

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC,
Patent Owner.

IPR2024-00213
Patent 9,338,140 B2

Before THOMAS L. GIANNETTI, STEPHEN E. BELISLE, and
DANIEL KAZHDAN, *Administrative Patent Judges*.

KAZHDAN, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Google LLC (“Petitioner”) filed a Petition (Paper 2, “Pet.”) requesting *inter partes* review of claims 1–10 (the “challenged claims”) of U.S. Patent No. 9,338,140 B2 (Ex. 1001, the “’140 patent”). Security First Innovations, LLC (“Patent Owner”) filed a Preliminary Response (Paper 7, “Prelim. Resp.”).

Congress gave the Director authority to determine whether to institute *inter partes* review, *see* 35 U.S.C. § 314, and she delegated that authority to the Board. *See* 37 C.F.R. § 42.4(a). The Board may not authorize an *inter partes* review unless the information in the petition and the preliminary response “shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a).

We determine that the Petition in this case does not establish a reasonable likelihood that Petitioner will prevail with respect to any of the challenged claims. We, therefore, deny institution of *inter partes* review.

II. BACKGROUND

A. Related matters

The parties identify the following proceedings as related matters:

- *Security First Innovations, LLC v. Google LLC*, No. 2:23-cv-00097 (E.D. Va.): Patent Owner accused Petitioner of infringing several of its patents, including the ’140 patent. The district court stayed the case pending our decision on whether to institute *inter partes* review. *See Security First*, ECF No. 313 (E.D. Va. Jan. 22, 2024).
- *Google LLC v. Security First Innovations, LLC*, Nos. IPR2024-00212 (U.S. Pat. No. 11,178,116), IPR2024-00214 (U.S. Pat. No.

IPR2024-00213
Patent 9,338,140 B2

11,068,609), and IPR2024-00215 (U.S. Pat. No. 10,452,854):
These three IPRs involve different patents.

See Patent Owner’s Mandatory Notices (Paper 4) at 1; Petitioner’s First Updated Mandatory Notices (Paper 6) at 1.

B. Real parties-in-interest

Both Petitioner and Patent Owner identify themselves as the real parties-in-interest. Pet. ix; Patent Owner’s Mandatory Notices (Paper 4) at 1. Petitioner states that it “is a subsidiary of XXVI Holdings Inc., which is a subsidiary of Alphabet Inc. XXVI Holdings Inc. and Alphabet Inc. are not real parties-in-interest to this proceeding.” Pet. ix n. 1.

C. The ’140 patent

The ’140 patent is titled “secure data parser method and system.” Ex. 1001, code (54).¹ The patent “relates in general to a system for securing data from unauthorized access or use.” *Id.* at 1:17–18. The ’140 patent explains that “an ever-increasing need exists for ensuring data stored and transmitted over [computer] systems cannot be read or otherwise compromised.” *Id.* at 1:27–29. “[O]ne aspect of the [’140 patent’s] invention” is to address this need by “provid[ing] a method for securing virtually any type of data from unauthorized access or use.” *Id.* at 2:33–35. “The method comprises one or more steps of parsing, splitting and/or separating the data to be secured into two or more parts or portions.” *Id.* at 2:35–37. In this manner, the “invention provides a system for securing virtually any type of data from unauthorized access or use.” *Id.* at 2:52–54.

¹ Throughout this decision, we alter the capitalization of the Title of patent applications and issued patents. For ease of reading, we do not separately note this fact each time.

Specifically, the '140 patent explains that portions of the data (or “shares”) can be secured by being distributed to multiple locations where clients can view the stored datasets but cannot view the underlying distribution of shares. *Id.* at 87:16–59; *see* Rubin Decl. (Ex. 2003) ¶¶ 36–38. The upside is that, because the data is split, “any possibility of compromise of secured data is effectively removed.” Ex. 1001 55:66–56:3.

D. Illustrative claim 1

The Petition challenges claims 1–10, of which only claim 1 is independent. Claim 1 is illustrative of the claimed subject matter and is reproduced below—with petitioner’s element labels added for convenience²:

1. [PRE] A secure storage network comprising:

[1A] a plurality of physical storage devices storing thereon a plurality of shares, the plurality of shares being associated with at least one session key used to secure a dataset; and

[1B] a secure storage system configured to:

[1B-1] present to a client device a virtual disk, the virtual disk comprising a directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device;

[1B-2] generate the plurality of shares for storage on the plurality of physical storage devices by performing a securing operation on the dataset received from the client device and distributing the dataset in the shares;

[1B-3] include with each of the plurality of shares data indicative of the at least one session key used to secure the dataset; and

[1B-4] reconstitute the dataset from at least a portion of the plurality of shares stored on the physical storage devices

² Patent Owner uses the same element labels. *See generally* Prelim. Resp.

in response to a request from the client device for information in the dataset.

Ex. 1001 98:2–22; Pet. 83.

E. Prior art references and other evidence

Petitioner raises four separate challenges (tabulated below in subsection II.F) using the following four prior art references:

- Sephy Ophir and Elic Yavor’s U.S. Patent Application Publication 2004/0143733 (Ex. 1007);
- Tsuneharu Takeda’s U.S. Patent Application Publication 2001/0053221 (Ex. 1008);
- Andrew Birrell *et al.*’s U.S. Patent No. 7,529,834 (Ex. 1033); and
- Alexander Dickinson *et al.*’s International Application Publication WO 2001/022322 (Ex. 1005).

Pet. 2. In addition to these references, Petitioner submitted a Declaration of Samrat Bhattacharjee, Ph.D. Ex. 1003. Patent Owner submitted a Declaration of Aviel Rubin, Ph.D. Ex. 2003.

F. Asserted grounds of unpatentability

Petitioner asserts the following four grounds of unpatentability. Pet. 2.

Claim(s) Challenged	35 U.S.C. §³	Reference(s)/Basis
1–6, 8, 10	103	Ophir, Takeda
7	103	Ophir, Takeda, Birrell
9	103	Ophir, Takeda, Dickinson

³ The ’140 patent issued from U.S. Patent Application No. 13/468,383 (the “383 application”), which was filed on May 10, 2012—i.e., before March 16, 2013. As such, the pre-AIA (“America Invents Act”) version of § 103 applies. *See* Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011). This decision’s citations to Section 103 are, therefore, to the pre-AIA version.

Claim(s) Challenged	35 U.S.C. § ³	Reference(s)/Basis
1–10	103	Dickinson, Takeda

G. The Petition and Patent Owner’s Preliminary Response

Petitioner provides an element-by-element analysis of the claims in relation to the prior art combinations. Pet. 6–78. Patent Owner’s Preliminary Response argues that the Petition “fails to demonstrate a reasonable likelihood of prevailing on at least one challenged claim.” Prelim. Resp. 1. It also argues that, because Dickinson was expressly considered by the Examiner, the Board should not reconsider the reference here. *See id.* at 44–47 (addressing 35 U.S.C. § 325(d)). *See infra*, Section III.D.3.

III. ANALYSIS OF THE CHALLENGED CLAIMS

A. Legal standards

Pre-AIA Section 103(a) provides that an inventor cannot receive a patent on an invention even if the invention is not anticipated under 35 U.S.C. § 102, “if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” The Supreme Court has explained that this analysis involves several factors: “the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved.” *KSR Int’l Co. v. Teleflex Inc.*,

550 U.S. 398, 406 (2007) (quoting *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966)).

We cannot institute an IPR unless “the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). By statute, “the petitioner shall have the burden of proving a proposition of unpatentability by a preponderance of the evidence.” 35 U.S.C. § 316(e); *see* 37 C.F.R. § 42.20(c) (“The moving party has the burden of proof to establish that it is entitled to the requested relief.”).

B. Level of ordinary skill in the pertinent art

According to Petitioner, a person of ordinary skill in the pertinent art “would have had at least a bachelor’s degree in computer science, computer engineering, or a related field, with three years of experience in the area of securing data from unauthorized access or use. A higher level of education may substitute for less experience.” Pet. 5 (citing Ex. 1003 ¶ 40). The Preliminary Response does not provide a description of the person of ordinary skill in the art or dispute Petitioner’s description. Patent Owner’s expert “accept[ed] Dr. Bhattacharjee’s proposed qualifications of a [skilled artisan]” for purposes of his declaration. Ex. 2003 ¶ 20.

For purposes of assessing institution, we adopt the formulation of the level of ordinary skill in the art proposed by Petitioner as it is consistent with the prior art before us in this proceeding.

C. Claim construction

We construe claim terms only as relevant to the parties’ contentions and only to the extent necessary to resolve the issues in dispute. *See Vivid*

Techs., Inc. v. Am. Sci. & Eng'g, Inc., 200 F.3d 795, 803 (Fed. Cir. 1999); *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). In IPR proceedings, we apply the claim construction standard governing federal courts—commonly called the “*Phillips* claim construction standard” after *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). See 37 C.F.R. § 42.100(b); *CUPP Computing AS v. Trend Micro Inc.*, 53 F.4th 1376, 1380 (Fed. Cir. 2022). Under that standard, “the words of a claim are generally given their ordinary and customary meaning” as understood by “a person of ordinary skill in the art in question at the time of the invention.” *Phillips*, 415 F.3d at 1312–13. “Importantly, the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification.” *Id.* at 1313. “In addition to consulting the specification, [the Federal Circuit has] held that a court should also consider the patent’s prosecution history, if it is in evidence.” *Id.* at 1317. Although “it is less significant than the intrinsic record in determining the legally operative meaning of claim language,” we may also look to “extrinsic evidence, which consists of all evidence external to the patent and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises.” *Id.*

Here the parties do not set out a clear claim construction dispute. The Petition includes a section on “claim interpretation” but does not list any terms as needing construction. Pet. 5–6. The Preliminary Response does not include such a section. This notwithstanding, there is a claim construction issue about how the recited “shares” are stored.

The Preliminary Response argues that limitations [1A] and [1B-2] “require storing two or more shares generated from a dataset on two or more physical storage devices.” Prelim. Resp. 5. This, purportedly, is “a central feature” of the invention. *Id.*; *see generally id.* at 4–7.

The relevant limitations recite: “[1A] a plurality of physical storage devices storing thereon a plurality of shares, the plurality of shares being associated with at least one session key used to secure a dataset” and a secure storage system configured to “[1B-2] generate the plurality of shares for storage on the plurality of physical storage devices by performing a securing operation on the dataset received from the client device and distributing the dataset in the shares.” *See* Ex. 1001 98:3–6, 98:12–15. As the Preliminary Response notes, the Federal Circuit has repeatedly held that “‘a plurality of’ means ‘at least two of.’” *SIMO Holdings Inc. v. Hong Kong uCloudlink Network Tech. Ltd.*, 983 F.3d 1367, 1377 (Fed. Cir. 2021) (citing cases); Prelim. Resp. 5. As the Preliminary Response further notes, the Petition itself seems to interpret the claims as requiring storage on at least two physical storage devices. Prelim. Resp. 7. Specifically, the Petition argues that “Dickinson-Takeda . . . stores encryption results . . . on **at least two** of storage devices D1-D4.” *Id.* (quoting Pet. 68); *see* Ex. 2003 ¶ 19. Implicit in this is the need for at least two separate physical storage devices. Thus, we conclude that the claims require storing the shares among two or more physical storage devices.

That does not resolve the issues because we still need to determine the scope of these separate “physical storage devices.” The specification provides some guidance. *First*, the specification contrasts storing shares in different “physical” locations with storing them in different “logical”

locations. *See* Ex. 1001 55:64–66. *Second*, the specification explains that “data shares [being] physically removed from the system” can be done “either by using a removable device, such as a data storage device, or by placing the share under another party’s control.” *Id.* at 55:66–56:3. *Third*, the specification gives the following examples of “suitable physical storage device[s]”: a “magnetic or optical disk” and a “USB key drive.” *Id.* at 66:4–6.

In light of these statements, we understand the requirement for storing on multiple “physical” storage devices to require storing the shares among at least two physical storage devices and those two devices need to be physically separable—e.g., two or more magnetic or optical disks or two or more USB key drives. Conversely, if such devices are not physically separable, then they are one physical storage device.

D. Description of the prior art references

1. Ophir (Ex. 1007)

Ophir is a U.S. patent publication titled “secure network data storage mediation.” Ex. 1007 Title; *see generally* Ex. 1003 ¶¶ 52–63. Ophir “relates to the secure storage of data over a network, and, more particularly, to a network mediating device for administering the security of data stored in devices connected over a network.” Ex. 1007 ¶ 1. Ophir teaches that “[t]he mediator connects over the network to one or more data clients and to one or more data storage devices, and provides secure storage of data for the data clients on the data storage devices.” *Id.* Abstract. The invention in Ophir is “a secure data storage mediator,” which Ophir illustrates in Figure 4, reproduced below. *Id.* ¶ 11.

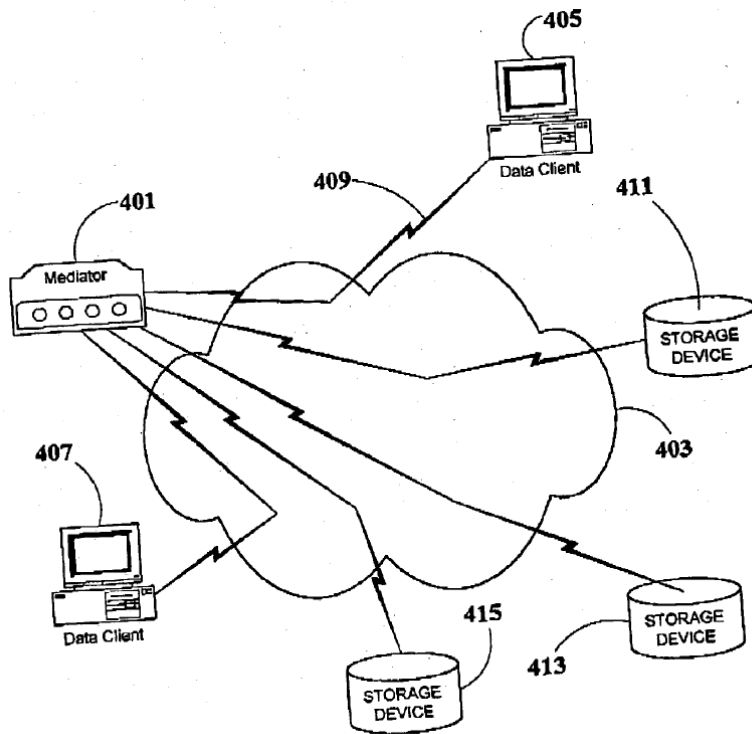


Figure 4 shows a mediator connected to a network where different data clients communicate with the mediator. *Id.* The mediator provides several different services to the clients, including “block device services, file services, and database services.” *Id.* ¶ 33 (numbers omitted). The mediator can also include an “[e]ncryption/decryption unit” that “encrypts data from the data clients into encrypted data for safe storage in data storage devices, and decrypts data retrieved from data storage devices into decrypted data for sending to data clients.” *Id.* ¶ 32. Ophir repeatedly emphasizes that the mediator can provide “secure virtual storage.” *Id.* Abstract; *see id.* ¶¶ 13, 33.

2. *Takeda (Ex. 1008)*

Takeda is a U.S. patent publication titled “ciphering apparatus and ciphering method.” Ex. 1008 Title; *see generally* Ex. 1003 ¶¶ 64–80. *Takeda* “relates to a ciphering apparatus and ciphering method.” Ex. 1008 ¶ 1.

Takeda explains that “conventional ciphering” divides stream data “into several regions (block) data, the respective blocks are subjected to a ciphering process, and all the data is ciphered.” *Id.* ¶ 3. The problem with conventional ciphering, Takeda explains, is that, “when a part of the ciphered data is deciphered, there is a risk or chance that all data will be deciphered.” *Id.* ¶ 4. One of Takeda’s goals “is to provide a ciphering apparatus using a ciphering technique in which even if a part of the data is deciphered, the rest of the data is not easily deciphered.” *Id.* ¶ 6. Takeda teaches dividing the text into separate parts in such a way that “the ciphering attribute of each part of the ciphertext can be changed.” *Id.* ¶ 9. In this way, “even if part of the ciphertext can be deciphered, the rest cannot be deciphered, and a more reliable ciphering technique can be provided.” *Id.*

3. *Dickinson (Ex. 1005)*

Dickinson is an international patent publication titled “electronic commerce with cryptographic authentication.” Ex. 1005 Title; *see generally* Ex. 1003 ¶¶ 32–36, 42–47, 188, 193–199. Petitioner provides a red-line comparison demonstrating that the ’140 patent includes many disclosures verbatim from Dickinson, while adding many new disclosures as well. *See* Ex. 1040 (comparing Dickinson and the ’140 patent).

Dickinson “relates to cryptographic authentication in electronic commerce” and, “[m]ore specifically, . . . to the use of cryptographic authentication to provide security to transactions in electronic commerce.” Ex. 1005 1:6–8. There is a trade-off, Dickinson explains, between security and convenience. *Id.* at 1:25–26. Dickinson’s goal is to “provide users and vendors with levels of security in authentication appropriate to the transactions being carried out while improving the ease of use of such

authentication for common tasks.” *Id.* at 2:3–5. Dickinson discloses that this can be accomplished by “provid[ing] a secure server, or trust engine, having server-centric keys, or in other words, storing cryptographic keys and user authentication data on a server.” *Id.* at 2:10–11.

Dickinson discloses that sensitive data (passwords, logins, credentials, etc.) can be stored in a “sensitive data vault.” *Id.* at 29:13–23. Dickinson discloses using “data splitting modules to divide sensitive data into undecipherable portions” and then “distributing the sensitive data into distinct and independent storage facilities . . . some or all of which may be advantageously geographically separated.” *Id.* at 19:32–20:5. The split data is encrypted with separate keys, and these are stored separately so “no single data storage facility . . . includes sufficient encrypted data to recreate the original sensitive data.” *Id.* at 20:25–21:12.

During examination of the ’140 patent, the Examiner analyzed Dickinson at length. *See, e.g.*, Ex. 1002 at 326–331, 740–746, 1235–1242. Particularly relevant is the Examiner’s rejection of application claim 14, which issued as claim 1 of the ’140 patent, reproduced above, with one important exception: application claim 14 did not have limitation [1B-3].⁴ *See id.* at 1247. The Examiner found that Dickinson taught all the claim limitations except [1B-1], which the Examiner found is disclosed by a reference that is not before us in this proceeding. *Id.* at 1235–1239. In response, the applicant added limitation [1B-3] and argued that “Dickinson does not teach or suggest including with each of the plurality of shares data

⁴ Limitation [1B-3] requires the secure storage network to “include with each of the plurality of shares data indicative of the at least one session key used to secure the dataset.”

indicative of the at least one session key used to secure the dataset, as claimed.” *Id.* at 1245–1246. The Examiner then allowed the claim. *Id.* at 1360.

E. Grounds 1–3: Obviousness of claims 1–10 over the combination of Ophir and Takeda and, for some claims, Birrell or Dickinson

1. Claim 1

Petitioner asserts that claim 1 would have been obvious over Ophir and Takeda—providing an element-by-element claim analysis, supported by expert testimony. *See* Pet. 6–43; Ex. 1003 ¶¶ 52–156. Patent Owner disputes this analysis and presents its own supporting expert testimony. Prelim. Resp. 3–32; Ex. 2003 ¶¶ 33–99.

As explained in the claim construction section above, for purposes of this decision we construe limitations [1A] and [1B-2] together to require storing two shares among at least two physical storage devices. Petitioner never addresses this requirement, and we find this to be a fatal flaw.

According to Petitioner, Takeda teaches limitations [1A] and [1B-2] as follows: “Takeda’s technique involves dividing plaintext – which is any non-encrypted (i.e., unciphered) information – into blocks, ciphering different blocks using different ‘ciphering attributes’ (e.g., ciphering keys and/or ciphering algorithms), and outputting the ciphered blocks with the ciphering attributes.” Pet. 10; *see generally id.* at 10–16, 28–31, 39–40. Patent Owner responds that “Takeda’s blocks are stored together in a single storage device,” and this does not disclose or suggest storing the shares on at least two physical storage devices. Prelim. Resp. 8; *see id.* at 8–9 (citing Ex. 2003 ¶¶ 51–53).

We agree with Patent Owner. Petitioner has not shown a reasonable likelihood that Takeda discloses or suggests storing data on physically separable storage devices. The Petition points to Takeda’s teaching that the data is “divided into blocks.” Pet. 11. As Patent Owner notes, Takeda teaches that these blocks are all stored on a single, physical device. Prelim. Resp. 8. Specifically, Takeda teaches that “[t]he ciphertext is stored in the removable recording medium 39 or the storage device 37.” Ex. 1008 ¶ 92.⁵ We determine that Takeda does not teach or suggest storing this data in at least two separate media, at least two separate storage devices, or at least one of each. Correspondingly, Takeda’s Figures show data blocks next to each other—i.e., on one physical device. *See id.* at Figs. 1–4. The Petition does not suggest that Ophir teaches storing shares among different physical storage devices. As the Petition itself notes, Ophir seems to use a single “mediator [to] provide[] secure virtual storage to data clients.” Pet. 9 (quoting Ex. 1007 Abstract) (emphasis omitted).

Ultimately, the Petition’s Grounds 1–3 do not address the limitation of storing on multiple storage devices. This is a limitation that the ’140 patent itself stresses as important for maintaining security. *See* Ex. 1001 55:66–56:3; Ex. 2003 ¶ 44. As Patent Owner’s expert Dr. Rubin explains:

What is missing [in the Petition] is any indication or argument that . . . a POSITA would be motivated to divide Takeda’s blocks from a given dataset across two or more of Ophir’s physical storage devices. That was the inventors’ insight

Ex. 2003 ¶ 61. We therefore determine that Petitioner does not demonstrate a reasonable likelihood of showing obviousness of claim 1 in Ground 1.

⁵ We prefer not bolding reference numerals and thus omit such bolding throughout—even where the underlying source document has such bolding.

Because we find that there is no reasonable likelihood of showing obviousness for this reason, we do not reach Patent Owner’s other arguments. *See* Prelim. Resp. 15–21, 24–32.

2. *Claims 2–10*

Petitioner’s challenges to dependent claims 2–6, 8, and 10 in Ground 1; dependent claim 7 in Ground 2; and dependent claim 9 in Ground 3 rely on the purported obviousness of claim 1. *See* Pet. 43–53. For the reasons given for claim 1, we determine that Petitioner fails to demonstrate a reasonable likelihood of prevailing on these challenges.

F. Ground 4: Obviousness of claims 1–10 over the combination of Dickinson and Takeda

Petitioner also asserts that claims 1–10 would have been obvious over the combination of Dickinson and Takeda—providing an element-by-element claim analysis, supported by expert testimony. *See* Pet. 54–81; Ex. 1003 ¶¶ 193–262. Patent Owner opposes and likewise has supporting expert testimony. Prelim. Resp. 33–67; Ex. 2003 ¶¶ 100–168.

Patent Owner’s opposition focuses on claim limitations [1B-1] and [1B-3]—the two limitations that the Examiner found were not disclosed in Dickinson. *See* discussion in Section III.D.3, *supra*. We find that the Petition has not shown a reasonable likelihood that limitation [1B-1] is disclosed or suggested. We therefore do not address the other limitations.

1. *Limitation [1B-1]*

Limitation [1B-1] recites a secure storage system configured to “present to a client device a virtual disk, the virtual disk comprising a

directory mapped to the plurality of physical storage devices such that physical locations of the shares are hidden from the client device.” We focus on the requirement that the “physical locations of the shares are hidden from the client device.”

Petitioner relies on Dickinson’s disclosures for this limitation. *See* Pet. 71–74. The Petition points to two sections of Dickinson in arguing that Dickinson discloses keeping the “physical locations of the shares . . . hidden from the client device.” *Id.* at 72 (citing Ex. 1005 16:28–31, 29:12–30:2). However, the Petition does not explain the relevance of these sections. Dr. Bhattacharjee’s declaration cites those same portions of Dickinson but with no further explanation. *See* Ex. 1003 ¶ 229. We examine both.

(1) The first cited passage is to Dickinson’s analysis of Figure 4, which is reproduced below.

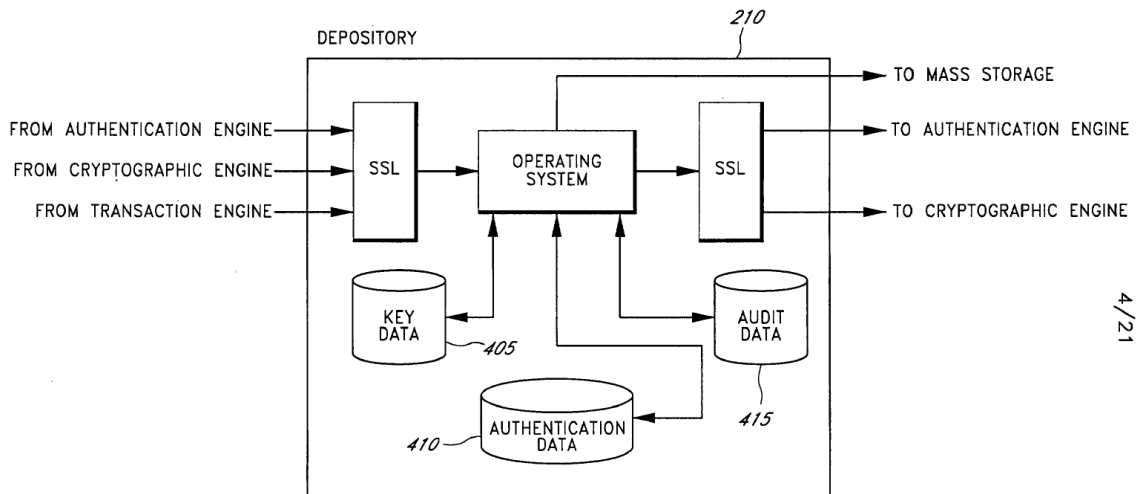


Figure 4 is a block diagram of the depository in Dickinson’s trust engine. *See* Ex. 1005 7:34–8:6. Dickinson provides the following description of Figure 4:

FIGURE 4 also shows that the directory server preferably stores data 405 corresponding to the cryptographic keys and data 410

corresponding to the enrollment authentication data. According to one embodiment, the depository 210 comprises a single logical memory structure indexing authentication data and cryptographic key data to a unique user ID.

Id. at 16:28–31. Petitioner does not explain the relevance of this passage, and Patent Owner argues that the passage “does not mention hiding the location of shares from the client device or storage facilities D1-D4.” Prelim. Resp. 54; *see* Ex. 2003 ¶ 138.

We agree with Patent Owner. While the cited disclosure from Dickinson mentions “cryptographic keys,” we see nothing in this disclosure about hiding the physical locations of the shares from the client device.

(2) The second cited passage relates to Dickinson’s discussion of Figure 10, which is reproduced below.

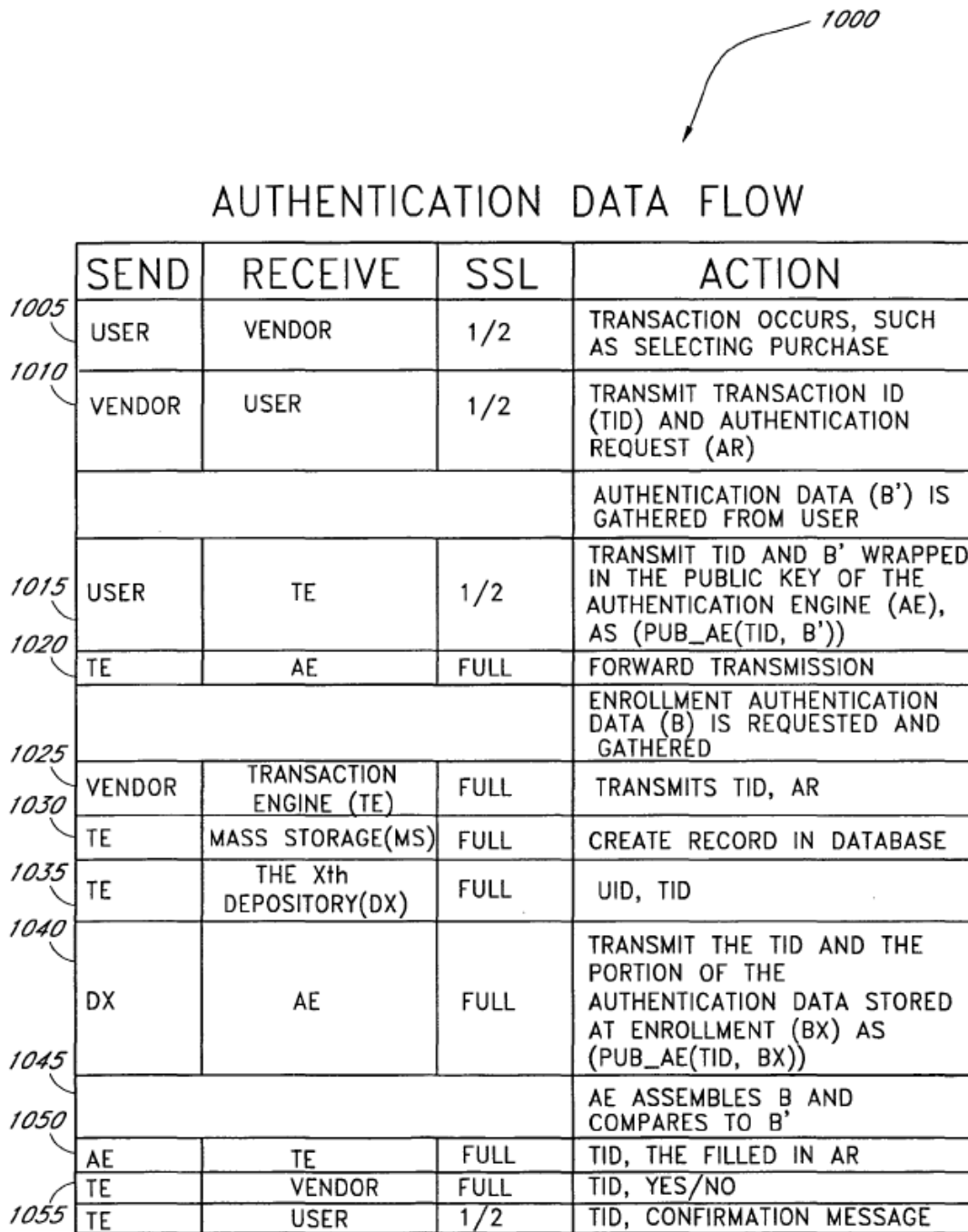


Figure 10 “illustrates a data flow of an authentication process according to aspects of an embodiment of the invention.” Ex. 1005 8:19–20. The Petition cites several paragraphs in Dickinson that discuss this authentication process. See Pet. 71 (citing Ex. 1005 29:12–30:2). Again, Petitioner does not

explain how the discussion is relevant. Patent Owner responds that “[t]here is no suggestion [in the cited passages] that the physical locations of the shares are ‘hidden from the client device.’” Prelim. Resp. 54. We agree. We see no disclosure of hidden locations in the citations provided by Petitioner. Therefore, we find that Petitioner has not shown a reasonable likelihood of prevailing on its challenges based on Dickinson and Takeda.

IV. DISCRETIONARY DENIAL

Section 325(d) of 35 U.S.C. provides that, “[i]n determining whether to institute or order [an IPR proceeding], the Director may take into account whether, and reject the petition or request because, the same or substantially the same prior art or arguments previously were presented to the Office.” Patent Owner argues that we should exercise our discretion under 35 U.S.C. § 325(d) and not institute trial in view of the fact that Dickinson was before the Examiner during prosecution. Prelim. Resp. 44–47. As discussed above, we ultimately find that Petitioner has failed to show a reasonable likelihood of prevailing on the merits. We therefore do not reach the question of discretionary denial.

V. CONCLUSION

For these reasons, we have determined that Petitioner has not shown a reasonable likelihood of prevailing with respect to any challenged claims. Thus, we do not institute *inter partes* review.

VI. ORDER

Upon consideration of the record before us, it is ORDERED that the Petition is *denied*, and no trial is instituted.

IPR2024-00213
Patent 9,338,140 B2

For PETITIONER:

Elisabeth H. Hunt
Richard F. Giunta
Thomas A. Franklin
WOLF, GREENFIELD & SACKS, P.C.
ehunt-ptab@wolfgreenfield.com
rgiunta-ptab@wolfgreenfield.com
mjohannes-ptab@wolfgreenfield.com

For PATENT OWNER:

Stephen Elliott
Andrei Iancu
SULLIVAN & CROMWELL LLP
elliotts@sullcrom.com
iancua@sullcrom.com

Kenneth Weatherwax
LOWENSTEIN & WEATHERWAX LLP
weatherwax@lowensteinweatherwax.com