ’678 patent provides “an example of creating a namespace for file chunks as part of the encryption process” as “each chunk can be encrypted based on public and private/secret keys defined by the encryption module 210” “where keys are managed based on user-assigned policies.” PO Resp. 20. Patent Owner asserts that “[t]hese policies therefore create a namespace that defines the naming convention for the file chunks (*e.g.* encryption based on a particular key).” *Id.* Patent Owner asserts that “storing the file chunks in a folder creates a namespace scope for the file chunks” and namespaces are configured by storing file content as file names. *Id.* (citing Ex. 2003 ¶ 71); *see* Tr. 8:5–11, 11:2–12:11.

d. Conclusion

In view of the foregoing, we adopt Petitioner’s proposed interpretation of “namespace” as “a set of names available for naming things.” Consistent with various exemplary embodiments described in the ’678 patent, the set of names available for naming things may be based on a policy that defines the naming convention for files or file chunks, and a namespace may be created by storing files or file chunks in a folder to create a namespace scope for the files or file chunks.

2. “the file is stored across two or more cloud platforms”

Neither party proposes a formal claim construction of this limitation in claims 11 and 25, but they disagree over whether Cidon’s backup and/or synchronization of a complete file on or between multiple storage services stores a file “across two or more cloud platforms” as recited in claims 11 and 25. Pet. 58–59; PO Resp. 41–42.

a. Petitioner’s contentions

Petitioner asserts that a skilled artisan would understand that backing up and/or synchronizing a file on or between storage services stores the file across two or more cloud platforms. Pet. 59. Dr. Lee testifies that archiving and backing up files to storage services and synchronizing files between multiple services is an example of storing files in more than one cloud service or platform and storing the file across two or more cloud platforms as recited in claims 11 and 25 of the ’678 patent. Ex. 1002 ¶ 137.

b. Patent Owner’s arguments

Patent Owner argues that storing a file across two or more cloud platforms requires the file to be divided into chunks and each chunk to be stored on a different cloud store. PO Resp. 41 (citing Ex. 1001, 7:43–45).

Dr. Black testifies that the plain meaning of storing “across” multiple platforms is that a single file has different parts stored on different platforms. Ex. 2003 ¶ 116. Dr. Black supports his opinion by citing the ’678 patent’s disclosure “[c]lients may also store such content across two or more stores 114 such that the content *is divided into multiple chunks and each chunk is stored on a different cloud store* 114.” *Id.* (citing Ex. 1001, 7:43–45).

c. Analysis

The ’678 patent provides the following description:

Clients 102 may store one or more files, directories, metadata, or parts thereof across one or more cloud stores 114. Clients may also store such content across two or more stores 114 such that the content is divided into multiple chunks and each chunk is stored on a different cloud store 114.

Ex. 1001, 7:41–45. This description indicates that a file(s) can be stored across (on) a single cloud store 114, or a file(s) can be stored across (on) multiple cloud stores. *Id.* at 7:41–42. There is no indication in this description or in the subject limitation itself that a file *must* be divided into parts in order to be stored *across* one or more cloud stores 114. *Id.*

The ’678 patent reinforces our understanding by disclosing a specific embodiment in which a file is divided into chunks and the chunks are stored in different cloud stores. The ’678 patent discloses that clients can *divide* content such as files into *multiple chunks* and “each chunk is stored on a different cloud store 114.” Ex. 1001, 7:43–45. Claims 11 and 25, however, do not recite storing file chunks or parts of files on different cloud platforms of the two or more cloud platforms. Claims 1 and 16, from which claims 11 and 25 depend, recite a step of dividing the file into a plurality of chunks. Ex. 1001, 19:65, 20:65.

Even though claims 1 and 16 recite steps of dividing the file into chunks, claims 11 and 25 recite that *the file* is stored across two or more cloud platforms rather than only the plurality of chunks in claims 1 and 16 are stored in different cloud platforms. Merely that a file is stored across two or more cloud platforms does not require each chunk of the file to be stored in different cloud platforms.

We do not credit Dr. Black’s testimony because Dr. Black relies on the embodiment that divides a file into chunks and stores each chunk on a different cloud store, but claims 11 and 25 are not limited to this one embodiment. Ex. 2003 ¶ 116; Ex. 1001, 7:43–45. We decline to limit claims 11 and 25 to a particular embodiment when the claim language is broader than that embodiment. Nor do we interpret the term “across” in claims 11 and 25 to limit the claims to an embodiment in the ’678 patent specification in which a file is divided into chunks with each chunk stored on a different cloud store absent a disavowal or definition, neither of which are asserted here. Ex. 1001, 7:43–45. *See Phillips*, 415 F.3d at 1316.

d. *Conclusion*

We interpret “a file is stored across two or more cloud platforms” to encompass the entire file being stored on two or more cloud platforms (e.g., the entire file being stored on one cloud platform and the entire file being stored on another cloud platform). We need not construe this limitation any further to resolve the controversy between the parties. *See Nidec Motor*, 868 F.3d at 1017 (stating that “we need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

C. Principles of Law

A patent claim is unpatentable “if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains.” 35 U.S.C. § 103. “The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). Similarly, “if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.” *Id.* at 417. Often, it will be necessary for courts to consider the interrelated teachings of multiple patents, the effects of demands known to the design community or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art to determine whether there was any apparent reason to combine the known elements in the manner claimed by the patent at issue. *Id.* at 418.

The question of obviousness is resolved based on 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 ordinary skill in the art; and (4) when in evidence, objective evidence of non-obviousness such as commercial success, long felt but unsolved needs, and failure of others. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Neither party has presented any objective evidence of non-obviousness.

D. Ground 1: Obviousness Over Cidon, Shikfa, Herrmann

Petitioner asserts unpatentability of claims 1–3, 8–14, 16, 17, and 21–27 under 35 U.S.C. § 103 over the combination of Cidon, Shikfa, and Herrmann. Pet. 15–69.¹²

1. Cidon

Cidon discloses management server 100 that stores encrypted files in segments using policies for file placement, access, and sharing as shown in Figure 2, reproduced below. Ex. 1004 ¶¶ 10, 102, 108, 206–212, 221–223.

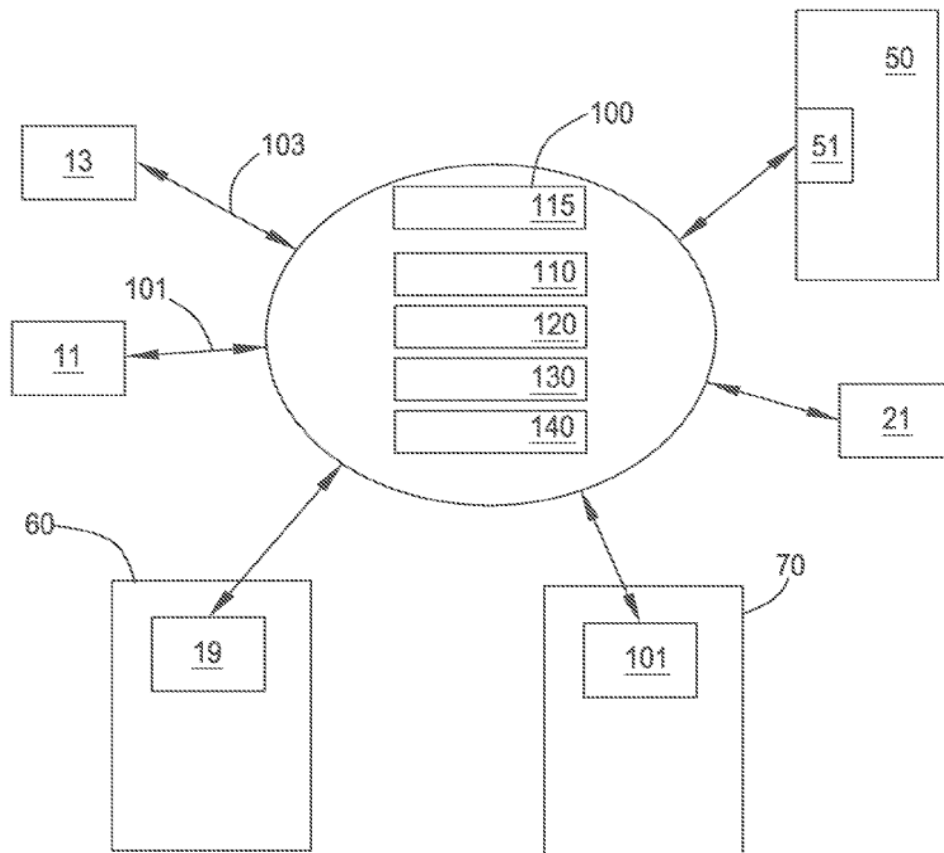


FIG. 2

¹² Petitioner lists claims 1–3, 8–14, and 16–27 as the challenged claims in Ground 1 (Pet. 15) but provides no substantive argument for claims 18–20 (*id.* at 15–69). *Id.* at 5 (seeking to cancel claims 1–3, 6, 8–17, and 21–27).

Figure 2 depicts management server 100 that encrypts cloud files and controls access to the files by providing decryption keys. Ex. 1004 ¶ 102. System metadata module 115 manages file metadata. *Id.* ¶¶ 105, 106. IP Policy Enforcement Module 120 allows administrators to organize users into groups and assign different access policies to each group. *Id.* ¶ 108. Data Manager and Login Module 130 processes requests to access a secure file. *Id.* ¶ 109. Encryption Key Manager 140 generates, stores, and retrieves encryption keys. *Id.* ¶ 110. The policies may specify the placement of files in specific directories, access and sharing permissions, copy control, and encryption. *Id.* ¶¶ 206–212. Files may be segmented, and each segment may be encrypted and stored. *Id.* ¶¶ 305, 309, 383, Fig. 13.

2. Shikfa

Shikfa's broker system encrypts and searches encrypted documents using encryption keys and indexes as shown in Figure 2, reproduced below.

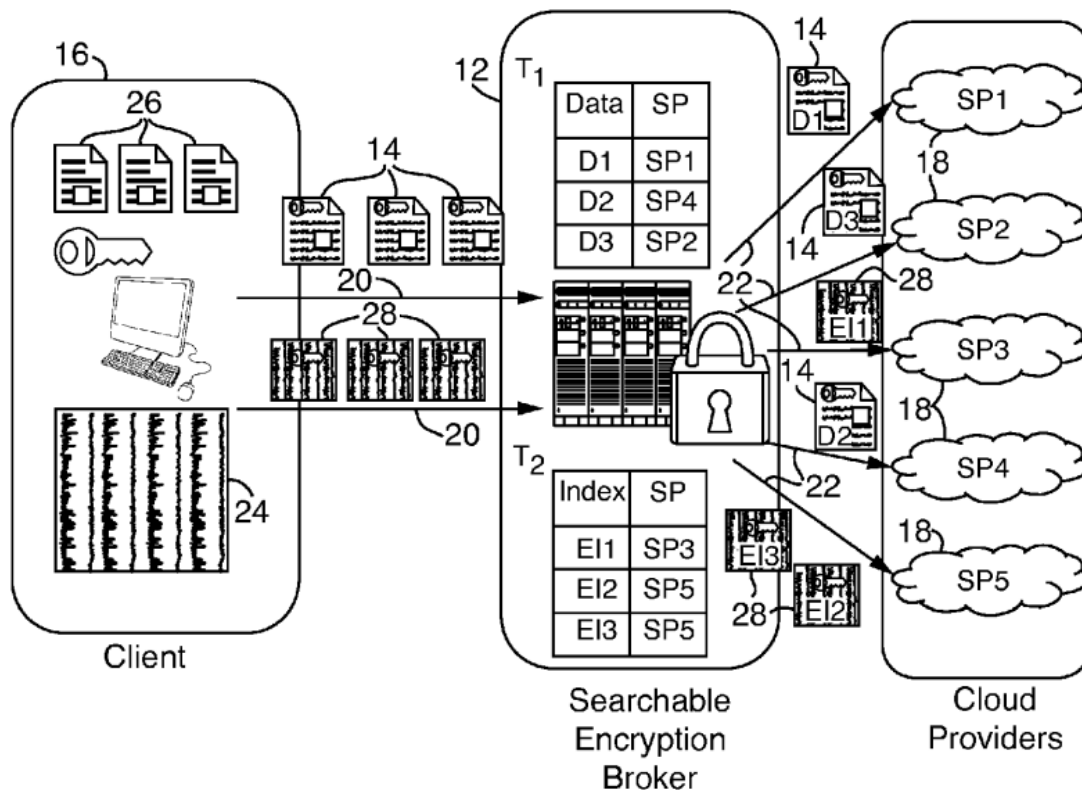


Figure 2 of Shikfa depicts a broker system for searchable encryption. Client 16 encrypts documents 26, generates indexes 24 for documents 26, encrypts indexes 24, and stores encrypted documents and indexes in cloud storage providers 18. Ex. 1006 ¶¶ 3, 10, 12, 29. Broker server 12 receives encrypted documents 14, encrypted indexes 28, and encryption information and generates a translation table T1 to identify which encrypted document 14 is stored on which cloud storage provider 18. *Id.* ¶¶ 31, 32. Index 28 includes keywords for encrypted documents 14 and pointers to documents containing the keywords. *Id.* ¶ 29. Broker server 12 may store encrypted indexes 28 locally or send them to cloud storage providers 18. *Id.* ¶ 32.

To search for encrypted document 14 that contains certain keywords, client 16 generates encrypted search query 30 for the keywords using the searchable encryption mechanism that encrypted indexes 28 and sends the encrypted query 30 to broker server 12. Ex. 1006 ¶ 34. Broker server 12 uses the searchable encryption mechanism that was used to encrypt query 30 and to encrypt indexes 28 as input to identify (via identifiers D1, D2, D3) encrypted documents 14 that satisfy the encrypted search query. *Id.* ¶¶ 34–36. Broker server 12 thereby allows clients 16 to store secure, encrypted documents 14 on cloud storage providers 18 and also provides searchable encryption so clients 16 can search and retrieve encrypted documents by using translation tables T1, T2 or encrypted indexes 28. *Id.* ¶ 37.

3. *Herrmann*

Herrmann uses gateway server 350 to control access of clients 310 to protected data 390 by verifying access is allowed. Ex. 1005 ¶ 60. Gateway server 350 grants access when integrity server 370 indicates that access is permitted under an applicable policy for client computer 310. *Id.* ¶¶ 60, 67.

4. *Motivation to combine*

a. *Petitioner's contentions*

Petitioner contends that a skilled artisan would have implemented Cidon's searchable encryption procedure on Herrmann's gateway and improved Cidon's search methodology with Shikfa's teachings to improve Cidon's ability to search encrypted documents. Pet. 21–22 (citing Ex. 1004 ¶ 100; Ex. 1005, Abstr.; Ex. 1006 ¶ 3; Ex. 1002 ¶¶ 67, 68). Petitioner asserts that Shikfa's search mechanism would enhance Cidon by “allowing a chunk-by-chunk search of encrypted documents stored on cloud storage that had no search capability.” *Id.* at 22 (citing Ex. 1004 ¶¶ 91, 166, 171; Ex. 1006 ¶ 2). Petitioner also asserts that Cidon and Herrmann would increase flexibility by using different access policies for users, and using Herrmann's gateway in Cidon's system would allow automatic policy assignment that improved efficiency and reduced human errors in assigning policies. *Id.* (citing Ex. 1004 ¶ 106; Ex. 1005 ¶¶ 50, 77; Ex. 1002 ¶ 69); *id.* at 28 (element 1[a][i]).

b. *Patent Owner's arguments*

Patent Owner does not contest these general motivations to combine the teachings of Cidon, Shikfa, and Herrmann. We address Patent Owner's specific arguments in Section II.D.5.h. below. *See* PO Resp. 28–30.

c. *Conclusion*

We determine the combination of familiar elements in Cidon, Shikfa, and Herrmann according to known methods would have yielded predictable results that improved Cidon's system. *KSR*, 550 U.S. at 416, 417; *see also DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1368 (Fed. Cir. 2006) (an implicit motivation to combine exists when an “improvement” makes a product faster or more efficient).

5. *Independent Claim 1*

a. *1[pre]: “A method comprising:”*

(1) *Petitioner’s contentions*

Petitioner asserts that Cidon discloses a method for encrypting files by segmenting the file, encrypting each file segment, and sending the encrypted segments to a storage service. Pet. 23 (citing Ex. 1004 ¶¶ 10, 309, Fig. 15).

(2) *Patent Owner’s arguments*

Patent Owner does not contest Petitioner’s assertions that Cidon discloses element 1[pre]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties’ contentions and record evidence, we determine that Cidon discloses element 1[pre] and we adopt Petitioner’s contentions.

b. *1[a][i]: “assigning to one or more users, by a gateway device, a policy for managing access to and processing a file to be stored on one or more cloud platforms”*

(1) *Petitioner’s contentions*

Petitioner asserts that Cidon’s management server 100 implements access policies for users and processes files to be stored on cloud platforms where they can be accessed. Pet. 24 (citing Ex. 1004 ¶¶ 99, 100, Fig. 2). Petitioner asserts that Cidon’s management server 100 defines and enforces access policy configurations for secure file access and allows IT departments to provide different access policies for secure files for different users and user groups. *Id.* at 25 (citing Ex. 1004 ¶¶ 102, 108; Ex. 1002 ¶¶ 74–79). Petitioner asserts that Cidon allowed administrators to define access policies through a web browser interface, and the policies for processing a file could dictate whether files were encrypted. *Id.* (citing Ex. 1004 ¶¶ 108, 224, 227).

Petitioner contends that Herrmann’s gateway server 350 verifies client computer 310 is authorized to access data 390 and assigns an access policy to client computer 310 based on policy specification 373 that is applicable to client computer 310 and is maintained in policy store 371 of integrity server 370 of gateway server 350 for users, group, or computers. Pet. 26–27 (citing Ex. 1005 ¶¶ 60, 67, 77, claim 16, Fig. 3; Ex. 1002 ¶ 79).

Petitioner asserts that a skilled artisan would have combined Herrmann’s gateway server and access policy assignment functionality with Cidon’s management server to assign access policies and accept access requests, and “the modified system would have allowed automatic policy assignment and implementation, improving system efficiencies,” and “would have allowed better real-time protection.” Pet. 27–28 (citing Ex. 1004, claim 21, Fig. 2; Ex. 1005 ¶¶ 60, 77; Ex. 1002 ¶¶ 80, 81). Petitioner asserts that gateways provide well-known network security functionalities, and Herrmann’s gateway server performed other functions using its integrity server. *Id.* at 28–29 (citing Ex. 1005 ¶¶ 18, 65, 66, 77, 82; Ex. 1002 ¶ 82).

(2) *Patent Owner’s arguments*

Patent Owner argues that Cidon lacks a policy for managing access to and processing a file to be stored on cloud platforms. PO Resp. 31. Patent Owner argues that Petitioner fails to show that Cidon processes files with a *user*-assigned policy because “Petitioner relies exclusively on an ‘encryption policy’ disclosed in Cidon’s paragraphs 224 and 227.” *Id.* Patent Owner argues that “Cidon’s encryption policy is assigned to a ‘*specific file*,’ not a user.” *Id.* at 32 (“The context of Cidon’s disclosure also makes clear that an encryption policy, as part of placement policies, is ‘*defined on documents*’ as a result of a file’s ancestry tree, not assigned to users.”).

(3) *Analysis*

We find that Cidon’s management server 100 assigns a policy to users and manages users’ access to, and processing of, secure files stored in cloud storage by encrypting the files and by providing the right decryption keys to users to access and process such files according to the policy and according to application interfaces (APIs) defined by the policy. Ex. 1004 ¶¶ 102, 108. The policy determines how management server 100 processes and controls access to files stored in the cloud and how users access and process such files using decryption keys and APIs defined by the single policy. *Id.* ¶ 102.

IT Policy Enforcement Module 120 of management server 100 allows IT departments to define different access and encryption policies for users and groups to access and process files on cloud platforms. Ex. 1004 ¶ 108.

These disclosures refute Patent Owner’s argument that the encryption policy is not assigned to a user and does not govern access management and file processing. PO Resp. 31, 35–38. Cidon also discloses that a user-based encryption may be applied to sensitive documents and corporate folders, and user devices may connect to web storage and *upload* encrypted files through a client interface enabled by the management server. Ex. 1004 ¶¶ 219–221.

Therefore, we disagree with the argument that Cidon does not disclose a policy for processing files because Cidon’s encryption policy applies only to uploaded files. PO Resp. 35. Cidon’s management server also processes “a file to be stored on one or more cloud platforms” in element 1[a][i] by encrypting and storing the files based on user-specific access and encryption policies. Ex. 1004 ¶¶ 102–117. When cloud files are encrypted, encrypted files are restored/stored based on the policy that controls how users access and process the encrypted file in the future. *Id.* ¶¶ 102–117, 309–317.

(4) *Conclusion*

Based on the parties' contentions and record evidence, we agree with and adopt Petitioner's analysis and determine that the combination of Cidon and Herrmann discloses or suggests element 1[a][i].

c. *1[a][ii]: "wherein the policy defines access rights of the one or more users"*

(1) *Petitioner's contentions*

Petitioner contends that Cidon's management server creates policies that define access rights of one or more users and provides access policy configuration for secure file access. Pet. 29 (citing Ex. 1004 ¶¶ 102, 108, 112, 115). Petitioner asserts that Herrmann corroborates Cidon's teachings by explaining that its file and data access policy could be assigned "by user or by group." *Id.* (citing Ex. 1005 ¶ 67; element 1[a][i]; Ex. 1002 ¶ 83).

(2) *Patent Owner's arguments*

Patent Owner does not contest the assertions that Cidon and Herrmann disclose or suggest element 1[a][ii]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and record evidence, we agree with and adopt Petitioner's analysis and determine that the combination of Cidon and Herrmann discloses or suggests element 1[a][ii].

d. *1[b]: "encrypting, by the gateway device, using cryptographic key information defined by the policy, content of the file to produce a searchable encrypted file by:"*

(1) *Petitioner's contentions*

Petitioner asserts a skilled artisan would have combined Herrmann's gateway server and Cidon's management server to conduct the claimed operations at a gateway. Pet. 29 (citing element 1[a][i]; Ex. 1002 ¶¶ 84–91).

Petitioner asserts that the Cidon-Herrmann gateway has functionality of Cidon's management server that encrypts the contents of a file to produce multiple encrypted file segments that form an encrypted file in the cloud. Pet. 29–32 (citing Ex. 1004 ¶¶ 102, 166, 171, 222, 303–305, 309, 337, Figs. 13, 15; Ex. 1002 ¶¶ 84–91). Petitioner asserts that Cidon teaches or suggests that a user could access the encrypted user file by browsing the web service account with an API that could be programmed with functionalities such as document search, and Cidon's management server extracted metadata from uploaded files to help in file search operations using text/tag-based searches. *Id.* at 32 (citing Ex. 1004 ¶¶ 91, 166, 171; Ex. 1002 ¶ 88).

Petitioner asserts that the '678 patent describes a policy that defines encryption keys, decryption keys, and encryption types for encrypting data, and Cidon uses different encryption parameters to encrypt files for different, specific users. Pet. 33 (citing Ex. 1001, 4:4–7; Ex. 1004 ¶¶ 324, 326; Ex. 1002 ¶ 89). Petitioner contends that a skilled artisan would have found it obvious that Cidon's encryption parameters would include “cryptographic key information” as claimed because encryption keys are a common, well-known encryption parameter used to encrypt a file, and Cidon's encryption parameters and cryptographic key information were part of access policies assigned to different users or groups. *Id.* at 33–34 (citing Ex. 1004 ¶¶ 108, 207, 208, 212, 324, 326; Ex. 1001, 4:4–7, 10:1–3; Ex. 1002 ¶¶ 90, 91).

(2) *Patent Owner's arguments*

Patent Owner argues that the policy is a single policy that also defines cryptographic key information such that “*a* policy must perform *both* the ‘managing’ *and* ‘processing’ steps, as well as defining ‘cryptographic key information.’” PO Resp. 37.

(3) *Analysis*

As discussed in Section II.D.5.b. *supra*, Cidon’s management server 100 allows IT departments to define user-specific access policies that control encryption schemes and keys for files to be stored in the cloud and enforce the access rights for the users and groups. Ex. 1004 ¶¶ 10, 43, 99–102, 108, 110, 116, 207–227, 237, 309. Each policy defines how files are processed (encrypted and stored) and how users access the secure files. *Id.* Encryption may differ by specific users and user groups. *Id.* ¶¶ 324, 326; Ex. 1002 ¶ 91.

(4) *Conclusion*

Based on the parties’ contentions and record evidence, we agree with and adopt Petitioner’s analysis and determine that the combination of Cidon and Herrmann discloses or suggests element 1[b].

e. 1[b][i]: “dividing the file into a plurality of chunks”

(1) *Petitioner’s contentions*

Petitioner asserts that Cidon divides a file into segments in Figure 13 in which file 1410 is divided into segments 1430 and Figure 15 in which files are retrieved from a storage service (step 1610), divided into multiple segments (step 1620), encrypted in segments using encryption keys (step 1640), and the encrypted segments are sent to the storage service (step 1650). Pet. 34–36 (citing Ex. 1004 ¶¶ 35, 305, 309, Abstr., Figs. 13, 15).

(2) *Patent Owner’s arguments*

Patent Owner does not contest Petitioner’s assertions that Cidon discloses element 1[b][i]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties’ contentions and record evidence, we agree with and adopt Petitioner’s analysis and determine that Cidon discloses or suggests element 1[b][i].

f. 1[b][ii]: “creating namespaces for one or more of the plurality of chunks; and”

(1) Petitioner’s contentions

Petitioner asserts that Cidon creates namespaces for one or more of the plurality of chunks in element 1[b][ii] by calculating a unique file segment identifier (or signature) for each file segment or chunk based on the content of a file segment using Secure Hash Algorithm 2 (SHA2) signature computation. Pet. 36–38 (citing Ex. 1004 ¶¶ 305, 309, 383, Figs. 13, 15). Petitioner asserts that a skilled artisan would have understood that segment identifiers calculated by using a SHA2 signature algorithm identified the corresponding segments, and Cidon assigned the calculated segment identifiers to the file segments. *Id.* at 38–39 (citing Ex. 1004 ¶¶ 106, 305, 309, Figs. 13, 15; Ex. 1002 ¶ 96). Petitioner asserts that a skilled artisan would have found it obvious that Cidon’s segment identifiers constituted “namespaces” because they were “the set of names available for naming” corresponding file segments consistent with the plain and ordinary meaning of this term. *Id.* at 39–40 (citing Ex. 1014; Ex. 1002 ¶ 98).

(2) Patent Owner’s arguments

Patent Owner argues, “Petitioner’s assertion that creating an identifier to assign to a file chunk meets the ‘creating namespaces’ limitation fails because an identifier is not a namespace.” PO Resp. 23. Patent Owner asserts that under Petitioner’s definition of namespace as “the set of names available for naming,” creating a namespace must involve the creation of the set of available names, and an identifier is a single name in a set of names. *Id.*; Ex. 2003 ¶ 77. Patent Owner asserts that the creation of the identifiers within the namespace is not a creation of the namespace itself. PO Resp. 23–24; Ex. 2003 ¶ 77.

(3) *Analysis*

We find that Cidon “creat[es] namespaces for one or more of the plurality of chunks” in element 1[b][ii] by defining a *namespace naming convention* that uses a SHA2 algorithm to calculate signatures as unique identifiers for each file chunk based on its content and encrypts these file segment identifiers with cryptographic keys based on user-assigned policies. Ex. 1004 ¶¶ 305, 383. This namespace “defines a set of allowable identifiers within a particular context” using SHA2 signatures and encryption similar to Patent Owner’s examples of creating a namespace. *See* PO Resp. 19–20.

Dr. Lee testifies that Cidon creates a namespace naming convention that calculates unique file segment identifiers (file segment signatures) using an SHA2 signature computation algorithm on each segment and encrypts the file segment identifiers. Dr. Lee testifies that this namespace provides a set of names available for naming file segments as unique identifiers to assign to each file segment to identify them uniquely. Ex. 1002 ¶¶ 94–98 (citing Ex. 1004 ¶¶ 106, 305, 309, 383, Figs. 13, 15; Ex. 1014); Pet. 36–40.

Dr. Lee’s testimony is consistent with Patent Owner’s arguments that policies that define keys for encrypting chunks “create a namespace that defines the naming convention for the file chunks (*e.g.* encryption based on a particular key).” PO Resp. 20. Cidon defines a naming convention for file chunks using a SHA2 signature algorithm and encryption. Ex. 1004 ¶¶ 305, 383. After Cidon calculates file segment identifiers using a SHA2 signature algorithm, identifiers and segments are encrypted with encryption keys for the file segment SHA2 signature and stored in a service. Ex. 1004 ¶ 305–309; Tr. 8:5–11. Patent Owner also asserts that “storing the file chunks in a folder creates a namespace scope for the file chunks.” PO Resp. 20.

Creating and encrypted segment identifiers for segments using a SHA2 signature algorithm and assigned key evidences that a namespace/policy was created for the chunks. Patent Owner recognizes as much by asserting “the identifier is at best a name *within* the namespace (*i.e. the set of SHA2 signatures*)” (*id.* at 24 (emphasis added)). Reply 6–8. Dr. Black also agrees that SHA2 signatures create a namespace. Ex. 2003 ¶ 77.

(4) *Conclusion*

Based on the parties’ contentions and record evidence, we determine that Cidon discloses or suggests element 1[b][ii].

- g. 1[b][iii]: “*configuring the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable;*”

(1) *Petitioner’s contentions*

Petitioner asserts that Cidon creates files as searchable encrypted files with segment identifiers, and Shikfa generates indexes of pointers/identifiers of documents 26 to allow search and retrieval of encrypted file segments of encrypted documents 14. Pet. 40–41 (citing Ex. 1006 ¶ 29, Fig. 2; Ex. 1002 ¶¶ 99–107). Petitioner asserts that pointers and identifiers are index fields that identify an encrypted document and provide a namespace to identify it. *Id.* at 41–42 (citing Ex. 1006 ¶¶ 29, 31, Fig. 2; Ex. 1002 ¶ 101; Ex. 1014).

Petitioner asserts that Shikfa’s identifiers stored in a translation table T1 are configured to allow encrypted documents to be searched when broker server 12 uses encrypted indexes 20 to search and return identifiers D1, D2, D3 that satisfy encrypted query 30, and translation table T1 is used to look up the identifier and retrieve the corresponding encrypted document 14 from storage providers 18 by mapping search keywords and encrypted documents. Pet. 42–43 (citing Ex. 1006 ¶¶ 31, 36, Figs. 2, 3; Ex. 1002 ¶ 103).

Petitioner asserts that a skilled artisan would have combined Shikfa's searchable encryption mechanism with Cidon's encryption technique that divided content into segments/chunks and created a segment identifier for each chunk (1) to allow file content to be encrypted and searched without requiring such capability at a storage provider thereby allowing storage of files on cloud storages that did not have search capabilities, and (2) to provide document searchability while protecting confidential information. Pet. 43–44 (citing Ex. 1006 ¶¶ 39, 50; Ex. 1002 ¶ 105). Petitioner asserts that Shikfa's identifiers would have allowed Cidon's system to search and locate files on a segment-by-segment basis on Herrmann's gateway server. *Id.* at 44–45 (citing Ex. 1004, Fig. 13; Ex. 1002 ¶ 106).

(2) *Patent Owner's arguments*

Patent Owner argues that Shikfa's encrypted index mapping keywords to pointers/identifiers and encrypted documents is not “configuring the namespaces” because identifiers are not namespaces. PO Resp. 25. Patent Owner asserts that “[a] namespace defines the set of names available within a particular context” and “an identifier is simply a single item within the set of allowed names It does not define the set of allowable names.” *Id.* at 26. Patent Owner argues that “Shikfa's use of identifiers within an index has no bearing on or relationship to the manner in which a file is encrypted [because] Shikfa is quite clear that its index is created *before* a document is encrypted . . . [and] Shikfa states that the document is encrypted ‘using any desired encryption mechanism known in the art.’” PO Resp. 27. Patent Owner asserts that the '678 patent describes a process where an encrypted index is embedded into the encrypted file by using the encrypted keywords as filenames for the file's chunks. *Id.* at 27–28.

(3) *Analysis*

As discussed in Section II.D.5.f. *supra*, Cidon creates a namespace as encrypted SHA2 signatures of file content, and Shikfa configures this namespace by saving chunks in the namespace with indexes mapping the identifiers to documents having the keywords so the file is encrypted in a manner that makes it searchable and retrievable by the indexed identifiers. Pet. 44–45; Reply 11–12; Ex. 1006 ¶¶ 29–36, Figs. 2, 3; *see* Tr. 43:20–23 (namespace is configured by placing encrypted chunks into the namespace). Indexes are searchable to identify and retrieve encrypted documents using keywords. Ex. 1006 ¶¶ 29–36, Figs. 2, 3; Pet. 40–43 (Shikfa’s identifiers allow searches of encrypted content by mapping keywords to documents).

(4) *Conclusion*

Based on the parties’ contentions and record evidence, we agree with and adopt Petitioner’s analysis and determine that the combination of Cidon, Herrmann, and Shikfa discloses or suggests element 1[b][iii].

h. Motivation to combine Shikfa with Cidon-Herrmann

(1) *Petitioner’s contentions*

Petitioner asserts that a skilled artisan would have combined Shikfa’s searchable encryption of documents with Cidon’s encryption of document chunks and created chunk identifiers to enable searches of encrypted chunks. Pet. 43–44. Petitioner asserts that the modified Cidon system would have benefited from Shikfa’s techniques of encrypting and searching file content without requiring this capability at a storage provider (thereby allowing users to choose cloud storages without search capability) and providing document searchability without compromising privacy needs to protect confidential information. *Id.* at 44 (citing Ex. 1006 ¶ 50; Ex. 1002 ¶ 105).

(2) *Patent Owner's arguments*

Patent Owner asserts that Petitioner implements Shikfa's identifiers in Herrmann's gateway server but "Shikfa already discloses its own 'gateway device,' namely the broker server, which acts as an intermediary between the client and cloud storage providers" so "there is no reason [a skilled artisan] would have incorporated Herrmann's gateway server into the modified system (because Shikfa already discloses one)." PO Resp. 28–29.

Patent Owner argues, "Shikfa is explicit that the client, not the broker server, performs the encryption of the document." PO Resp. 29. Patent Owner assert that a skilled artisan seeking to modify Cidon, which performs encryption on a management server, would not consider Shikfa, "which emphasizes the importance of using the user device to encrypt files (because of the lack of trust of other devices)." *Id.* at 30. Patent Owner asserts that Shikfa teaches away from performing encryption on a gateway. *Id.*

(3) *Analysis*

By arguing a skilled artisan would not have incorporated Herrmann's gateway server because Shikfa discloses one (PO Resp. 29), Patent Owner attacks the references individually. *In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986). The asserted combination implements Cidon's searchable encryption on Herrmann's gateway with Shikfa's search techniques that configure namespaces for searching encrypted document chunks. Pet. 21–22 (citing Ex. 1002 ¶ 67). The Cidon-Herrmann management server-gateway encrypts namespace identifiers, so there is no reason to encrypt files at a client device. Cidon and Shikfa both encrypt files external to the cloud file stores for security reasons. Tr. 17:4–18:22. In the combination, encryption would occur at the external gateway server of Cidon and Herrmann.

Incorporating Herrmann's techniques into Cidon would have allowed the automatic policy assignment and implementation to improve system efficiency and reduce human errors. Pet. 22 (citing Ex. 1005 ¶ 77; Ex. 1002 ¶ 69). We agree with Dr. Lee that adding Herrmann's gateway functions for assigning access policies to Cidon's system would have allowed automatic policy assignment and implementation, which would have improved Cidon's system efficiency and reduced human errors in assigning policies for better real-time protection as Herrmann teaches. Ex. 1002 ¶ 69.

Shikfa discloses its intermediary searchable encryption broker server 12 may act as an aggregator of searchable encryption mechanisms to support different searchable encryption mechanisms. Ex. 1006 ¶ 38. Petitioner proposes to aggregate Shikfa's searchable mechanism of encrypted indexes of namespace identifiers mapped to keywords and files into Cidon's similar intermediary management server 100 for similar results of configuring namespaces of file chunks so the file content is encrypted in a manner that makes it searchable as claimed. Pet. 43–45; Reply 14 (Shikfa also performs encryption at a gateway device). We agree with Petitioner that Shikfa did not criticize using its searchable encryption in a gateway with functionality of Cidon-Herrmann. Reply 13. Shikfa and Cidon both control access to encrypted cloud files. Ex. 1006 ¶¶ 2, 3, 28–36; Ex. 1004 ¶¶ 91, 99–108.

(4) Conclusion

Based on the parties' contentions and record evidence, we determine that Petitioner has demonstrated by a preponderance of the evidence that it would have been obvious to combine the teachings of Cidon, Shikfa, and Herrmann in the manner asserted.

- i. *1[c]: “storing, by the gateway device, the searchable encrypted file on the one or more cloud platforms based on the policy; and”*

(1) Petitioner’s contentions

Petitioner contends that the Cidon-Herrmann-Shikfa gateway device would include the functionality of Cidon’s management server that stores encrypted files on a cloud platform based on the policy. Pet. 46. Petitioner asserts that Cidon’s management server sends encrypted segments of a file to cloud storage, and a skilled artisan would have understood that searchable encrypted files were stored in specific directories in cloud storage based on the policy. *Id.* at 47–49 (citing Ex. 1004 ¶¶ 10, 43, 208, 209, 214, 215, 229, 309, Abstr., claim 1, Fig. 15; Ex. 1002 ¶ 110).

(2) Patent Owner’s arguments

Patent Owner argues that “the policy” in element 1[c] has antecedent basis from “a policy” recited in element 1[a][i]. PO Resp. 39. Patent Owner asserts that Cidon’s policies for the placement of files in specific directories or shares may satisfy the “storing” limitation of element 1[c], but placement policies are not the same “policy” that Petitioner asserted for element 1[a][i]. *Id.* at 39–40. Patent Owner argues that Petitioner relies on paragraphs 102 and 108 of Cidon to disclose an “access policy” defined for users but cites paragraphs 208 and 209 to disclose placement policies, which are “defined on documents.” *Id.* at 40. Patent Owner asserts that “Cidon’s placement policies apply as a result of file-specific properties such as ‘similarities and ancestry trees’ and are not assigned to the users.” *Id.* Patent Owner argues that the functions performed by the management server in paragraph 102 are distinct from the “placement policies” described in paragraphs 206–208, and “access policies are assigned by IT departments for different users.” *Id.*

(3) *Analysis*

Element 1[c] does not require “placement policies” as Patent Owner argues. It recites “storing . . . the searchable encrypted file on the one or more cloud platforms based on the policy.” Ex. 1001, 20:4–6. As discussed in Sections II.D.5.b. and II.D.5.d. for elements 1[a][i] and 1[b], Cidon allows IT departments/administrators to define policies for *storing files* on cloud storage services according to a policy that controls access by users or groups to encrypted files stored in the cloud by providing the right keys to decrypt files stored in cloud storage based on user-defined policies. Ex. 1004 ¶¶ 99–103, 108. A single policy defines how files are stored in cloud platforms and how files are encrypted, stored, and accessed by a particular user/group as claimed. *Id.* ¶¶ 99–108, 206–217, 309–326.

(4) *Conclusion*

Based on the parties’ contentions and record evidence, we agree with and adopt Petitioner’s analysis and determine that the combination of Cidon, Herrmann, and Shikfa discloses or suggests element 1[c].

j. *1[d]: “managing access to the searchable encrypted file by the one or more users based on the policy.”*

(1) *Petitioner’s contentions*

Petitioner asserts that Cidon manages access to searchable encrypted files by users based on the policy by providing access policies for secure file access to files in cloud storage for users and enforcing such access policies. Pet. 49 (citing Ex. 1004 ¶¶ 102, 108; Ex. 1002 ¶ 112). Petitioner also asserts that Cidon’s management server provides user management that allowed an administrator to define access policies that are enforced through API feeds to cloud storage providers. *Id.* (citing Ex. 1004 ¶¶ 67, 108, 113).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions that Cidon discloses element 1[d]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and record evidence, we agree with and adopt Petitioner's analysis and determine that Cidon discloses or suggests element 1[d].

k. *Conclusion*

We determine that Petitioner has established by a preponderance of evidence that claim 1 is unpatentable over Cidon, Herrmann, and Shikfa.

6. *Independent Claim 16*

a. *Petitioner's contentions*

Petitioner asserts that Cidon discloses a secure cloud storage system in element 16[pre]. Pet. 50–51 (citing Ex. 1004 ¶¶ 57, 99, 100, Fig. 2; Section VIII.A.2.a.). Petitioner asserts that Cidon's program runs on a management server and a processor in element 16[a]. *Id.* at 51 (citing Ex. 1004 ¶¶ 307, 407, 416). Petitioner asserts that Cidon's management server receives user requests to decrypt files or send encryption keys to user devices, connects to file repositories, and accesses stored files using a communication interface in element 16[b]. *Id.* at 51–52 (citing Ex. 1004 ¶¶ 100, 101, 309, 340, 342; Ex. 1002 ¶ 118). Petitioner asserts that Cidon's management server 100 has internal data storage operatively coupled to a processor in element 16[c]. *Id.* at 52 (citing Ex. 1004 ¶¶ 50, 101, 102, 307, 407, 412, 416; Ex. 1002 ¶ 119). Petitioner asserts that Cidon's management server 100 includes an IT policy enforcement module that could define access policies for users/groups in element 16[c][i]. *Id.* at 53 (citing Ex. 1004 ¶¶ 50, 101, 108; Ex. 1002 ¶ 121).

Petitioner asserts that “Cidon’s policy define[s] and manage[s] access to and processing of a file to be uploaded on a cloud” in element 16[c][i][A] as asserted for element 1[a][i] in the Petition. *Id.* at 53 (citing Ex. 1004 ¶¶ 50, 101, 108). Petitioner asserts that Cidon’s policy defines access rights of the user in element 16[c][i][B] as asserted for element 1[a][ii]. *Id.* at 53. Petitioner asserts that a skilled artisan would have understood that Cidon encrypts with an encryption module and instructions executable by the processor in element 16[c][ii]. *Id.* at 54 (citing Ex. 1004 ¶¶ 50, 102; Ex. 1002 ¶ 124). Petitioner asserts that Cidon uses cryptographic key information defined by the policy to produce a searchable encrypted file by encrypting content of the file, and Cidon stores encrypted content across a cloud platform(s) in element 16[c][ii][A] as asserted for element 1[b]. *Id.* (citing Ex. 1004 ¶ 174; Ex. 1002 ¶ 125). Petitioner asserts that Cidon discloses element 16[c][ii][B] as asserted for element 1[b][i] in the Petition. *Id.* Petitioner contends that Cidon discloses element 16[c][2][C] as asserted for element 1[b][ii] in the Petition. *Id.* at 55. Petitioner contends that Cidon and Shikfa configure namespaces of chunks to make file content searchable in element 16[c][ii][D] as for element 1[b][iii] in the Petition. *Id.*

Petitioner contends that Cidon’s management server stores searchable encrypted files on the cloud storage based on the policy in element 16[c][iii] as asserted for element 1[c] in the Petition. *Id.* at 55 (citing Ex. 1004 ¶¶ 50, 102; Ex. 1002 ¶ 130; Pet. Sections VIII.A.3.b., VIII.A.3.d.). Petitioner asserts that Cidon’s server manages user access to searchable encrypted files based on the policy using executable instructions in element 16[c][iv]. *Id.* at 55–56 (citing Ex. 1004 ¶¶ 50, 102; Ex. 1002 ¶ 131; Pet. Sections VIII.A.3.b., VIII.A.3.d.).

b. Patent Owner's argument

Patent Owner does not present separate arguments for claim 16 apart from the arguments that were presented for claim 1. *See* PO Resp. 21–41.

c. Analysis

We disagree with Patent Owner's arguments for the reasons provided in Section II.D.5. *supra* for claim 1.

d. Conclusion

Based on the full trial record and parties' contentions, we determine that Petitioner has established by a preponderance of evidence that claim 16 is unpatentable over the combination of Cidon, Shikfa, and Herrmann.

7. Dependent Claims 2, 3, 8–10, 12, 13, 17, 21–24, 26, and 27

a. Petitioner's contentions

Petitioner contends that Cidon's management server allows users to download the searchable encrypted file to a local device as recited in claims 2 and 17 by connecting to their web storage services on cloud platforms. Pet. 56 (citing Ex. 1004 ¶¶ 221, 231, 299; Ex. 1002 ¶ 132). Petitioner asserts that Cidon discloses local devices could be mobile computing devices such as an iPhone, iPad, or Windows laptop as recited in claim 3. Pet. 56 (citing Ex. 1004 ¶¶ 95, 108, 109, 116; Ex. 1002 ¶ 133). Petitioner asserts that Cidon's management server can encrypt files independent of the service provider of the cloud platforms as recited in claim 8. Pet. 57 (citing Ex. 1004 ¶¶ 99, 102, 113, 221; Ex. 1002 ¶ 134). Petitioner contends that Cidon allows different IT departments to implement different policies to access secure files for different groups of users as recited in claims 9 and 23. Pet. 57 (citing Ex. 1004 ¶ 108; Ex. 1005 ¶ 67; Ex. 1002 ¶ 135).

Petitioner contends that Cidon's policy defines the manner in which the file is stored in specific directories, accessed, and processed as recited in claims 10 and 24 by placing files in specific directories (storing), providing access and sharing permissions (accessing), and providing encryption and copy control (processing). Pet. 57–58 (citing Ex. 1004 ¶¶ 102, 108, 207–212, 401, 402, Fig. 23).

Petitioner contends that Cidon renders obvious storing searchable encrypted files on cloud platforms independent of the service provider by archiving and backing up files to other storage services, synchronizing files between services, and storing encrypted files to different web storage services as recited in claim 12. Pet. 59–60 (citing Ex. 1004 ¶¶ 100, 173, 174, 221, Fig. 2; Ex. 1001, 13:54–59; Ex. 1002 ¶ 138).

Petitioner contends that Cidon and Herrmann select a policy from a plurality of policies stored in a database operatively coupled to the gateway device as recited in claim 13. Pet. 61 (citing Ex. 1004 ¶¶ 101, 108, 115; Ex. 1005 ¶¶ 50, 67; Ex. 1002 ¶¶ 141–146). Petitioner asserts that a skilled artisan would have been motivated to store Cidon's policies in a database coupled to the management server with Herrmann's gateway to enable selecting a policy from stored policies for the same user instead of having to repeatedly create a new policy to improve efficiency and consistency. Pet. 61–62 (citing Ex. 1004 ¶¶ 103, 110, 119; Ex. 1005 ¶ 67; Ex. 1002 ¶¶ 145, 146).

Petitioner asserts that Herrmann implements modules and functions such as the policy assignment module, encryption module, storage module, and management module recited in claim 21 on Herrmann's gateway server and integrity server. Pet. 65–66 (citing Ex. 1005 ¶¶ 60, 65, Fig. 3).

Petitioner asserts that Cidon renders obvious a mediation module that implements a policy assignment, encryption, storage, or policy management module independent of the service provider as recited in claim 22. Pet. 67. Petitioner asserts that Cidon's management server connects to different consumer-based file repositories (Dropbox 13, Gmail 11, and Evernote) through APIs to provide user management and API access to cloud storage services. *Id.* at 67–68 (citing Ex. 1004 ¶¶ 100, 113, Fig. 2). Petitioner asserts that Cidon also carries out encryption and storage independent of the cloud platform service provider, and management server 100 acted as a proxy between cloud services and user devices as a complete software system that encrypted files in the cloud and enforced secure access to the cloud files. *Id.* at 68–69 (citing Ex. 1004 ¶¶ 102, 221, Fig. 2; Ex. 1002 ¶ 162; Pet. Sections VIII.A.3.b., VIII.A.3.d., VIII.A.6., VIII.A.10.).

Petitioner asserts that Cidon renders obvious a group of policies that are stored in a database operatively coupled to the system as recited in claim 26. Pet. 69 (citing Pet. Section VIII.A.3.e.; Ex. 1002 ¶ 164).

b. Patent Owner's arguments

Patent Owner does not contest expressly Petitioner's assertions that the combination of Cidon, Shikfa, and Herrmann discloses or suggests claims 2, 3, 8–10, 12, 13, 17, 21–24, 26, and 27. *See generally* PO Resp.; Sur-reply.

c. Conclusion

Based on the parties' contentions and record, we agree with and adopt Petitioner's analysis and determine that Petitioner has established by a preponderance of evidence that claims 2, 3, 8–10, 12, 13, 17, 21–24, 26, and 27 are unpatentable over the combination of Cidon, Shikfa, and Herrmann.

8. *Claims 11 and 25: “wherein the file is stored across two or more cloud platforms.”*

a. *Petitioner’s contentions*

Petitioner contends that Cidon stores the file across two or more cloud platforms as recited in claims 11 and 25 by archiving and backing files up to other storage services and synchronizing files between services. Pet. 58–59 (citing Ex. 1004 ¶ 174). Petitioner asserts that a skilled artisan would have understood that backing up and synchronizing files on or between storage services constituted storing the file across two or more cloud platforms. *Id.* at 59 (citing Ex. 1004 ¶ 221; Ex. 1002 ¶ 137).

b. *Patent Owner’s arguments*

Patent Owner argues that archiving/backing up files to other locations does not store a file *across* multiple locations. PO Resp. 41. Patent Owner asserts that storing “across” multiple platforms means that a single file is divided into multiple chunks that each are stored on a different cloud store 114. *Id.* (citing Ex. 1001, 7:43–45). Dr. Black testifies that storing “across” multiple platforms means a single file has different parts stored on different platforms. Ex. 2003 ¶ 116 (citing Ex. 1001, 7:43–45).

c. *Analysis*

As discussed in Section II.B.2. *supra*, we interpret the limitation “the file is stored across two or more cloud platforms” to encompass the entire file being stored on multiple cloud platforms. We disagree that storing a file “across” two or more cloud platforms *requires* the file to be divided into chunks *and* each chunk to be stored on a different cloud store. PO Resp. 41 (citing Ex. 1001, 7:43–45). Absent a lexicographic definition or a disclaimer, we do not limit the claims to a particular embodiment when the language is broader than that embodiment. *Phillips*, 415 F.3d at 1316.

We agree with Petitioner that Cidon’s archiving and backup of files to other storage services and synchronization of files between storage services teaches and suggests to store files across two or more cloud platforms. Pet. 58–59 (citing Ex. 1004 ¶ 174). We agree Dr. Lee’s testimony that a skilled artisan would understand that Cidon’s backup and/or synchronization of files on or between different storages results in the file being stored across two or more cloud platforms. Ex. 1002 ¶ 137. His testimony is consistent with the ’678 patent’s disclosure that a file can be stored on more than one cloud store. Ex. 1001, 7:40–42. Shikfa also discloses that broker server 12 may transmit one or more of the encrypted documents 14 to more than one cloud storage provider 18 (e.g., SP1, SP2, etc.). Ex. 1006 ¶ 31.

d. Conclusion

Based on the parties’ contentions and record evidence, we agree with and adopt Petitioner’s analysis and determine that Petitioner has established by a preponderance of evidence that claims 11 and 25 are unpatentable over the combination of Cidon, Herrmann, and Shikfa.

9. *Claim 14: “wherein the policy defines one or more of a set of encryption keys, a set of decryption keys, search indices, a type of encryption and one or more authorized locations to which the file may be stored.”*

a. Petitioner’s contentions

Petitioner asserts that Cidon uses encryption keys to encrypt files, Shikfa encrypts documents and indexes using different algorithms, and Herrmann uses encryption. Pet. 63 (citing Ex. 1004 ¶ 110; Ex. 1005 ¶ 21; Ex. 1006 ¶ 29; Ex. 1002 ¶ 149). Petitioner asserts that Cidon creates, stores, and retrieves keys to encrypt and decrypt files according to policies assigned to users. *Id.* (citing Ex. 1004 ¶¶ 43, 102, 108, 110; Ex. 1002 ¶ 150).

Petitioner asserts that Cidon stores modified files to new authorized locations to prevent users from accessing the files and it would have been obvious to manage file locations as part of Cidon's security policy to prevent unauthorized users from accessing files to improve data security. Pet. 64 (citing Ex. 1004 ¶¶ 364, 367; Ex. 1006 ¶ 29; Ex. 1002 ¶¶ 152, 153).

b. Patent Owner's arguments

Patent Owner argues that Petitioner identifies Cidon's disclosure of moving an encrypted file to another location but does not identify how Cidon's security policy defines and manages the location information, and Cidon does not disclose that relocation is done based on a policy. PO Resp. 42–43 (citing Ex. 1004 ¶ 364; Ex. 2003 ¶ 119).

c. Analysis

As discussed in Section II.D.5.b. *supra*, Cidon generates policies that control users' access to secure files and encryption and decryption of files by providing the right encryption keys to users. Ex. 1004 ¶¶ 99–102, 108, 219–227. Cidon applies this user-based policy by uploading files to specific file directories and providing access and sharing permissions to encrypted files to control users' access to files and storage locations. *Id.* ¶¶ 102–105, 135–146, 148, 149, 206–229. Cidon may store a file at a different location to prevent users from accessing the file at an unauthorized storage location. *Id.* ¶¶ 364, 367 (cited in Pet. 64). We agree with Petitioner that a skilled artisan would have found it obvious that Cidon's policy would define decryption keys and authorized locations where a file may be stored as part of the user-defined access and encryption policies. Pet. 64; Reply 20. Shikfa similarly teaches to store a document in more than one cloud storage location as part of its access control policy for users and files. Ex. 1006 ¶ 31.

d. Conclusion

Based on the parties' contentions and record evidence, we agree with and adopt Petitioner's analysis and determine that Petitioner has established by a preponderance of evidence that claim 14 is unpatentable over the combination of Cidon, Herrmann, and Shikfa.

E. Ground 2: Obviousness Over Cidon, Shikfa, Herrmann, and Fellenstein

Petitioner asserts claim 6 is unpatentable under 35 U.S.C. § 103 over the combination of Cidon, Shikfa, Herrmann, and Fellenstein. Pet. 69–70.

1. Fellenstein

Fellenstein discloses a method that adds one or more keywords from the content of a file to a file name so the file name includes the keywords. Ex. 1007 ¶ 8. When keywords of a file name match a file retrieval word, the file name with the keywords "is regarded as a result of retrieval." *Id.*

2. Claim 6: "wherein the step of configuring the namespaces comprises storing content of the file as filenames."

a. Petitioner's contentions

Petitioner asserts that Fellenstein adds keywords from the content of a file to the filename and uses the keywords to retrieve the file. Pet. 70 (citing Ex. 1007 ¶ 8). Petitioner contends that a skilled artisan would have been motivated to add this functionality into the Cidon-Herrmann-Shikfa combination to provide another search option for the modified system. *Id.* Petitioner asserts that searching only filenames could be done with simple string-matching operations that would yield quicker results, and one or more keywords (disclosed in Fellenstein) and file segment identifiers (disclosed in Cidon) would have been included as part of the file segment's filename. *Id.* (citing Ex. 1007 ¶ 8; Pet. Section VIII.A.2.f.; Ex. 1002 ¶ 167).

b. Patent Owner's arguments

Patent Owner argues that Ground 2 fails because it relies on Ground 1 for limitations of independent claim 1, and Cidon, Herrmann, and Shikfa do not render claim 1 obvious. PO Resp. 43 (citing Ex. 2003 ¶ 121).

c. Analysis

Because Petitioner has established by a preponderance of evidence that claim 1 is unpatentable over the combination of Cidon, Herrmann, and Shikfa, there is no deficiency in claim 6 due to its dependency from claim 1.

d. Conclusion

Based on the parties' contentions and record evidence, we agree with and adopt Petitioner's analysis and determine that Petitioner has established by a preponderance of evidence that claim 6 is unpatentable over the combination of Cidon, Herrmann, Shikfa, and Fellenstein.

F. Ground 3: Alleged Obviousness Over Cidon, Shikfa, Herrmann, and Hirai

Petitioner asserts claim 15 is unpatentable under 35 U.S.C. § 103 over the combination of Cidon, Shikfa, Herrmann, and Hirai. Pet. 71–72.

1. Hirai

Hirai discloses a file retrieval system including extracting section 6 that extracts a file name and keywords related to file data from file data that is decoded using an extracting program. Ex. 1008, 5:64–67. Decoding section 7 decodes encoded file data using a cryptographic key (public key) prepared in advance by using a decoding program. *Id.* at 6:1–4. Encoding section 8 encodes the extracted keywords and the file name by using an encoding program, and the encoding and decoding sections store cryptographic key data and programs. *Id.* at 6: 5–13.

2. *Claim 15: “. . . wherein said encrypting further comprises encrypting one or more of filename and search indices.”*

a. Petitioner’s contentions

Petitioner contends that Shikfa encrypts search indices of keywords of encrypted documents used to search encrypted documents. Pet. 71 (citing Ex. 1006 ¶ 29, Fig. 2; Ex. 1002 ¶ 170). Petitioner asserts that Hirai’s system generates a file name and a plurality of keywords related to the file data and encodes the keywords and the file name. *Id.* at 72 (citing Ex. 1008, 5:64–6:13). Petitioner asserts a skilled artisan would have added Shikfa’s and Hirai’s functions to Cidon because filenames and search indexes often describe file contents and would reveal confidential data so encrypting file names, keywords, and indexes “would help prevent confidential information in the filenames and search indexes from being revealed to the cloud storage provider.” Pet. 72 (citing Ex. 1006 ¶ 50; Ex. 1002 ¶ 172).

b. Patent Owner’s arguments

Patent Owner argues that Ground 3 fails because it relies on Ground 1 for limitations of independent claim 1, and Cidon, Herrmann, and Shikfa do not render claim 1 obvious. PO Resp. 43 (citing Ex. 2003 ¶ 121).

c. Analysis

Because Petitioner has established by a preponderance of evidence that claim 1 is unpatentable over the combination of Cidon, Herrmann, and Shikfa, claim 15 is not deficient due to its dependency from claim 1.

d. Conclusion

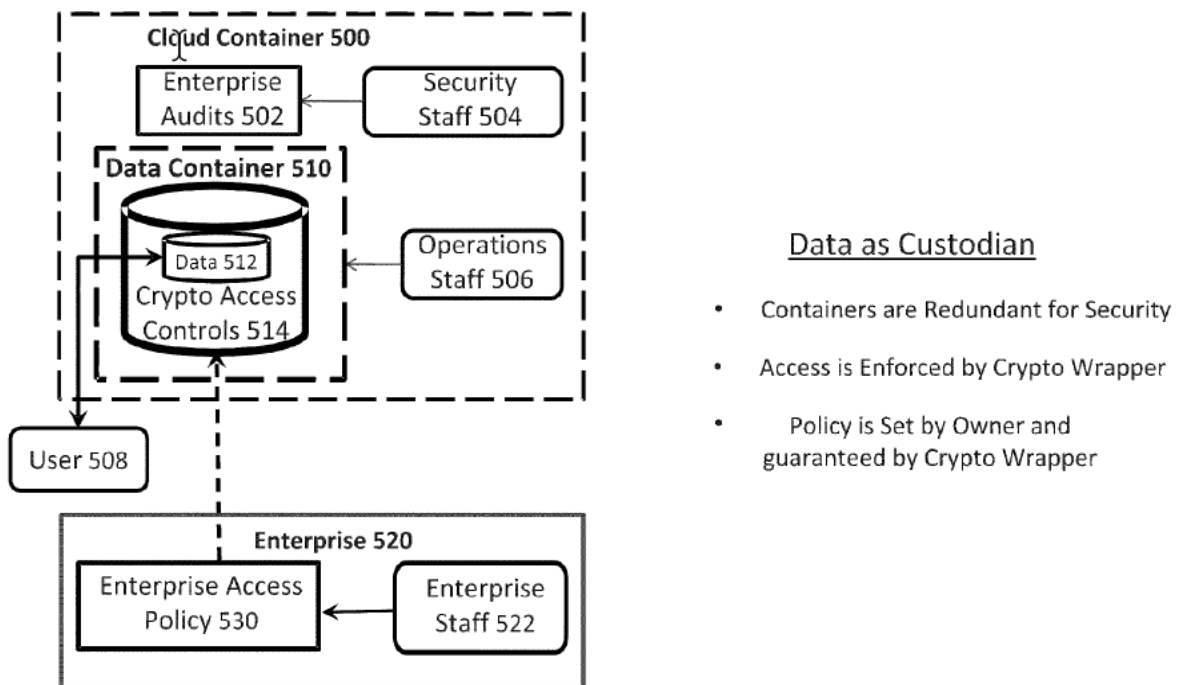
Based on the parties’ contentions and record evidence, we agree with and adopt Petitioner’s analysis and determine that Petitioner has established by a preponderance of evidence that claim 15 is unpatentable over the combination of Cidon, Herrmann, Shikfa, and Hirai.

G. Ground 4: Obviousness Over Auradkar, Chiueh, and Chambers

Petitioner asserts claims 1–3, 8–17, and 21–27 are unpatentable under 35 U.S.C. § 103 over the combination of Auradkar, Chiueh, and Chambers.¹³ Pet. 72–135.

1. Auradkar

Auradkar manages access to encrypted data in cloud storage by using cryptographic keys. Ex. 1009 ¶¶ 10, 71, 73, 76, 85, 89, 97, 108, 112, 119, Fig. 1. Enterprise access policy 530 determines how data 512 in container 510 of cloud container 500 is accessed, manipulated, retrieved, and searched using crypto access controls 514 based on enterprise access policy 530 to protect data 512 from unwarranted access by users 508 as shown in Figure 5, which is reproduced below. Ex. 1009 ¶ 117.



¹³ Petitioner asserts that claims 1–3, 8–19, and 21–27 are unpatentable over Auradkar, Chiueh, and Chambers (Pet. 7, 72), but Petitioner presents no substantive arguments for claims 18 and 19 (*id.* at 72–135).

Figure 5 depicts enterprise access policy 530 set by enterprise staff 522 to control how data 512 in data container 510 is accessed, manipulated, retrieved, and searched. Ex. 1009 ¶ 117. “[E]nterprise access policy 530 can be set by the enterprise owners and guaranteed by the crypto wrapper as implemented by the crypto access controls 514.” *Id.* Encrypted records, tags, and indexes are uploaded to the cloud as searchable, encrypted data records and encrypted indexes so content and records can be identified by searching indexes. We reproduce Figure 15 of Auradkar below to illustrate this arrangement. *See* Ex. 1009 ¶¶ 125, 127, 130, 131.

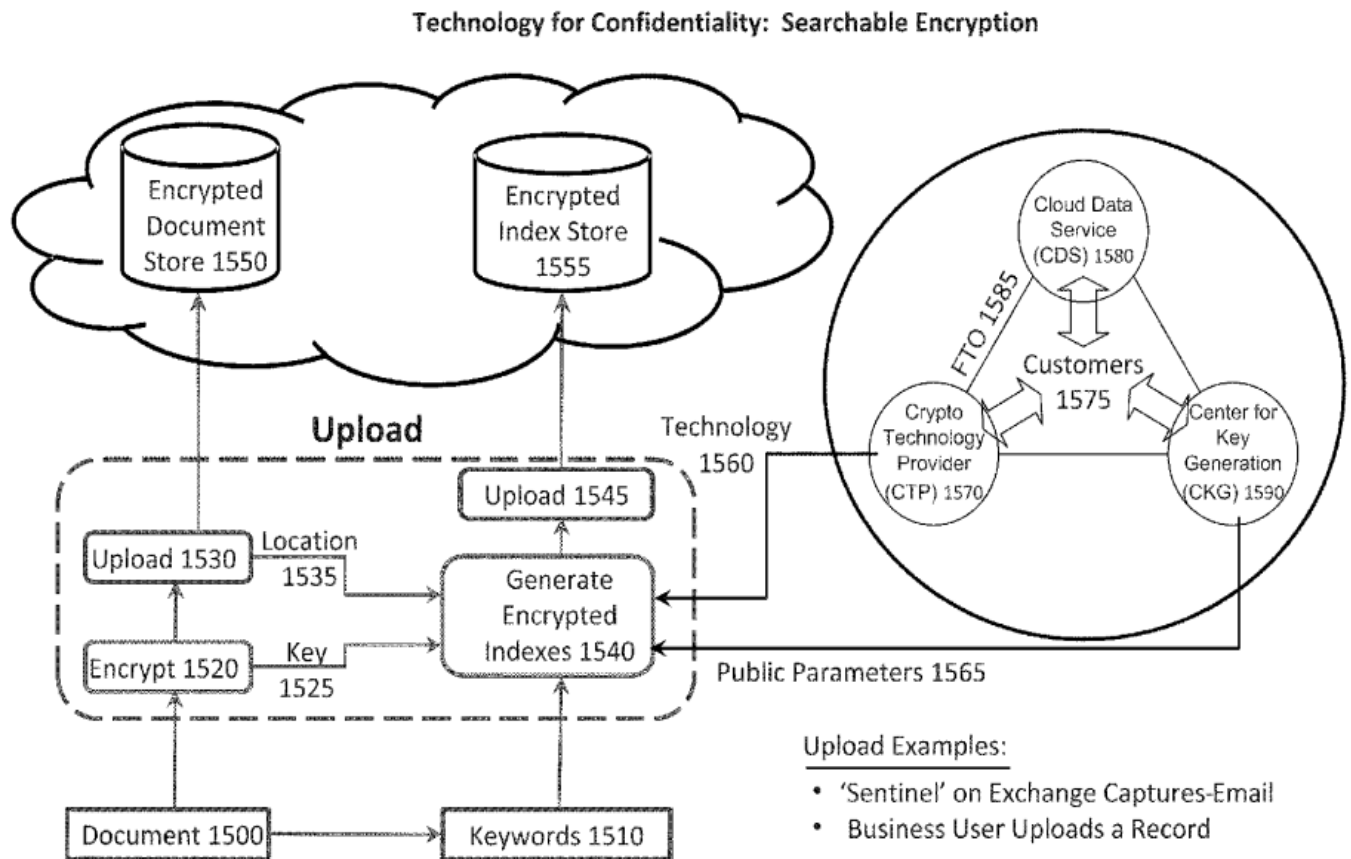


FIG. 15

Figure 15 illustrates document 1500 and keywords 1510 that are encrypted and uploaded to the cloud into stores 1550, 1555. Ex. 1009 ¶ 130.

2. Chiueh

Chiueh's system stores encrypted document pages and words in the Global Search Index (GSI) of a Significant Word Set (SWS). Encrypted keyword searches can obtain a first index that identifies encrypted pages with the encrypted keywords. Ex. 1011 ¶¶ 8, 20, 25, 40, Fig. 3. Each encrypted word in the GSI maps to a document ID that identifies an encrypted page where the word is found. *Id.* ¶ 40.

3. Chambers

Chambers uses network access device 102 to apply access control policies 117 to client devices 108 as shown in Figure 1, reproduced below.

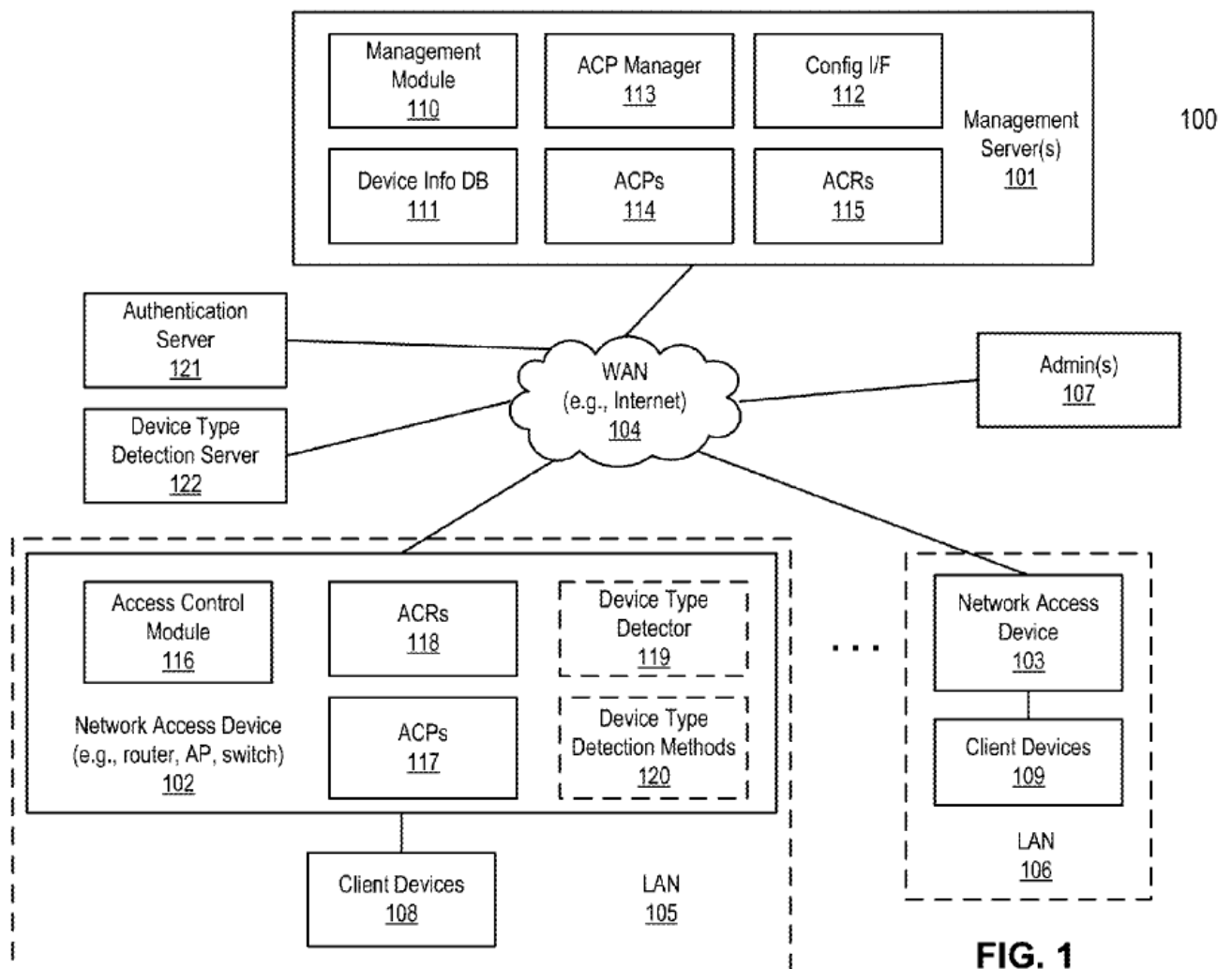


FIG. 1

Figure 1 illustrates management server 101 and access control policy manager 113 that transmits access control policies (ACPs) 117 and access control rules (ACRs) 118 to control access of client devices 108 by enforcing ACPs 117 and ACRs 118. Ex. 1010 ¶¶ 24, 27, 28.

4. *Independent Claim 1*

a. *1[pre]*

(1) *Petitioner's contentions*

Petitioner asserts that Auradkar discloses a method of encrypting and storing files. Pet. 79–80 (citing Ex. 1009, Abstr., Fig. 15; Ex. 1002 ¶ 190).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions that Auradkar discloses element 1[pre]. *See generally* PO Resp.; Sur-reply.

(3) *Conclusion*

Based on the parties' contentions and record evidence, we adopt Petitioner's analysis and determine that Auradkar discloses element 1[pre] to the extent the preamble is limiting.

b. *1[a][i]*

(1) *Petitioner's contentions*

Petitioner asserts that Auradkar teaches a gateway device that assigns a policy for managing access to and processing a file to be stored on cloud platforms as recited in element 1[a][i] by assigning access policy 530, 630 to enterprise staff 522, 622 to manage users' access to files stored on cloud container 500 and manage how data 512 was stored, accessed, manipulated, retrieved, and searched using crypto access controls 514 guided by enterprise access policy 530 to protect data 512 from unwarranted access by users 508. Pet. 80–83 (citing Ex. 1009 ¶¶ 112, 113, 116, 117, 119, Figs. 1, 2, 5, 6; Ex. 1001, 9:11–19).

Petitioner asserts that Chambers discloses a network access device (NAD 102) as a gateway device that automatically selects and applies an appropriate access policy to client devices 108 and groups of users. *Id.* at 83–85 (citing Ex. 1010 ¶¶ 21, 24, 46, Figs. 1, 4A; Ex. 1002 ¶¶ 195–198).

Petitioner asserts that a skilled artisan would have found it obvious to use Chambers’ gateway to implement Auradkar’s “assigning” and the other claimed functions and automatically assign security policies based on a user’s role in the organization or the user’s devices to provide consistent policy application thereby improving system efficiency and reducing human errors by automatically configuring, assigning, and implementing policies. Pet. 85–87 (citing Ex. 1009, Fig. 11; Ex. 1010 ¶¶ 5, 6, 21, 29; Ex. 1002 ¶¶ 200, 201). Petitioner asserts that a skilled artisan would have expected success because gateways were well-known for network security. *Id.* at 87 (citing Ex. 1010 ¶¶ 66, 82; Ex. 1005 ¶¶ 18, 77; Ex. 102 ¶ 202).

(2) *Patent Owner’s arguments*

Patent Owner argues that Auradkar’s policy applies to files that have been uploaded to a cloud service. PO Resp. 54–55. Patent Owner asserts that Auradkar’s policy affects how data 512 stored in data container 510 of cloud container 500 could be accessed, manipulated, retrieved, and searched, and Auradkar’s crypto access controls reside on the cloud server and govern data that already was uploaded. *Id.* at 55 (citing Ex. 1009 ¶ 117, Fig. 5; Ex. 2003 ¶ 147). Patent Owner argues, “Auradkar is explicit that access to the data is controlled by ‘crypto access controls’ that reside within the cloud container—these controls are ‘guided by, but separated from, enterprise access policy 530’ [and] cannot affect data that is ‘*to be uploaded*’ on a cloud because the crypto access controls . . . only reside on the cloud server.” *Id.*

(3) *Analysis*

We find that Auradkar uploads encrypted documents to the cloud to encrypted document store 1550 based on enterprise access policy. Ex. 1009 ¶¶ 117, 127–130. Location 1535, key 1525 for *uploads*, and keywords 1510 are input to generate encrypted indexes 1540 of the encrypted, uploaded documents, and indexes are uploaded 1545 to encrypted index store 1555. *Id.*; Pet. 73–74, 88–91. Auradkar controls access to encrypted indexes and documents uploaded to cloud storage based on an enterprise’s access policy. Ex. 1009 ¶¶ 117–131. Auradkar encrypts and uploads records, indexes, and tags to the cloud using a trust overlay in searchable format to control access by users based on privileges in a policy. *Id.* ¶¶ 119, 124–131; Pet. 75, 88–93. This process controls access to indexes for searches or other operations, and it controls access to the encrypted data via cryptographic wrappers that are applied to the uploaded data. *Id.* ¶¶ 127–131.

(4) *Conclusion*

Based on the parties’ contentions and record evidence, we agree with and adopt Petitioner’s analysis and determine that the combination of Auradkar and Chambers discloses or suggests element 1[a][i].

c. *1[a][ii]*

(1) *Petitioner’s contentions*

Petitioner asserts that Auradkar discloses that its policy defines user access rights so that logs are encrypted and accessible only with the specific capabilities granted to a user, the policy affects how data stored in data container 510 of cloud container can be accessed, manipulated, retrieved, and searched, and crypto access controls protect data 512 from unwarranted access by users. Pet. 87–88 (citing Ex. 1009 ¶¶ 112, 117).

(2) *Patent Owner's arguments*

Patent Owner does not contest Petitioner's assertions that Auradkar discloses element 1[a][ii]. *See generally* PO Resp.; Sur-reply.

(3) *Analysis*

Auradkar allows enterprises to create and enforce encryption and data access policies based on the specific capabilities of users. Ex. 1009 ¶ 112. Auradkar discloses that enterprises can set access policy 530 to control how data are stored, accessed, manipulated, retrieved, and searched with crypto access controls, and different access policies and crypto access controls can be applied to different entities or tasks of enterprise staff. *Id.* ¶ 117, Fig. 5 (cited in Pet. 80–83 for “a policy”). As discussed in Section II.G.4.b. *supra*, a different enterprise access policy can be applied to each different accessing entity or task, and each policy 530 “can be reflected by the crypto access controls 514 of data container 510.” *Id.* ¶¶ 124–131; Pet. 73–74, 88–93.

(4) *Conclusion*

Based on the parties' contentions and record evidence, we agree with and adopt Petitioner's analysis and determine that Auradkar discloses or suggests element 1[a][ii].

d. *1[b]*

(1) *Petitioner's contentions*

Petitioner contends that Auradkar discloses encrypting record 1102 (data payload) and associated metadata and tags 1100 to produce encrypted metadata and tags, and Auradkar uploads encrypted record 1112 to the cloud into encrypted document store 1550 in searchable format similar to the way that the '678 patent encrypts and indexes keyword content of a file for searching the encrypted document. Pet. 88–92 (citing Ex. 1009 ¶¶ 124, 125, 127, 130, 133, Figs. 11, 12, 15, 16; Ex. 1001, 12:44–47, Fig. 3B).

Petitioner asserts that the '678 patent discloses that a selected policy can be used to define encryption keys, decryption keys, and encryption type, and Auradkar's policy defines the encryption type and length of encryption/decryption keys for encrypting sensitive data with AES 256 encryption. Pet. 92–93 (citing Ex. 1009 ¶ 96; Ex. 1001, 4:4–7). Petitioner contends that a skilled artisan would have combined Chambers' gateway with Auradkar's system to perform operations at the gateway as explained for element 1[a][i]. *Id.* (citing Ex. 1009 ¶ 96; Pet. Section VIII.D.2.b.; Ex. 1002 ¶¶ 210, 211).

(2) *Patent Owner's arguments*

Patent Owner argues that “Petitioner has failed to show any policy that defines cryptographic key information.” PO Resp. 53. Patent Owner asserts that a skilled artisan would understand that “cryptographic key information” includes defining the encryption and/or decryption keys and the encryption type. *Id.* Patent Owner argues that a policy for encrypting sensitive medical data with AES 256 encryption is for secrecy classification of a paragraph in a document, and it is not the Enterprise Access Policy that manages access to and processing of a file to be stored as recited in claim 1. *Id.* at 54. Patent Owner argues that the antecedent basis for “the policy” that defines cryptographic key information is “a policy for managing access to and processing a file to be stored.” *Id.*

(3) *Analysis*

As discussed in Section II.D.5.b. *supra* for Ground 1, the '678 patent describes a policy that includes sub-policies that control functions such as file access, file uploading, file encryption, file storage, and file processing. Ex. 1001, 2:17–22, 3:25–52, 4:1–4, 7:64–8:14, 9:11–67. Files are encrypted *based on* assigned policies. *Id.* at 4:1–19, 9:53–67.

Auradkar allows enterprise staff 522 to configure access policy 530 to control how data is stored in cloud data container 510 and how users access, manipulate, retrieve, and search it. Ex. 1009 ¶ 117. Crypto access controls 514 *guided by* enterprise access policy 530 protect data 512 from access by users. *Id.* Enterprise access policy 530 is *reflected by* crypto access controls 514 for data container 510 for different accessing entities to restrict visibility to users to whom access should be enabled. *Id.* Crypto access controls encrypt data stored in the cloud *based on* enterprise access policy 530 in the same way that the '678 patent describes an encryption module encrypting files based on an assigned policy. *Id.*; *see* Ex. 1001, 9:53–10:12.

Auradkar states that “enterprise access policy 530 can be set by the enterprise owners and *guaranteed by* the crypto wrapper as implemented by the crypto access controls 514” to control access by “users 610 wishing to access data 612.” Ex. 1009 ¶ 117 (emphasis added), 119. Enterprises can set and enforce access policies by placing cryptographic wrappers on data, metadata, and tags 1100 of encrypted records 1102 to allow or disallow access by users based on class, privileges, and capabilities granted to users by the enterprise’s access control policy. Ex. 1009 ¶¶ 112, 124, 125. In this way, data acts as its own custodian by using crypto controls to control and guarantee access policies set by enterprise owners. Ex. 1009 ¶¶ 109, 112.

(4) *Conclusion*

Based on the parties’ contentions and record evidence, we agree with and adopt Petitioner’s analysis and determine that the combination of Auradkar and Chambers discloses or suggests element 1[b].

e. 1[b][i]

(1) Petitioner's contentions

Petitioner asserts that Auradkar “divid[es] the file into a plurality of chunks” as recited in element 1[b][i] by dividing a document into XML fragments with different protection levels of Public, Secret and Top Secret to generate encrypted XML fragments, and Auradkar applies confidentiality level labels to each fragment to control access to each part of the XML document. Pet. 93–94 (citing Ex. 1009 ¶¶ 92, 95, 98, 150, Figs. 11, 12, 19).

(2) Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions that Auradkar discloses element 1[b][i]. *See generally* PO Resp.; Sur-reply.

(3) Conclusion

Based on the parties' contentions and record evidence, we agree with and adopt Petitioner's analysis and determine that Auradkar discloses or suggests element 1[b][i].

f. 1[b][ii]

(1) Petitioner's contentions

Petitioner asserts that Auradkar creates tags 1200, 1900 for payloads (payload 1202, XML fragment 1902 (chunks)) and the tag uses a *payload filename* (FName: fox.tx), and Auradkar encrypts the tags for searching. Pet. 94–96 (citing Ex. 1009 ¶¶ 125, 150, Figs. 12, 19). Petitioner asserts that the tags evidence a namespace because they are a set of names available for naming payloads. *Id.* at 96 (citing Ex. 1014; Ex. 1002 ¶ 217). Petitioner asserts that Chiueh divides a document into pages and encrypts each page to produce encrypted pages with a document ID (namespace) assigned to the page to indicate where a given encrypted word can be found. Pet. 96–97 (citing Ex. 1011 ¶¶ 20, 40; Ex. 1002 ¶¶ 218, 219).

Petitioner asserts that Chiueh’s document ID encrypts a file name and page offset in the document similar to Auradkar’s tag 1200, which includes a filename with tag information. Pet. 97 (citing Ex. 1009, Fig. 12; Ex. 1011 ¶ 40). Petitioner asserts that the combined teachings would create document IDs that identified document portions (pages, XML fragments), and a skilled artisan would have modified Auradkar’s whole-document search to retrieve encrypted portions to save bandwidth. Pet. 97 (quoting Ex. 1011 ¶ 28 and citing Ex. 1002 ¶ 220). Petitioner asserts that a skilled artisan would have had a reasonable expectation of success in doing so. *Id.* (citing Ex. 1009 ¶¶ 125, 150, Figs. 12, 19; Ex. 1011 ¶ 40, Fig. 2; Ex. 1002 ¶ 221).

(2) *Patent Owner’s arguments*

Patent Owner argues that creating a namespace involves creating a set of available names rather than creating an identifier because an identifier is a single item within a set rather than a namespace. PO Resp. 44–45 (citing Ex. 2003 ¶¶ 122–144), 47. Patent Owner argues that the set of available names is not created or defined during the encryption process. PO Resp. 46 (“[T]he system does not *create* the namespace during the encryption process because it was created in advance.”) (citing Ex. 2003 ¶¶ 126–128).

(3) *Analysis*

We find that Auradkar creates tags 1200 for payloads 1200 during the encryption process so payloads can be searched for and retrieved by the tags, and Auradkar creates a namespace convention or rule for creating tags 1200 *based on a chunk’s filename and content*. A tag “fox” is used for a file with a filename “fox.txt,” and “fox” and “dog” tags are used for file content with those words. Ex. 1009 ¶¶ 124, 125, Fig. 12; Reply 21–22; Pet. 94–96. We reproduce Figure 12 of Auradkar below to illustrate this namespace creation.

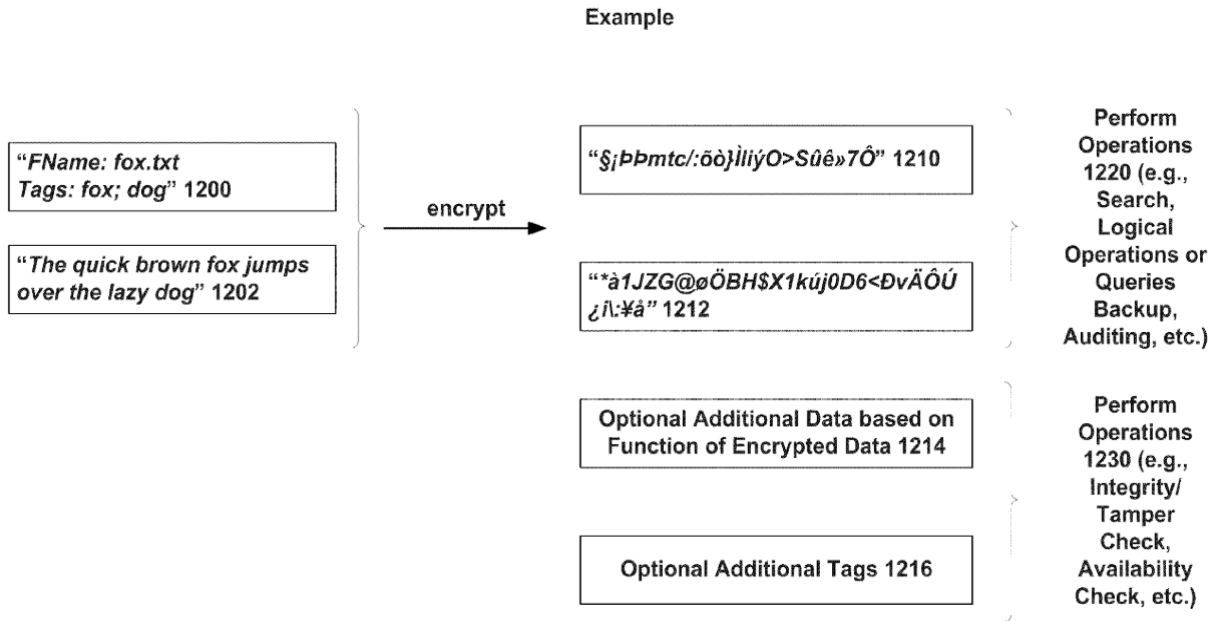


FIG. 12

Figure 12 of Auradkar shows payload (chunk) 1202 with content “The quick brown fox jumps over the lazy dog,” a filename of “FName: fox.txt,” and tags of “fox” and “dog” generated based on the filename and content of the payload chunk under Auradkar’s namespace policy. Ex. 1009 ¶ 125. Tags 1200 and data of payload 1202 are encrypted to form encrypted tags 1210 and encrypted data that is searchable as recited in element 1[b][iii]. *Id.*

A rule for creating namespace tags for files based on a filename or file content defines a set of allowable identifiers in a particular context according to Patent Owner’s definition of namespace. PO Resp. 19–21. It stores a file by searchable tags based on a filename or content of a file (e.g., fox, dog) as recited in claim 6 (Ex. 1001, 20:20–22). Ex. 1009 ¶¶ 125, 127, 130–133.

Tag identifiers in Auradkar are created in this namespace for payload chunks as (1) tags that use the filename of the payload (fox.txt) and (2) tags based on the content of the payload (i.e., fox, dog). Ex. 1009 ¶ 125, Fig. 12.

We also find that Chiueh creates namespaces for chunks (pages) of a document by creating and assigning document IDs for each encrypted page (chunk). Ex. 1011 ¶¶ 20, 40, Fig. 2; Pet. 96–97. A Document ID is created by a namespace convention that combines the filename and page offset in the document so that the document is stored and searched by the unique document ID. *Id.* ¶¶ 20, 40, Fig. 2. The namespace is created by a creating a namespace policy that names a document by its file name and page offset to encrypt the document in a searchable format. *Id.* ¶¶ 20–25, 40, Fig. 2. A unique document ID is created in the namespace when document pages are encrypted as recited in element 1[b][ii]. *Id.* ¶ 20.

(4) *Conclusion*

Based on the parties’ contentions and record evidence, we agree with and adopt Petitioner’s analysis and determine the combination of Auradkar and Chiueh discloses or suggests element 1[b][ii].

g. 1[b][iii]

(1) *Petitioner’s contentions*

Petitioner asserts that the Auradkar-Chiueh combination configures the namespaces of chunks so the content of the file is encrypted in a manner that makes it searchable as recited in element 1[b][iii]. Pet. 98. Petitioner asserts that Auradkar creates and encrypts tags for a payload (e.g., an XML fragment) based on a filename and file content in Figure 12. Pet. 98–99 (citing Ex. 1009 ¶¶ 125, 150, Figs. 12, 19). Petitioner asserts that Auradkar encrypts document 1500 and keywords to generate an encrypted document and encrypted indexes of keywords that are uploaded to the cloud where the indexes can be searched to identify content or records with matching keywords. Pet. 99–101 (citing Ex. 1009 ¶¶ 127, 130, 133, Figs. 15, 16).

Petitioner contends that Chiueh discloses encrypting individual document pages (chunks) and assigning an ID (namespace) to each of the encrypted pages. Pet. 101–102 (citing Ex. 1010 ¶¶ 20, 40, Fig. 2; Pet. Section VIII.D.2.f.). Petitioner asserts that Chiueh also creates an index of a significant word set that mapped encrypted keywords to document IDs of the encrypted pages so content of the encrypted pages could be searched using the keywords in the index as a global search index of encrypted significant words indexed to an encrypted page where the encrypted significant word could be found. Pet. 102–103 (citing Ex. 1011 ¶¶ 21–24, 40, Fig. 2).

Petitioner contends that a skilled artisan would have found it obvious that Chiueh’s system configured document IDs in namespaces for encrypted pages (chunks) and mapped the IDs (in the index) to keywords appearing in the document pages so the encrypted content was searchable using a search keyword. Pet. 105–106 (citing Ex. 1011 ¶¶ 23, 24, 40, Fig. 3; Ex. 1002 ¶ 232). Petitioner asserts that a skilled artisan would have added Chiueh’s functionality to Auradkar’s system to allow retrieval of individual pages instead of the whole document so bandwidth of the communication network could be saved, with a reasonable expectation of success. Pet. 106 (citing Ex. 1011 ¶ 28; Ex. 1002 ¶ 233; Pet. Section VIII.D.2.f.).

(2) *Patent Owner’s arguments*

Patent Owner argues that “Chiueh’s teaching of an encrypted index that maps keywords document identifiers does not meet the limitation ‘configuring the namespaces’ because identifiers are not namespaces.” PO Resp. 47. Patent Owner argues that “[a] namespace defines the set of names in a particular context [and] [s]tanding alone, an identifier is simply a single item or name within the set of allowed names, not the namespace.” *Id.* at 48.

Patent Owner argues that Chiueh discloses a universe of filenames and page offsets as the alleged namespace but the document identifiers (filenames) are *used*, not configured, in Chiueh's indexes because they were defined in advance by the reference. PO Resp. 48.

(3) *Analysis*

We find that Auradkar's storage of file chunks by encrypted filenames and tags based on file chunk content that they uniquely identify configures namespaces of the chunks so the file content is encrypted in a manner that makes it searchable by tags as recited in element 1[b][iii]. As discussed in Section II.G.4.f. *supra*, creating a namespace of filename and file content tags allows chunks to be stored by filename and content (configuring the namespace) and retrieved by searching the filenames and tags. *See* Ex. 1009 ¶ 125, Fig. 12. Auradkar also encrypts and uploads documents to the cloud into encrypted document store 1550 and configures the namespace tags of the documents to make them searchable. Ex. 1009 ¶¶ 130, 131, Fig. 15.

We find that Chiueh configures namespaces of chunks so the content of a file is searchable by storing document pages (chunks) in remote server 120 with assigned document IDs configured in a namespace of file name and page offset discussed above and mapped to keywords and pages in a global search index so that remote server 120 can search for and retrieve encrypted pages containing particular keywords. Ex. 1011 ¶¶ 20–25, Figs. 1–3.

(4) *Conclusion*

Based on the parties' contentions and record evidence, we agree with and adopt Petitioner's analysis and determine that the combination of Auradkar and Chiueh discloses or suggests element 1[b][iii].

h. 1[c], 1[d]

(1) Petitioner's contentions

Petitioner contends that Auradkar uploads a searchable, encrypted file on cloud platforms based on a policy that controls how and where data is stored and uploaded by encrypting and uploading a document to encrypted document store 1550 of cloud service providers as recited in element 1[c]. Pet. 106–108 (citing Ex. 1009 ¶¶ 96, 189, Figs. 15, 28; Ex. 1002 ¶ 236; contentions for element 1[a][i]). Petitioner contends that Auradkar manages access to searchable encrypted files via crypto access controls that guarantee enterprise access policy and protect data from unwarranted access as recited in element 1[d]. Pet. 108–109 (citing Ex. 1009 ¶¶ 112, 113, 117, Fig. 5).

(2) Patent Owner's arguments

Patent Owner does not contest Petitioner's assertions that the combination of Auradkar and Chambers discloses or suggests elements 1[c] and 1[d]. *See generally* PO Resp.; Sur-reply.

(3) Conclusion

Based on the parties' contentions and record evidence, we agree with and adopt Petitioner's analysis and determine that the combination of Auradkar and Chambers discloses or suggests elements 1[c] and 1[d].

i. Motivation to combine

(1) Petitioner's contentions

Petitioner asserts that combining Auradkar's system that stored and searched encrypted data with Chiueh's mechanism that searched individual pages would enable more efficient search and retrieval of pages or chunks rather than entire documents for more secure access to remotely-stored files. Pet. 79 (citing Ex. 1009 ¶¶ 127, 133, Fig. 16, Abstr.; Ex. 1010 ¶¶ 20, 40, Figs. 2, 3, Abstr.; Ex. 1011 ¶ 3; Ex. 1002 ¶ 186), 96–97, 105–106.

(2) *Patent Owner's arguments*

Patent Owner argues that Chiueh's client device encrypts document pages because the remote server is not reliable and a document stored in the remote server could be leaked if the remote server has decryption abilities. PO Resp. 51 (citing Ex. 1010 ¶¶ 5, 20–24; Ex. 2003 ¶ 138). Patent Owner asserts that a skilled artisan seeking to modify Auradkar and Chambers, which performs encryption on a remote gateway device, would not look to Chiueh, which uses user devices to encrypt files because of the lack of trust of external cloud storage devices. PO Resp. 52 (citing Ex. 2003 ¶ 140).

(3) *Analysis*

Petitioner's proposed combination implements Auradkar at a gateway, as taught by Chambers, to encrypt chunks (pages) of encrypted documents in a searchable index format that Chiueh teaches to improve the efficiency of the search process and bandwidth allocation by obviating the need to search for and retrieve an entire document when only a chunk of the document is needed to respond to a keyword search query. Pet. 80–87, 98–106.

Both Auradkar and Chiueh encrypt files at an enterprise or client that is remote from a cloud server before storing encrypted data on a remote cloud server. Ex. 1009 ¶¶ 108–124, Figs. 5, 6; Ex. 1011 ¶¶ 20–24, Fig. 2. Chiueh allows client computers to encrypt document pages and word sets to send to a remote server that cannot decrypt this data. Ex. 1011 ¶¶ 10, 19–24. Auradkar also places access “policy and enforcement within the control of users or an enterprise.” Ex. 1009 ¶¶ 112, 113. Chiueh's encryption would improve Auradkar's system by placing enterprise encryption policies in a searchable index format to improve the efficiency of the search process and bandwidth allocation. Ex. 1009 ¶ 117, Fig. 5; Ex. 1011 ¶¶ 20–24, Fig. 2.

(4) *Conclusion*

Based on the parties' contentions and record evidence, we determine that it would have been obvious to combine the teachings of Chiueh with those of Auradkar and Chambers in the manner asserted in the Petition for claim 1 with a reasonable expectation of success.

j. *Conclusion*

We determine that Petitioner has established by a preponderance of evidence that claim 1 is unpatentable over the combination of Auradkar, Chambers, and Chiueh.

5. *Claim 16*

a. *Petitioner's contentions*

Petitioner provides detailed contentions to supports its assertion that claim 16 is unpatentable over Auradkar, Chambers, and Chiueh. Pet. 109–118.

b. *Patent Owner's arguments*

Patent Owner presents the same arguments for claim 16 that Patent Owner asserted for claim 1. *See* PO Resp. 44–55.

c. *Analysis*

We disagree with Patent Owner's arguments for the reasons set forth in Section II.G.4. *supra* for claim 1.

d. *Conclusion*

Based on the parties' contentions and record evidence, we agree with and adopt Petitioner's analysis and determine that Petitioner has established by a preponderance of evidence that claim 16 is unpatentable over the combination of Auradkar, Chambers, and Chiueh.

6. *Dependent Claims 2, 3, 8–15, 17, and 21–27*

a. *Petitioner’s contentions*

Petitioner provides detailed contentions that claims 2, 3, 8–15, 17, and 21–27 are unpatentable over the combination of Auradkar, Chambers, and Chiueh. Pet. 118–135.

b. *Patent Owner’s arguments*

Patent Owner does not separately contest the patentability of claims 2, 3, 8–15, 17, and 21–27. *See generally* PO Resp.; Sur-reply.

c. *Conclusion*

Based on the parties’ contentions and record evidence, we agree with and adopt Petitioner’s analysis and determine that Petitioner has established by a preponderance of evidence that claims 2, 3, 8–15, 17, and 21–27 are unpatentable over the combination of Auradkar, Chambers, and Chiueh.

H. Ground 5: Obviousness Over Auradkar, Chiueh, Chambers, and Inoue

Petitioner asserts that claim 6 is unpatentable under 35 U.S.C. § 103 over Auradkar, Chiueh, Chambers, and Inoue. Pet. 135–138.

1. *Inoue*

Inoue correlates extracted keywords with image data for searches. Inoue also uses keywords as titles of image data. Ex. 1012 ¶ 104, Fig. 4.

2. *Claim 6*

a. *Petitioner’s contentions*

Petitioner asserts that Auradkar encrypts keywords of file content for searching encrypted content, and Inoue correlates extracted keywords with image data and a keyword as a title. Pet. 135–137 (citing Ex. 1009 ¶ 130, Fig. 15; Ex. 1012 ¶ 104, Fig. 4; Ex. 1002 ¶¶ 299–306; Ex. 1001, 12:7–9; Pet. Section VIII.D.2.d. contentions for element 1[b] in Ground 4).

Petitioner contends that a skilled artisan would have combined these complementary teachings to expand search options with a reasonable expectation of success. Pet. 138 (citing Ex. 1009 ¶ 130; Ex. 1011 ¶ 40; Ex. 1012, Abstr.; Ex. 1008 ¶ 8; Ex. 1017 ¶ 8; Ex. 1002 ¶¶ 305, 306).

b. Patent Owner's arguments

Patent Owner argues that Inoue uses a filename to store content of a file or search the content of the file as recited in claim 6. PO Resp. 55–56. Patent Owner argues that Inoue extracts one keyword from input voice data that a user uses to label an image and sets the keyword as the title. *Id.* at 56.

c. Analysis

Patent Owner's individual attacks on the references' teachings are not availing. Auradkar stores file content as a filename (e.g., FName: fox.txt). Ex. 1009 ¶¶ 125–131, 150, Figs. 12, 15. We find that a skilled artisan would have improved Auradkar's search techniques by using a keyword of file content as a filename, as Inoue teaches, to expand the search options of Auradkar. Pet. 137–138. Patent Owner does not dispute that this modification would have improved Auradkar. *See* PO Resp. 55–57; *KSR*, 550 U.S. at 417.

d. Conclusion

Based on the parties' contentions and record evidence, we agree with and adopt Petitioner's analysis and determine that Petitioner has established by a preponderance of evidence that claim 6 is unpatentable over the combination of Auradkar, Chambers, Chiueh, and Inoue.

III. CONCLUSION

Petitioner has demonstrated by a preponderance of evidence that claims 1–3, 6, 8–17, and 21–27 of the '678 patent are unpatentable as summarized below.

Claim(s)	35 U.S.C. §	References	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–3, 8–14, 16–19, 21– 27	103	Cidon, Shikfa, Herrmann	1–3, 8–14, 16– 19, 21–27	
6	103	Cidon, Shikfa, Herrmann, Fellenstein	6	
15	103	Cidon, Shikfa, Herrmann, Hirai	15	
1–3, 8–19, 21–27	103	Auradkar, Chiueh, Chambers	1–3, 8–19, 21– 27	
6	103	Auradkar, Chiueh, Chambers, Inoue	6	
Overall Outcome			1–3, 6, 8–17, 21–27	

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–3, 6, 8–17, and 21–27 of the '678 patent have been shown to be unpatentable; and

FURTHER ORDERED that because this is a Final Written Decision, parties to this proceeding seeking judicial review of this Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.¹⁴

¹⁴ Should Patent Owner wish to amend the challenged claims in a reissue or reexamination proceeding, we draw Patent Owner's attention to the *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16654 (Apr. 22, 2019). If Patent Owner files a reissue application or request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

IPR2023-00458
Patent 9,280,678 B2

PETITIONER:

Thomas Millikan
Babak Tehranchi
Wei Yuan
PERKINS COIE LLP
Millikan-ptab@perkinscoie.com
Tehranchi-ptab@perkinscoie.com
Yuan-ptab@perkinscoie.com

PATENT OWNER:

James Glass
John McKee
Quincy Lu
Andrew Holmes
Ognjen Zivojnovic
QUINN EMANUEL URQUHART & SULLIVAN LLP
jimglass@quinnemanuel.com
johnmckee@quinnemanuel.com
quincylu@quinnemanuel.com
drewholmes@quinnemanuel.com
ogizivojnovic@quinnemanuel.com