In the United States Court of Federal Claims

No. 17-307
(Filed: 20 January 2023)

MICHAEL HADDAD,	*	
	*	
Plaintiff,	*	
	*	
v.	*	
	*	
THE UNITED STATES,	*	
	*	
Defendant,	*	Claim Construction; *Markman* Hearing;
	*	Plain and Ordinary Meaning; Means Plus
TRANS DIGITAL TECHNOLOGIES LIMITED LIABILITY COMPANY,	*	Function; Intrinsic Record; Indefinite;
	*	Person Having Ordinary Skill in the Art;
	*	28 U.S.C. § 112.
Third-Party Defendant,	*	
	*	
and	*	
	*	
IDEMIA IDENTITY & SECURITY USA LLC,	*	
	*	
	*	
Third-Party Defendant.	*	
	*	

Geoffrey Mason, MOARBES, LLP, of Washington, DC, for plaintiff.

Conrad J. DeWitte, Jr., Assistant Director, with whom were *Gary L. Hausken*, Director, Commercial Litigation Branch, and *Brian M. Boynton*, Principal Deputy Assistant Attorney General, Civil Division, Department of Justice, all of Washington, DC, for defendant.

Richard L. Brophy, Armstrong Teasdale LLP, of St. Louis, MO, for third-party defendants Trans Digital Technologies LLC and Idemia Identity & Security USA LLC.

CLAIM CONSTRUCTION OPINION AND ORDER

HOLTE, **Judge.**

Plaintiff Michael Haddad accuses the government of infringing U.S. Patent No. 7,639,844. The government noticed Trans Digital Technology LLC and Morpho Trust USA, LLC (now Idemia Identity & Security USA LLC), distributors of the allegedly infringing

product, who joined the government in defending the claims against patent infringement. The parties filed claim construction briefs seeking to construe the meaning of various disputed claim terms. The Court held a *Markman* hearing to construe the disputed terms. Defendants argue thirteen of the fifteen claim terms are indefinite under 35 U.S.C. § 112. This Claim Construction Opinion and Order construes the disputed terms and finds sole independent claim 1 indefinite and accordingly finds the entire '844 patent invalid. The Court further orders the plaintiff to show cause why this case should not be dismissed.

I. Background

A. Patents, Property, and Presumption of Validity

In 1876, the Supreme Court held "[a] patent for an invention is as much property as a patent for land. The right rests on the same foundation, and is surrounded and protected by the same sanctions." *Consol. Fruit-Jar Co. v. Wright*, 94 U.S. 92, 96 (1876). In more recent years, the Supreme Court has established the right to exclude as "one of the most essential sticks in the bundle of rights that are commonly characterized as property." *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979). The Federal Circuit confirms "a patent grants only the right to exclude others and confers no right on its holder to make, use, or sell [an invention]." *Bio-Tech. Gen. Corp. v. Genentech, Inc.*, 80 F.3d 1553, 1559 (Fed. Cir. 1996) (quoting *Vaupel Texilmaschinen KG v. Meccanica Euro Italia S.P.A.*, 944 F.3d 870, 879 n.4 (Fed. Cir. 1991)) (internal quotations omitted).

In addition to patents being property, "[p]atents are presumed to be valid." *Procter & Gamble Co. v. Teva Pharm. USA, Inc.*, 566 F.3d 989, 994 (Fed. Cir. 2009) (citing *Kao Corp. v. Unilever U.S., Inc.*, 441 F.3d 963, 968 (Fed. Cir. 2006)). "[T]he [United States] Patent and Trademark Office [('USPTO')] only grants those patent applications that meet the statutory patentability requirement." Adam Mossoff, *Who Cares What Thomas Jefferson Thought about Patents–Reevaluating the Patent Privilege in Historical Context*, 92 Cornell L. Rev. 953, 999 (2007) (citing *Intervet Am., Inc. v. Kee-Vet Labs., Inc.*, 887 F.2d 1050, 1054 (Fed. Cir. 1989) ("The presumption of validity under 35 U.S.C. § 282 carries with it a presumption the examiner did his duty and knew what claims he was allowing"); *Am. Hoist & Derrick Co. v. Sowa & Sons, Inc.*, 725 F.2d 1350, 1359 (Fed. Cir. 1984) (noting § 282 is based on the "basic proposition that a government agency such as the then Patent Office was presumed to do its job")). "The burden of establishing invalidity of a patent claim . . . rest[s] on the party asserting invalidity." 35 U.S.C. § 282(a). "An issued patent enjoys a presumption of validity[, and] a party challenging patent validity has the burden to prove its case with clear and convincing evidence." *Impax Labs., Inc. v. Aventis Pharm., Inc.*, 545 F.3d 1312, 1314 (Fed. Cir. 2008).

B. Factual History

Plaintiff Michael Haddad is the sole inventor, owner, and assignee of U.S. Patent No. 7,639,844 ("the '844 patent"). Compl. ¶¶ 1, 6, 9, ECF No. 1. The '844 patent is a "[c]ontinuation-in-part of [U.S.] application No. 11/220,282 [('the '282 application')], filed on 7 September 2005, now Pat[ent] No. 7,401,732 [('the '732 patent')], and a continuation-in-part of

[U.S.] application No. 10/330,981, filed on 30 December 2002, now abandoned." '844 patent at [63].

The '844 patent, titled "Airport Vehicular Gate Entry Access System," relates to methods of "securing airport vehicular gate entries by providing" "means of authenticating drivers' licenses, verifying employee status, printing temporary passes, printing a temporary vehicle entry pass and certificate" and "providing the airport police with a handheld apparatus capable of reading the entry certificate and wirelessly verifying its authenticity." *Id.* at [54], [57]. The system also provides means of matching vehicle drivers and passengers "against the TSA NO-FLY and SELECTEE lists." *Id.* at [57]. The system is "fully automated and is touch screen capable, thus requiring a minimal amount of human interaction." *Id.*

C. Procedural History

Plaintiff filed his complaint on 6 March 2017, alleging the Credential Authentication Technology-Boarding Pass Scanning System ("CAT/BPSS") used by the government and provided by third-party defendants Trans Digital Technology LLC ("TDT") and Idemia Identity & Security USA LLC[1] ("Idemia") (collectively "defendants") for its airport security systems infringes the '844 patent. *See* Compl. ¶¶ 15–16, 19, 33. The government moved to notice interested third parties, BAE Systems Information Solutions, Inc., NCR Government Systems, LLC, Trans Digital Technologies, Inc., and MorphoTrust USA, Inc., and the interested third parties were noticed on 3 May 2017. Mot. for Notice to Third Parties, ECF No. 8; *see* Notice to Third Parties, ECF No. 11. On 28 February 2018, this court dismissed plaintiff's claims for patent infringement accruing prior to 27 October 2016. *See* Order Granting Gov't's Mot. to Dismiss at 15–16, ECF No. 39. On 27 July 2018, this court dismissed third-party defendants BAE Systems Information Solutions, Inc. and NCR Government Systems, LLC. *See* Order Dismissing Third-Party Defs. at 2, ECF No. 45. This case was reassigned to the undersigned judge on 29 July 2019. *See* Order, ECF No. 81.

On 9 February 2021, defendants filed a joint status report stating each party's views on a proposed discovery schedule, whether the parties had claim construction disputes, and each party's proposed schedule for claim construction briefing. *See* Joint Status Report, ECF No. 116. On 16 February 2021, the Court issued a scheduling order for the exchange of: preliminary infringement contentions; preliminary invalidity contentions; claim terms for construction; proposed claim constructions; and extrinsic evidence supporting claim construction positions. *See* Scheduling Order at 2–3, ECF No. 117. On 19 March 2021, defendants filed a motion to compel plaintiff to serve supplemental infringement contentions. *See* Mot. to Compel, ECF No. 120. After the parties fully briefed the issue, the Court denied the motion to compel as moot when plaintiff agreed to serve infringement contentions. *See* Order, ECF No. 131.

On 23 November 2021, defendants filed their opening claim construction brief. *See* Defs.' Opening Claim Construction Br. ("Defs.' Cl. Constr. Br."), ECF No. 137. Plaintiff filed his response to defendants' opening claim construction brief on 20 December 2021. *See* Pl.'s Resp. to Defs.' Opening Claim Construction Br. ("Pl.'s Resp. Cl. Constr. Br."), ECF No. 140.

[1] Idemia Identity & Security USA LLC was formerly known as MorphoTrust USA, LLC. Notice of Name Change, ECF No. 60.

On 7 January 2022, defendants filed their reply to plaintiff's response. *See* Defs.' Reply Claim Construction Br. ("Defs.' Reply Cl. Constr. Br."), ECF No. 141. Plaintiff filed a surreply to defendants' reply on 21 January 2022. *See* Pl.'s Surreply Claim Construction Br. ("Pl.'s Surreply Cl. Constr. Br"), ECF No. 144. The Court held a *Markman* hearing on 12 July 2022. *See* Order, ECF No. 151.

D. The Technology of the '844 Patent

On 27 August 2007, plaintiff filed U.S. Patent Application No. 11/895,656, later issued as the '844 patent. *See* '844 patent at [10], [21]–[22]. Plaintiff asserts infringement of sole independent claim 1 of the '844 patent and dependent claims 3, 5, and 6. *See* Compl. ¶¶ 19–32.

The '844 patent "relates to a method of securing airport vehicular gate entry/exit gates" by allowing "security personnel to process a vehicle entry as a group of verifiable objects interrelated, including an employee host, a vehicle registration card, a vehicle driver and vehicle passengers." '844 patent col. 1 ll. 13–14, 36–39. The background of the '844 patent describes the field as being "prone to excessive error rates, lower security standards, increased inefficiencies and decreased reliability" because "[a]irport vehicular entry gates rely on human intervention and manual data entry." *Id.* col. 1 ll. 22–25. The patent discloses "an enterprise platform where multiple airport vehicular gates comprise one workstation each, interconnected in a network configuration, controlled by a central database server" making "all data immediately available at all workstations" because "[a]ll workstations collect and store data in the central database server." *Id.* col. 2 ll. 41–45. The platform "uses a computer system, the apparatus of [the '282 application], and the software application of [the '282 application] customized for the purpose [of providing], a commercial [i]dentification card authentication apparatus, and various computer peripherals." *Id.* col. 1 ll. 40–44.

The system provides an "entry/exit workstation" for airport gate attendants, "which would be located at an airport vehicular gate booth" preferably having "a touch screen LCD" or another display screen. *Id.* col. 2 ll. 31–38. The workstation contains a "reader for standardized personal identification credentials, . . . a suitable camera, . . . a central processing unit color, . . . plastic card printers, . . . one ID card authenticator, . . . a keyboard, a laser printer, . . . and a display monitor." *Id*. (cleaned up). Each workstation is "interconnected in a network configuration, controlled by a central database server," and "[a]ll workstations collect and store data in the central database server." '844 patent col. 2 ll. 42–45. Figure 1, reproduced below, "schematically illustrates the elements of an entry/exit workstation." '844 patent col. 2 ll. 31–32, fig.1.

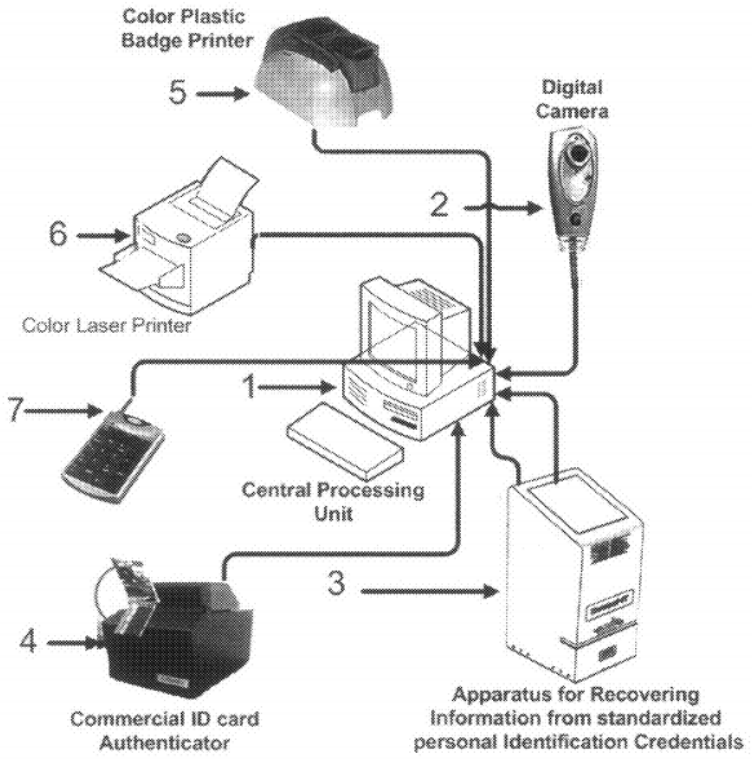

FIG. 1

The system provides "a vehicle entry . . . formed of a group of collected records, processed sequentially" including the following records: "1–ESCORTER"; "2–[Department of Motor Vehicles ('DMV')] Vehicle Registration Information"; "3–Driver Information"; and "4–Passengers Information." *Id.* col. 2 ll. 58–64. "Upon the arrival of a vehicle at an airport vehicular entry gate," an airport employee "presents its airport ID to the reader for standardized personal identification credentials device" and is then requested "to enter a security code in the numeric keypad." *Id.* col. 2 l. 65–col. 3 l. 3. "The information read from the ID serves to locate the ESCORTER record in the airport employee database," "verifies employment status," and "[i]f active . . . match[es the employee] against the TSA NO-FLY and SELECTEE lists." *Id.* col. 3 ll. 5–9. The system "provides a security alert if the employee is not active" or "matched during the TSA NO-FLY and SELECTEE list search." *Id.* col. 3 ll. 9–13.

"After processing the employee, the employee becomes the ESCORTER of the entry group," and the system "automatically moves into the vehicle registration mode." *Id.* col. 3 ll. 19–21. "The gate attendant places the DMV vehicle registration card in the authenticator, as requested by the display message," which in turn "acquires an image of the registration card." '844 patent col. 3 ll. 25–28. The authenticator then "sends the image to the system for proceeding with character recognition" which "becomes the second record in the entry group." *Id.* col. 3 ll. 29–30.

"The system automatically moves into the DRIVER mode," requiring the gate attendant to "follow[] operational steps" such as presenting a credential to the reading apparatus and following the "warning window" message if prompted. *Id.* col. 3 ll. 31, 35–38, 49. When a

credential "is presented to the reading apparatus, . . . [t]he system decodes the encoded data and encrypts the sensitive information, . . . checks database information to determine whether the individual is an employee," and checks the "ID credential against the TSA NO-FLY and SELECTEE lists." *Id.* col. 3 ll. 37–48. "If all checks are negative, the process continues. The system picks up the individual photo provided by the authenticator returned record, and prints a time sensitive encoded temporary pass." *Id.* col. 3 ll. 61–64.

"Upon completing the DRIVER entry record, the system moves automatically into the 'PASSENGER' mode . . . ." *Id.* col. 3 ll. 65–66. "The gate attendant proceeds with collecting passengers' records, one after another, in a sequential manner, following the same functional steps mentioned earlier during the DRIVER ID processing." '844 col. 4 ll. 3–6. The gate attendant then selects the "'CERTIFICATE' touch button" on the screen causing the "printing of the Temporary Vehicle Entry Certificate and Permit" which "is to be displayed at the vehicle windshield." *Id.* col. 4 ll. 15–16, 29. "A wireless handheld apparatus reader . . . is provided to the airport police to read the certificate on the premises and instantly verify the displayed certificate records, through a wireless access to the system database." *Id.* col. 4 ll. 30–33.

E. Overview of Claims

Plaintiff asserts infringement of claims 1, 3, 5, and 6. These claims are directed toward a CAT/BPSS. *See* Compl. ¶¶ 19–32. Claims 3, 5, and 6 depend on claim 1.

Based on the Court's detailed review of the patents, the disputed terms appear in the claims as follows:

Term #	Disputed Term	Applicable Claim(s)
1	"standardized credential reader means"	Claim 1
2	"credential encoded with personal identification"	Claims 1, 3
3	"build individual real time records"	Claim 1
4	"credential collected information match"	Claim 1
5	"system database"	Claims 1, 5, 6
6	"the type of entry, visitor, employee, contractor, supplier, or vendor, is determined"	Claim 1
7	"an ID authenticator"	Claim 1
8	"means to read non-encoded credentials"	Claim 1
9	"authentication data record"	Claim 1
10	"authenticity risk rating" / "authentication rating" / "ID forgery risks rating"	Claim 1
11	"automatically determines the source"	Claim 1
12	"credential data record"	Claim 1
13	"to be checked against a security list, TSA NO-FLY list, SELECTEE list, other alternative credentials"	Claim 1
14	"warning window[, as a result of the individual credentials match and ID forgery risks rating contained in the authentication data record]"	Claim 1

15	"individual credentials match"	Claim 1

Claim 1 of the '844 patent, reproduced below, provides a representative example of all of the disputed claim terms:

> 1. An automated access control system for securing airport vehicular gates and airport sterile areas comprising:
>
> a *standardized credential reader means* for reading a *credential encoded with personal identification* to be used at entry point into the airport sterile areas and automatically collects data to *build individual real time records*;
>
> a software application for recovering information from the standardized credential reader, wherein one or more of the following processing is performed:
>
> real time records are checked searching for a *credential collected information match*; individual suspicious status is checked against a security list stored in a *system database*; employee records are checked to determine if the individual is an employee; the *type of entry, visitor, employee, contractor, supplier, or vendor, is determined*; and admission is processed as entry or re-entry of the individuals,
>
> an *ID authenticator*, wherein a credential to be authenticated is presented, a credential physical aspect and embedded security features are analyzed to determine the possibility of any tempering or forgery and provide an *authenticity risk rating*, said *ID authenticator* comprises *means to read non-encoded credentials*, whereas said *ID authenticator* generates an *authentication data record* comprising presented credential information and *authentication rating*,
>
> a central processing unit for receiving information from the standardized credential reader and the ID authenticator;
>
> wherein, upon a credential reading, the automated access control system automatically determines the source of the *credential data record*, and automatically extracts personal *information to be checked against a security list, TSA NO-FLY list, SELECTEE list, other alternative credentials*; whereas upon the credential authentication, the automated access control system automatically extracts authentication information from the authentication data record, and subsequently displays a *warning window*, as a result of the *individual credentials match* and *ID forgery risks rating* contained in the *authentication data record*.

Claim 3 of the '844 patent, reproduced below, provides a representative example of one disputed claim term ("credential encoded with personal identification") indicated in italics:

> 3. An automatic access control system as claimed in claim 1, wherein the standardized credential reader can read any one of: drivers license identification, passports, boarding passes or any other standardized *credentials* presented as a *personal identification* upon entry into the airport, and whereas standardized credentials refer to identification documents *encoded* using established standards.

Claim 5 of the '844 patent, reproduced below, provides a representative example of one disputed claim term ("system database") indicated in italics:

> 5. An automated access control system as claimed in claim 1, wherein the *system database* includes one or more interrelated group of records: the airport employee as ESCORTER, the DMV vehicle registration card information, the driver identification record and the passengers' identification records.

Claim 6 of the '844 patent, reproduced below, provides a representative example of one disputed claim term ("system database") indicated in italics:

> 6. An automated access control system as claimed in claim 1, includes: a wireless barcode reader, a *system database*, a suitable camera, a color plastic card printer, a keyboard, a laser printer, an intranet package and a display monitor.

'844 patent col. 4 l. 66–col. 6 l. 18.

II. Applicable Law for Claim Construction

A. Claim Term Interpretation

"[T]he interpretation and construction of patent claims, which define the scope of the patentee's rights under the patent, is a matter of law exclusively for the court." *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 970–71 (Fed. Cir. 1995). "To construe a claim term, the trial court must determine the meaning of any disputed words from the perspective of one of ordinary skill in the pertinent art at the time of filing."[2] *Chamberlain Grp. Inc. v. Lear Corp.*, 516 F.3d 1331, 1335 (Fed. Cir. 2008). "[T]he words of a claim 'are generally given their ordinary and customary meaning,' . . . [and] the ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)). "There are only two exceptions to this general rule: (1) when a patentee sets out a definition and acts as his

[2] At oral argument, the parties agreed none of their claim constructions rely on one particular definition of a person having ordinary skill in the art ("PHOSITA"), and the Court need not decide the parties' dispute over who a PHOSITA is at this stage. Cl. Constr. Tr. ("Tr.") at 10:2–11, ECF No. 153 ("THE COURT: [I]s it plaintiff's understanding that there's any argument about specific terms that would be affected by the definition of PHOSITA? [PLAINTIFF]: No, you honor, I don't think we have to decide at this point. . . . THE COURT: [D]o defendants believe that there is any specific claim construction that may be affected by PHOSITA definition? [DEFENDANTS]: Not in this case . . . ."). *See also Cave Consulting Grp., Inc. v. Truven Health Analytics Inc.*, No. 15-cv-02177-SI, 2016 WL 2902234, at *3 (N.D. Cal. May 13, 2016).

own lexicographer, or (2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution." *Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (citing *Vitronics*, 90 F.3d at 1580).

The analysis of any disputed claim term begins with the intrinsic evidence of record, as "intrinsic evidence is the most significant source of the legally operative meaning of disputed claim language." *Vitronics*, 90 F.3d at 1582. Additional claims, whether asserted or not, "can also be valuable sources of enlightenment as to the meaning of a claim term" when determining consistent language usage throughout the patent, differences amongst particular terms, and various limitations added throughout the dependent claims. *Phillips*, 415 F.3d at 1314. The claims do not stand on their own; "they are part of 'a fully integrated written instrument,' consisting principally of a specification that concludes with the claims." *Id.* at 1315 (quoting *Markman*, 52 F.3d at 978). The claims are therefore read in view of the specification. *Markman*, 52 F.3d at 979. It is important limitations from preferred embodiments are not read "into the claims absent a clear indication in the intrinsic record that the patentee intended the claims to be so limited." *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 913 (Fed. Cir. 2004).

Federal Circuit caselaw "instructs that different claim terms are presumed to have different meanings." *MicroStrategy Inc. v. Bus. Objects Americas*, 238 F. App'x 605, 609 (Fed. Cir. 2007) (citing *CAE Screenplates, Inc. v. Heinrich Fiedler GmbH & Co. KG*, 224 F.3d 1308, 1317 (Fed. Cir. 2000) ("In the absence of any evidence to the contrary, we must presume that the use of these different terms in the claims connotes different meanings."); *Applied Med. Res. Corp. v. U.S. Surgical Corp.*, 448 F.3d 1324, 1333 n.3 (Fed. Cir. 2006) ("[T]he use of two terms in a claim requires that they connote different *meanings* . . . .")).

B. Prosecution History Weight and Interpretation

The prosecution history may serve as an additional source of intrinsic evidence. *Markman*, 52 F.3d at 980. The prosecution history "consists of the complete record of the proceedings before the [USPTO] and includes the prior art cited during the examination of the patent." *Phillips*, 415 F.3d at 1317. The prosecution history "represents an ongoing negotiation between the [US]PTO and the applicant, rather than the final product of that negotiation." *Id.* "Any explanation, elaboration, or qualification presented by the inventor during patent examination is relevant, for the role of claim construction is to 'capture the scope of the actual invention' that is disclosed, described, and patented." *Iridescent Networks, Inc. v. AT&T Mobility, LLC*, 933 F.3d 1345, 1352–53 (Fed. Cir. 2019) (quoting *Fenner Invs., Ltd. v. Cellco P'ship*, 778 F.3d 1320, 1323 (Fed. Cir. 2015)). After considering all intrinsic evidence of record, the court has discretion to consider sources of extrinsic evidence, such as dictionaries, treatises, and expert and inventor testimony, "if the court deems it helpful in determining 'the true meaning of language used in the patent claims.'" *Phillips*, 415 F.3d at 1318 (quoting *Markman*, 52 F.3d at 980). While sometimes helpful, extrinsic evidence is "less significant than the intrinsic record in determining the legally operative meaning of claim language." *Id.* at 1317 (internal quotation marks and citations omitted) (quoting *C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 862 (Fed. Cir. 2004).

"Prosecution disclaimer 'preclud[es] patentees from recapturing through claim interpretation specific meanings disclaimed during prosecution.'" *Aylus Networks, Inc. v. Apple Inc.*, 856 F.3d 1353, 1359 (Fed. Cir. 2017) (quoting *Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1323 (Fed. Cir. 2003)). Federal Circuit caselaw "requires that the alleged disavowing actions or statements made during prosecution be both clear and unmistakable" in order to apply the principles of prosecution disclaimer. *Id.* "[W]hen the patentee unequivocally and unambiguously disavows a certain meaning to obtain a patent, the doctrine of prosecution history disclaimer narrows the meaning of the claim consistent with the scope of the claim surrendered." *Biogen Idec, Inc. v. GlaxoSmithKline LLC*, 713 F.3d 1090, 1095 (Fed. Cir. 2013). Further, "statements made by a patent owner during an [*inter partes* review] proceeding can be considered during claim construction and relied upon to support a finding of prosecution disclaimer." *Aylus Networks, Inc.*, 856 F.3d at 1361. "Where the alleged disavowal is ambiguous, or even 'amenable to multiple reasonable interpretations,' [the Federal Circuit has] declined to find prosecution disclaimer." *Avid Tech., Inc. v. Harmonic, Inc.*, 812 F.3d 1040, 1045 (Fed. Cir. 2016) (quoting *Cordis Corp. v. Medtronic AVE, Inc.*, 339 F.3d 1352, 1359 (Fed. Cir. 2003)).

C. Use of a Parent Patent as Part of the Intrinsic Record

Federal Circuit cases "draw[] a distinct line between patents that have a familial relationship and those that do not" when considering whether a "related patent or its prosecution history is available to construe the claims of a patent at issue." *Goldenberg v. Cytogen, Inc.*, 373 F.3d 1158, 1167 (Fed. Cir. 2004). "When a parent application includes statements involving 'common subject matter' with the terms at issue, those statements are relevant to construction of the terms in the child patent." *E.I. du Pont de Nemours & Co. v. Unifrax I LLC*, 921 F.3d 1060, 1070 (Fed. Cir. 2019). When an application cites a parent application as prior art or in the prosecution history, these familial applications, moreover, become incorporated into the intrinsic record.[3] *Goldenberg*, 373 F.3d at 1167; *Unifrax I*, 921 F.3d at 1070 (citing *Advanced Cardiovascular Sys., Inc. v. Medtronic, Inc.*, 265 F.3d 1294, 1305–06 (Fed. Cir. 2001) ("[I]t is plainly appropriate to treat a parent application as intrinsic evidence[] when considering two related patents with identical claim terms.").

Further, as "claims must be read in light of the specification," "any patents incorporated by reference are effectively part of the host patent." *Finjan LLC v. ESET, LLC*, 51 F.4th 1377, 1382 (Fed. Cir. 2022) (first citing *Phillips*, 415 F.3d at 1315; then citing *X2Y Attenuators, LLC v. U.S. Int'l Trade Comm'n*, 757 F.3d 1358, 1362–63 (Fed. Cir. 2014)). Accordingly, "[i]ncorporation by reference of a patent 'renders the entire contents of that patent's disclosure a

[3] At oral argument, defendants agreed there was no significant difference between the '282 application and the subsequent '732 patent specification. Tr. at 14:13–17 ("THE COURT: [R]elated to the specification, it sounds like there was no change or new information that was added as the '282 application became the '732 patent? [DEFENDANTS]: That's my understanding."). Accordingly, the Court references the '282 application and the '732 interchangeably. Defendants also agreed "the prosecution history of the parent application as well as the prosecution of the '844 patent, can all be considered part of what's referred to as intrinsic evidence." *See* Tr. at 17:15–18:11. During argument for claim term 13, defendants agreed the parent patent is part of the intrinsic record. Tr. at 136:10–17. Plaintiff also agreed the '732 parent patent could be used for construing a term of the '844 patent. Tr. at 18:12–17. ("THE COURT: [P]laintiff generally agrees that the Court can refer to the parent patent, the '732 patent, to construe a term and that that would be intrinsic evidence? [PLAINTIFF]: Yes . . . .").

part of the host patent'" and "may inform the construction of claim terms common across patents." *Id.* (quoting *X2Y Attenuators, LLC*, 757 F.3d at 1362–63).

D. Indefiniteness

"[I]ndefiniteness is a question of law and in effect part of claim construction." *ePlus, Inc. v. Lawson Software, Inc.*, 700 F.3d 509, 517 (Fed. Cir. 2012). "Indefiniteness must be proven by clear and convincing evidence." *Sonix Tech. Co. v. Publ'ns Int'l, Ltd.*, 844 F.3d 1370, 1377 (Fed. Cir. 2017). A patent specification must conclude with claims distinctly pointing out the subject matter of the invention. 35 U.S.C. § 112, ¶ 2.[4] Patent claims must apprise "a skilled artisan [of] the scope of the claimed invention with reasonable certainty." *Sonix Tech. Co.*, 844 F.3d at 1376. If the claim language fails to apprise a skilled artisan with reasonable certainty, the patent claim is indefinite under § 112, ¶ 2. *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 910 (2014). General knowledge "sufficiently well established in the art and referenced in the patent," does not render a claim indefinite. *Presidio Components, Inc. v. Am. Tech. Ceramics Corp.*, 875 F.3d 1369, 1377 (Fed. Cir. 2017).

Claim construction may contain indefiniteness inquries, but other invalidity arguments under § 112, such as lack of enablement or lack of adequate written description, are separate and distinct. *See ePlus, Inc.*, 700 F.3d at 517; *Philips*, 415 F.3d at 1327 ("[W]e have certainly not endorsed a regime in which validity analysis is a regular component of claim construction."); *see also, e.g., Metabolite Labs., Inc. v. Lab. Corp. of Am. Holdings*, 370 F.3d 1354, 1361 (Fed. Cir. 2004); *Sw. Software, Inc. v. Harlequin Inc.*, 226 F.3d 1280, 1297–98 (Fed. Cir. 2000). Despite invalidity conceptually overlapping with indefiniteness, parties must use the proper standard when arguing invalidity. *See, e.g., Augme Techs., Inc. v. Yahoo! Inc.*, 755 F.3d 1326, 1340 (Fed. Cir. 2014) ("Appellants' arguments appear to be based on the wrong legal standard, i.e., written description or enablement as opposed to indefiniteness."); *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1358 n.2 (Fed. Cir. 1999) ("[D]efiniteness and enablement are analytically distinct requirements [of validity], even though both concepts are contained in 35 U.S.C. § 112.").

E. Means-Plus-Function Claims

Patent claims may also be directed to a combination comprising a series of elements. "A patentee may express an 'element in a claim for a combination' 'as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof.'" *HTC Corp. v. IPCom GmbH & Co., KG*, 667 F.3d 1270, 1278 (Fed. Cir. 2012) (quoting 35 U.S.C. § 112, ¶ 6). Known as means-plus-function claiming, this claim drafting technique pursuant to § 112, ¶ 6 results in a claim construction covering "the corresponding structure, material, or acts described in the specification and equivalents thereof." 35 U.S.C. § 112, ¶ 6.

[4] The paragraphs of 35 U.S.C. § 112 were replaced with newly designated subsections when the America Invents Act ("AIA"), Pub. L. No. 112–29, took effect on 16 September 2012. The application resulting in the patent-at-issue in this case was filed before that date, so the Court refers to the pre-AIA version of § 112.

The presence or absence of the word "means" in a patent claim impacts the claim limitation's interpretation. *See Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1348 (Fed. Cir. 2015). The presence of the word "means" creates a rebuttable presumption indicating invocation of § 112, ¶ 6 but is not the "essential inquiry" of means plus function claiming structure. *Id.* Instead, the analysis turns on "whether the words of the claim are understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure." *Id.* Sufficient structure is recited "'if the claim term is used in common parlance or by persons of skill in the pertinent art to designate structure, even if the term covers a broad class of structures and even if the term identifies the structures by their function.'" *Skky, Inc. v. MindGeek, S.A.R.L.*, 859 F.3d 1014, 1019 (Fed. Cir. 2017) (quoting *TecSec, Inc. v. Int'l Bus. Machs. Corp.*, 731 F.3d 1336, 1347 (Fed. Cir. 2013)). If both the claim and the specification fail to disclose sufficient structure to perform the claimed function, then the claim is indefinite. *Williamson*, 792 F.3d at 1352.

III. Disputed Claim Term #1: "standardized credential reader means"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Here the claimed function is to 'read a credential.' The patent in suit identifies one or more standard devices for performing this function. However, the patent covers both such standard devices and any equivalents. You have heard testimony in the trial of this matter relating to whether or not the accused products are such equivalents. As the fact finder, your role is to decide whether the products accused of infringing by plaintiff are such equivalents or not." Pl.'s Resp. Cl. Constr. Br. at 2–3.	"Indefinite. To the extent the term is construed, Defendants propose: A device, separate from the ID authenticator, for reading a credential encoded with personal identification that has a fixed 2D imaging assembly, an angled window on which the credential is placed, an ID/object detector, and a 3-track magstripe reader, all of which are mounted in a housing. The device does not rely on any of the following to improve the image resolution: movement or rotation of any component, mirroring, focused circuitry, a display screen, movable support, a longitudinal axis, a support shroud, an optics rotating assembly, or a user visible indicator." Defs.' Cl. Constr. Br. at 4.

The disputed term is used in claim 1:

> a *standardized credential reader means* for reading a credential encoded with personal identification to be used at entry point into the airport sterile areas and automatically collects data to build individual real time records;

'844 patent col. 5 ll. 1–4.

A. Parties' Arguments

Defendants argue "standardized credential reader means" is indefinite because the specification of the '844 patent "fails to disclose adequate corresponding structure for the claimed function." Defs.' Cl. Constr. Br. at 4. Defendants state, "[N]o description is given as to the actual structure of this element that would enable it to read encoded credentials" in either the figures or the specification. *Id.* at 5. Defendants assert Figure 1 "includes merely a perspective view of an outer housing of [the apparatus for recovering information from standardized personal identification credentials], with no visible internal structure," whereas "the specification describes the reader element in purely functional terms." *Id.* at 5–6. While acknowledging "in some circumstances, 'familial patents inform the construction of a claim term and are appropriately treated as intrinsic evidence,'" defendants argue "'material incorporated by reference cannot provide the corresponding structure necessary to satisfy the definiteness requirement for a means-plus-function clause.'" *Id.* at 6 (quoting *E.I. du Pont de Nemours & Co. v. Unifrax I LLC*, 921 F.3d 1060, 1070 (Fed. Cir. 2019); *Default Proof Credit Card Sys., Inc. v. Home Depot U.S.A. Inc.*, 412 F.3d 1291, 1301 (Fed. Cir. 2005); then citing *Atmel Corp. v. Info. Storage Devices, Inc.*, 198 F.3d 1374, 1382 (Fed. Cir. 1999); *Fiber, LLC v. Ciena Corp.*, 792 F. App'x 789, 795 (Fed. Cir. 2019)). Defendants argue, moreover, "even if 'one of skill in the art may have been able to find a structure that would work' to implement the recited function, that does not satisfy § 112, ¶ 6" because "a patentee is only entitled to claim 'corresponding structure . . . *described in the specification* and equivalents thereof.'" Defs.' Reply Cl. Constr. Br. at 3 (emphasis in original) (quoting *Ergo Licensing, LLC v. CareFusion 303, Inc.*, 673 F.3d 1361, 1364 (Fed. Cir. 2012). Defendants argue plaintiff's reference to his '282 application—now the '732 patent—for which the '844 patent is a continuation-in-part, cannot satisfy the definiteness requirement for a means-plus-function clause. Defs.' Cl. Constr. Br. at 6.

If not indefinite, defendants argue their proposed construction is the "only one that accurately captures the structure disclosed in the ['732 parent patent]." *Id.* According to defendants, plaintiff's proposed construction "is silent as to what actual structure would result in infringement of the claim." *Id.* at 7. Defendants also argue plaintiff's proposed construction, "'read a credential,' completely reads out the claim terms 'standardized' and 'encoded,' each of which modifies the term 'credential' in the limitation at issue." *Id.* at 5. If the Court gives effect to plaintiff's definition, defendants argue, the claim could encompass the "reading of *any* type of credential, regardless of whether the credential was 'standardized' or contained 'encoded' information." *Id.*

Plaintiff refutes defendants' indefiniteness argument by contending "standard credential reader means are well known to one of the ordinary skill in the art." Pl.'s Resp. Cl. Constr. Br. at 3. "There are only a few such machines commercially available at any given time," plaintiff argues, "and anyone of ordinary skill working in the field is well aware of what those machines are." *Id.*; *see also* Pl.'s Surreply Cl. Constr. Br. at 5. Plaintiff quotes *Atmel* to argue "the knowledge of one skilled in the particular art may be used to understand what structure(s) the specification discloses . . . [and] even a dictionary or other documentary source may be helpful for such assistance." Pl.'s Resp. Cl. Constr. Br. at 3 (quoting *Atmel Corp.*, 198 F.3d at 1382). Plaintiff argues "the patent in suit identifies one or more standard devices for performing this function," as seen in Figure 1 and the detailed description of Figure 1. Pl.'s Surreply Cl. Constr.

Br. at 3. Asserting the claim is definite, plaintiff argues the Court should construe the term as claiming the function, "to 'read a credential.'" Pl.'s Resp. Cl. Constr. Br. at 2–3.

B. Analysis

1. The Court's Preliminary Construction

Before the *Markman* hearing, the Court provided the parties with the Court's preliminary construction after considering both parties' claim construction briefs and all referenced materials in full. *See* Tr. at 8:15–19. The government asserts in briefing both parties agreed the term should be construed under 35 U.S.C. § 112, ¶ 6 "but dispute the precise function involved." Defs' Cl. Constr. Br. at 4. Accordingly, the Court initially construed the term under a means-plus-function analysis. As the claim term contains the word "means," the Court looked to identify what function the means was intended to perform. The parties dispute what credentials the function applies to and limitations surrounding the apparatus performing the function, but both parties generally agree the claimed function is to "read a credential." *See id.* at 4–5 (arguing the construction, among other limitations, includes "reading a credential"); Pl.'s Resp. Cl. Constr. Br. at 2–3 (contending the construction should be, "read a credential"). After identifying a function, the Court then "identif[ied] the structure in the specification that is clearly linked with this function . . . ." *Rain Computing Inc. v. Samsung Elecs. Am., Inc.*, 989 F.3d 1002, 1007 (Fed. Cir. 2021). The Court relied on the '732 patent's description, as referenced the '844 patent, column 1 lines 39–40, for the apparatus components for a corresponding structure of the "standardized credential reader means" function and, therefore, preliminarily found the term not indefinite. *See HTC Corp. v. IPCom GmbH & Co., KG*, 667 F.3d 1270, 1279 (Fed. Cir. 2012). The Court preliminarily construed the term as the apparatus in the the '732 patent or "a device for reading a credential encoded with personal identification that has a fixed 2D imaging assembly, an angled top window, an ID/object detector, and a 3-track magstripe reader, all of which are mounted on a housing. The device is stationary with no moveable components."[5]

2. The Court's Final Construction

At the *Markman* hearing, plaintiff confirmed the disputed term invokes a means-plus-function construction. Tr. at 27:13–14 ("[PLAINTIFF]: [The claim] was a means-plus-function claim."), 31:16–18 ("THE COURT: [Y]our point is that it does invoke 112(f)? [PLAINTIFF]: Yes, using that structure."). Defendants agreed the language of the term invokes means-plus-function construction. Tr. at 45:4–7 ("[DEFENDANTS]: [B]oth parties contend this is a means-plus-function construction."). Ordinarily, the word "means" in a claim creates a rebuttable

[5] The Court initially construed the term as the apparatus disclosed in the '732 patent because of a shared Figure 1 and the reference to the apparatus in the '844 patent. *See* '844 patent col. 1 l. 39–40 ("Such method uses a computer system, the apparatus of [the '732 patent], and the software application of the [the '732 patent]."). While the '732 patent is incorporated by reference and therefore "provides context" to claim construction, the '844 patent does not provide a comprehensive explanation linking the structure to the performance of the function. *Fiber*, 792 Fed. App'x at 795 (quoting *Default Proof Credit Card Sys., Inc.*, 412 F.3d at 1301 ("As an initial matter, material incorporated by reference cannot provide the corresponding structure necessary to satisfy the definiteness requirement for a means-plus-function clause.") (internal quotes and citation omitted)); *see Finjan LLC v. ESET, LLC*, 51 F.4th 1377, 1382 (Fed. Cir. 2022). As a preliminary construction, however, the Court was willing to construe in favor of validity, despite the tenuous link between structure and performance of the function.

presumption § 112, ¶ 6 applies, which the party seeking to overcome the presumption has the burden to proffer evidence to rebut. *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1348 (Fed. Cir. 2015); *Apex, Inc. v. Raritan Comput., Inc.*, 325 F.3d 1364, 1371–72 (Fed. Cir. 2003) (placing the evidentiary burden to rebut on the party seeking to overcome the presumption). Here, neither party seeks to rebut a mean-plus-function construction, so the Court need not determine whether the rebuttable presumption is overcome and instead analyzes definiteness under the mean-plus-function construction.

Determining definiteness under a means-plus-function construction requires a two-step analysis. *Williamson*, 792 F.3d at 1351. First, a court will "identify the claimed function." *Id.* at 1351 (citing *Noah Sys., Inc. v. Intuit Inc.*, 675 F.3d 1302, 1311 (Fed. Cir. 2012)). "Then, the court [will] determine what structure, if any, disclosed in the specification corresponds to the claimed function." *Id.* at 1349.

First, the Court identifies the claimed function. Both parties agree the claimed function is to "read a credential." *See* Defs.' Cl. Constr. Br. at 4–5 (arguing the construction, among other limitations, includes "reading a credential"); Pl.'s Resp. Cl. Constr. Br. at 2–3 (contending the construction should be "read a credential"). The Court agrees "reading a credential" is at least the primary claimed function here as it is consistent with the claim language. '844 patent col. 5 ll. 1–2 (emphasis added) ("a standardized credential reader *means for reading a credential*"). Claim 1 also suggests the standardized credential reader may store some information for some amount of time. The claim states a "software application" can "recover[] information *from* the standardized credential reader," and "a central processing unit" can "receiv[e] information *from* the standardized credential reader." '844 patent col. 5 ll. 5–6, 24–25 (emphasis added).

Second, the Court determines whether the specification discloses sufficient structure corresponding to the claimed function. *Williamson*, 792 F.3d at 1351. When asked where the specification discloses structure corresponding to the credential reader's function, plaintiff could not point to anything in the '844 patent specification describing structure necessary for a standardized credential reader means. Tr. at 44:16–24 ("THE COURT: [C]an you read from the spec[ification] where . . . the requisite structure is given? [PLAINTIFF]: Not from the spec[ification], no. You have to refer to external devices and the knowledge of one of ordinary skill in the art in terms of what those devices are.").

The Court in its preliminary construction relied on the '732 patent to find corresponding structure and prevent indefiniteness, but at oral argument, plaintiff disclaimed the references to the '732 patent in this context, specifically Figure 1 contained in both patents and column 1 lines 39 to 40. Tr. at 28:9–14 ("THE COURT: Isn't [Figure 1] a picture from the '732 patent?" [PLAINTIFF]: It is a picture from the '732 patent, but it's a generic reference . . . we've never said that this is what we're actually using as our structural reference."). Plaintiff asserted Figure 1 of the '844 patent was used to denote a generic credential reader understood as a wide variety of readers for the purpose of credential reading by a PHOSITA, not a specific structure. Tr. at 28:20–29:14. Indeed, plaintiff argues, "The patent-in-suit identifies one or more standard devices for performing this function. However, the patent covers both such standard devices and any equivalents." Pl.'s Resp. Cl. Constr. Br. at 2–3. Plaintiff, however, cannot point to other language in the '844 patent describing products or characteristics of products which could be

used for the purpose of reading credentials. *See* Tr. at 30:10–16 ("THE COURT: Is there anywhere where it says that it could be a variety of certain products or a reader that has certain attributes or may have certain attributes? [PLAINTIFF]: Not to my knowledge."). Even using the reference to the '732 figure, the link between the apparatus and the performance of function was tenuous; with plaintiff disclaiming the '732 figure as a specific structure, the '844 patent specification cannot adequately explain how the apparatus, including the apparatus incorporated though the '732 patent, performs the function. By characterizing Figure 1 as a generic and cabining its structure to the '732 patent, the specification, including its figures, now do not link any structure to the claimed function. *See Williamson*, 792 F.3d at 1351–54.

To support a structure, plaintiff states the generic reader is sufficient "to refer to a group of electronic devices by one of ordinary skill in the art." *See* Tr. at 28:23–29:7. Plaintiff asserts the Federal Circuit in *Telcordia* held the word "controller" was deemed to have sufficient structure for a "means-plus-function claim because the record shows that an ordinary artisan would have recognized the controller as an electronic device of known structure." *Id. Telcordia*, however, is distinguishable from the current case because the meaning of "controller" was clarified and supported by expert testimony, whereas no such testimony in support of "credential reader" exists here. *Telcordia Techs., Inc. v. Cisco Sys., Inc.*, 612 F.3d 1365, 1377 (Fed. Cir. 2010).

"The indefiniteness inquiry is concerned with whether the bounds of the invention are sufficiently demarcated, not with whether one of ordinary skill in the art may find a way to practice the invention." *ePlus, Inc. v. Lawson Software, Inc.*, 700 F.3d 509, 517 (Fed. Cir. 2012). Plaintiff's boundless mention of devices is an insufficient demarcation of the invention. *Id.* Plaintiff agrees the claim invokes means-plus-function claiming yet fails to point to any structure "in the specification [corresponding] to the claimed function." *Williamson*, 792 F.3d at 1351. Plaintiff is unable to prove "the claim term is used in common parlance or by persons of skill in the pertinent art to designate structure, even if the term covers a broad class of structures and even if the term identifies the structures by their function." *Skky, Inc. v. MindGeek, S.A.R.L.*, 859 F.3d 1014, 1019 (Fed. Cir. 2017) (cleaned up) (quoting *TecSec, Inc. v. Int'l Bus. Machs. Corp.*, 731 F.3d 1336, 1347 (Fed. Cir. 2013)). Under 35 U.S.C. § 112, ¶ 6, a person of ordinary skill in the art is unable to recognize the structure in the specification and associate it with the corresponding function in the claim; the means-plus-function clause of "standardized credential reader means" is therefore indefinite. *See Williamson*, 792 F.3d at 1354.

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Here the claimed function is to 'read a credential.' The patent in suit identifies one or more standard devices for performing this function. However, the patent covers both such standard devices and any equivalents. You have heard testimony in the trial of this matter relating to whether or not the accused products are such equivalents. As the fact finder, your role is to decide whether the	"Indefinite. To the extent the term is construed, Defendants propose: A device, separate from the ID authenticator, for reading a credential encoded with personal identification that has a fixed 2D imaging assembly, an angled window on which the credential is placed, an ID/object detector,

products accused of infringing by plaintiff are such equivalents or not."	and a 3-track magstripe reader, all of which are mounted in a housing. The device does not rely on any of the following to improve the image resolution: movement or rotation of any component, mirroring, focused circuitry, a display screen, movable support, a longitudinal axis, a support shroud, an optics rotating assembly, or a user visible indicator."
Court's Construction	
Indefinite.	

IV. Disputed Claim Term #2: "credential encoded with personal identification"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning."[6] Pl.'s Cl. Constr. Br. at 4.	"Indefinite. To the extent the term is construed, Defendants propose: A credential used to prove an individual's identity containing a machine-readable magnetic stripe or bar code which stores at least the individual's full name." Defs.' Cl. Constr. Br. at 7.

The disputed term is used in claims 1 and 3. *See* '844 patent col. 5 ll. 1–4, col. 5 l. 44–col. 6 l. 5. The following claim limitations highlight selected usage of the term in context:

> a standardized credential reader means for reading a *credential encoded with personal identification* to be used at entry point into the airport sterile areas and automatically collects data to build individual real time records;

id. col. 5 ll. 1–4.

> An automatic access control system as claimed in claim 1, wherein the standardized credential reader can read any one of: driver license identification, passports, boarding passes or any other standardized *credentials* presented as a *personal identification* upon entry into the airport, and whereas

[6] Plainitiff inadvertently pasted in the proposed construction of a different disputed term for term 2 in exchange of proposed construction. Plaintiff, however argues disputed term 2 as plain meaning. *See* Pl.'s Cl. Constr. Br. at 4 n.2 ("Plaintiff regrets the inadvertent provision of the definition for another term in the supplemental exchange of definitions. (*See* Ex. C at 3). The parties have exchanged numerous tables for the claim terms with unfortunately many different orders for the terms even for each party, so while cut and pasting is helpful, it has its hazards. In any event, rather than ask for a supplemental definition, Defendants construed this mistake as an argument for 'a credential,' stripping the term of its requirement that it be encoded with personal identification. As with many of the other claims that have clearly understood terms, Plaintiff intended to argue only for plain meaning.")

> standardized credentials refer to identification documents *encoded* using established standards.

Id. col. 5 l. 44–col. 6 l. 5.

A. Parties' Arguments

Defendants primarily argue the term is indefinite under § 112, ¶ 2. Defendants raise several indefiniteness arguments concerning the "multiple types of credentials" plaintiff attempts to claim and the ambiguity surrounding "which ones include information 'encoded' thereon that qualifies as 'personal identification.'" Defs.' Cl. Constr. Br. at 7. Defendants asserts "it is impossible to determine whether the airport ID so described is also a 'credential encoded with personal identification'" because after the reader device reads an airport ID, the reader device requires the employee to enter a security code in a numeric keypad. *Id.* at 8. Defendants argue "[i]t is unclear whether using the information read from the airport ID to verify 'employment status' . . . would qualify . . . as 'personal identification' . . . or . . . would not qualify because the separate security code entered on a keypad . . . is necessary to establish the identity of the holder." *Id.* (emphasis omitted).

Plaintiff rebuts defendants' indefiniteness arguments by defining "encode" as "to convert into a coded form" and narrowing "personal identification" to "personal identification information" because "encoding with personal identification" requires information. Pl.'s Resp. Cl. Constr. Br. at 4. Plaintiff argues both "encode" and "personal information" "have very clear meanings to one of ordinary skill," and "read together, it is clear all that is meant is that the credential have plain text personal identification information encoded on it in some fashion, i.e.[,] a bar code or magnetic stripe." *Id.* at 4–5. Plaintiff argues the claim does not exclude airport IDs, contrary to defendants' position, because the keypad security code merely functions as an "additional security measure so [airport IDs] are not misused." *Id.* at 5. If "information sufficient to identify an individual is encoded," plaintiff argues, "this claim limitation is met." *Id.*

If the claim is definite, defendants argue, the Court should construe the scope of the claim in accordance with the "structures disclosed in the intrinsic record, and in particular [the '732 patent,]" which would require limiting the "personal information" to information encoded in magnetic strips or bar codes. Defs.' Cl. Constr. Br. at 8. Plaintiff argues the examples of encoded information in the '732 patent "do not overrule the plain meaning" of "credential encoded with personal identification." Pl.'s Resp. Cl. Constr. Br. at 6. According to plaintiff, "credential encoded with personal identification" should be given its ordinary meaning: "[a] credential used to prove an individual's identity containing a machine-readable aspect (e.g., a magnetic stripe or bar code) which stores a name or number that, alone or in combination with other information, is sufficient to identify a specific individual." *Id.*

B. Analysis

1. The Court's Preliminary Construction

Before the *Markman* hearing, the Court provided the parties with the Court's preliminary construction after considering both parties' claim construction briefs and all referenced materials in full. Tr. at 8:15–19. The Court first addressed defendants' indefiniteness arguments. Defendants argue two embodiments described in the specification suggest competing interpretations of "credential encoded with personal identification," so the patent should fail for indefiniteness. Defs.' Cl. Constr. Br. at 7–8. Defendants do not explain why the term cannot cover both types of identification.

The specification language referenced by defendants suggests a broad interpretation. *Id.* The '844 patent, when describing the operation of the system, indicates a driver's license is merely offered as an example. '844 patent col. 3 ll. 37–38 ("[a] credential, *in this case a driver license*, is presented to the reading apparatus) (emphasis added). Language in dependent claim 3 further supports a broad reading which would cover both types of credentials: "the standardized credential reader can read any one of: driver license identification, passports, boarding passes or any other standardized credentials presented as a personal identification . . . whereas standardized credentials refer to identification documents encoded using established standards." '844 patent col. 5 l. 44–col. 6 l. 5. The PHOSITA is not left in the "zone of uncertainty" as to whether the term refers to a driver's license or airport ID because the claim term explicitly covers both. *Id.* Accordingly, the Court preliminarily rejected defendants' indefiniteness arguments.

Claim terms are "generally given their ordinary and customary meanings" unless the patentee acts as his own lexicographer or disavows the full scope of the claim in the specification or during patent prosecution. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005); *Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (citing *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1580 (Fed. Cir. 1996)). The embodiments referenced by defendants provide context for evaluating the scope of the patent, but do not limit the Court's construction. *See Phillips*, 415 F.3d at 1323–24. The described embodiments merely exemplify operation of the system and do not act as explicit definitions or overcome the presumptive use of plain and ordinary meaning. *See Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 980 (Fed. Cir. 1995); *Jack Guttman, Inc. v. Kopykake Enters., Inc.*, 302 F.3d 1352, 1360–61 (Fed. Cir. 2002). The Court, therefore, rejected the construction offered by defendants which requires encoding of at least the individual's full name. Defs.' Cl. Constr. Br. at 7–8. Likewise, the Court also rejected defendants' argument the patent should be limited to use of only magnetic stripe or bar code as a method for encoding. *Id.* at 8. Such limitations are not clearly adopted by the '844 patent and are merely contemplated by the '732 patent. *See* '844 patent; '732 patent. Finally, neither the specification nor the prosecution history demonstrates an intention by the patentee to disavow the scope of the plain and ordinary meaning, and neither party argrues otherwise in the briefing. *See* '844 patent; Defs.' Cl. Constr. Br.; Pl.'s Resp. Cl. Constr. Br.; Defs.' Reply Cl. Constr. Br.; Pl.'s Surreply Cl. Constr. Br. As neither of the two exceptions for ordinary meaning are met, *supra* Section II.A., the Court did not adopt the limitations provided by the '732 patent and instead preliminarily adopted the plain and ordinary meaning of this term. *See Phillips*, 415 F.3d at 1312–13. Insofar as a specific definition is useful, the Court offered the following: "a certified document containing information relating to a particular individual converted from one system of communication into another." *Credential*, Merriam-Webster Dictionary, https://www.merriam-

webster.com/dictionary/credential (last visited Jan. 10, 2023) ("testimonials or certified documents showing that a person is entitled to credit or has a right to exercise official power); *Encode*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/encode (last visited Jan. 10, 2023) ("to convert (something, such as a body of information) from one system of communication into another"); *Personal*, Webster's Third New International Dictionary (2002) ("of or relating to a particular person").

2. The Court's Final Construction

At the *Markman* hearing, the parties agreed with the Court's preliminary construction with certain modifications. *See* Tr. at 52:1–60:25. Consistent with defendants' request, a list of documents including "driver's license, passport, boarding pass, airport ID" has been added. Tr. at 56:11–20. Consistent with plaintiff's request, the term "certified" is replaced with "standardized." Tr. at 58:18–59:17. The Court's final construction is: "a driver's license, passport, boarding pass, airport ID, or other standardized documents containing information relating to a particular individual converted from one system of communication into another."

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning."	"Indefinite. To the extent the term is construed, Defendants propose: A credential used to prove an individual's identity containing a machine-readable magnetic stripe or bar code which stores at least the individual's full name."
Court's Construction	
Plain meaning: "a driver's license, passport, boarding pass, airport ID, or other standardized documents containing information relating to a particular individual converted from one system of communication into another."	

V. Disputed Claim Term #3: "build individual real time records"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning. The system generates a data record in real time. The data and entry decision are displayed to the operator but not accessed by the system operator. Accessing data means ability to edit, update and make changes, which is not the case here." Pl.'s Resp. Cl. Constr. Br. at 6.	"Indefinite. To the extent the term is construed, Defendants propose: Create and store a record of information obtained from each credential reading, including at least the individual's photo and all information extracted from the machine-readable magnetic stripe or bar code, which

	may be accessed by the system operator at any time" Defs.' Cl. Constr. Br. at 9.

The disputed term in used in claim 1:

> a standardized credential reader means for reading a credential encoded with personal identification to be used at entry point into the airport sterile areas and automatically collects data to *build individual real time records*;

'844 patent col. 5 ll. 1–4.

A. Parties' Arguments

Defendants contend plaintiff's plain meaning construction is indefinite because the claim provides no explanation of how records are built, what constitutes a record, or how the record building is done in real time, leaving one of ordinary skill in a zone of uncertainty as to what activity is covered by this claim term. Defs.' Cl. Constr. Br. at 9. According to defendants, plaintiff's "general dictionary definitions" do not remedy this uncertainty. Defs.' Reply Cl. Constr. Br. at 4–5. Plaintiff disagrees, asserting the "information collected and processed" from a standardized credential reader means would be "known to one of ordinary skill" because the art uses "only a few" machines for this function. Pl.'s Surreply Cl. Const. Br. at 5.

Plaintiff argues "build individual real time records" is not indefinite. Pl.'s Resp. Cl. Constr. Br. at 6–8. Plaintiff relies on general dictionary definitions for "build" and "real time" to demonstrate "build" and "real time" are well understood and therefore not indefinite. *Id.* at 6–7 (defining build as to "construct (something) by putting parts or material together," and real time as "a system, in which input data is processed within milliseconds so that it is available virtually immediately as feedback") (quoting Exs. D, ECF No. 140-5 (Google definition of "build"), E, ECF No. 140-6 (Google definition of "real time").

Both parties also offer alternative constructions. Plaintiff suggests the term should be construed broadly as "any step of storing data received by a credential reader," if the Court does not adopt the plain meaning construction. *Id.* at 8. Defendants reject this reading as "overbroad" because the construction "would apply to essentially any step of storing data received by an accused credential reader." Defs.' Cl. Constr. Br. at 10. Plaintiff argues breadth is irrelevant, for "[p]atentees are entitled to claim as broadly or as narrowly as they like, so long as the patent is valid." Pl.'s Resp. Cl. Constr. Br. at 7. Defendants' alternative construction, in contrast, imposes two limitations related to "what data is collected and stored in the process of 'building' the records": (1) the record must include the "individual's photo and all information extracted from the machine-readable magnetic stripe or bar code"; and (2) the "system operator" must be able to "access" the record "at any time." Defs.' Cl. Constr. Br. at 9. Plaintiff characterizes these limitations as attempts to "seize on illustrations in the patent to try to claim a definition limited to those illustrations." Pl.'s Resp. Cl. Constr. Br. at 7.

B. Analysis

1. The Court's Preliminary Construction

Before the *Markman* hearing, the Court provided the parties with the Court's preliminary construction after considering both parties' claim construction briefs and all referenced materials in full. Tr. at 8:15–19. At the onset, the Court noted there are two types of records created by practicing claim 1 of the '844 patent: (1) "individual real time records" generated by a "standardized credential reader means," '844 patent col 5. ll. 1–4; and (2) an "authentication data record" generated by an "ID authenticator," *id.* at col. 5 ll. 21–23. "[D]ifferent claim terms are presumed to have different meanings," so the Court considered intrinsic evidence concerning the individual real time records. *MicroStrategy Inc. v. Bus. Objects Ams.*, 238 F. App'x 605, 609 (Fed. Cir. 2007) (citations omitted). For clarity, the Court construed the term by parsing it into two phrases: first construing "real time" and then addressing what is required to "build individual records."

The '844 patent and '732 patent specifications extensively detail what "real time" means and include disclosures supporting plaintiff's proffered dictionary definition. *Compare* Pl.'s Resp. Cl. Constr. Br. Ex. E (Google definition of "real time") (defining real time as "a system, in which input data is processed within milliseconds so that it is available virtually immediately as feedback"), *with* '844 patent col. 5 ll. 26–29 ("upon a credential reading, the automated access control system automatically determines the source of the credential data record, and automatically extracts personal information"), *and* the '732 patent col. 9 ll. 56–60 ("A large number of workstations are connected to a local area network . . . controlled by a central database server . . . . In such a[n interconnected] network, all data is immediately available at all workstations."). The Court agrees the "information collected and processed" from a standardized credential reader means would be "known to one of ordinary skill" as it was well known in the art. *Presidio Components, Inc. v. Am. Tech. Ceramics Corp.*, 875 F.3d 1369, 1376 (Fed. Cir. 2017) ("A patent need not explicitly include information that is already well known in the art."). Indeed, reading credentials and generating real time records is "sufficiently well established in the art and referenced in the patent to render the claims not indefinite." *Id.* The Court accordingly accepted plaintiff's proffered definition for "real time." *See id.*

Turning to "build[ing] individual records," the claims describe a process where a "standardized credential reader means" reads a "credential encoded with personal identification [information]." '844 patent col. 5 ll. 1–4. The '844 patent claims mention personal identification information is "automatically collect[ed] . . . to build individual real time records," *id.*; the '732 patent provides some necessary clarification.[7] The claims of the '732 patent outline the potential arrangement of the system: each "*workstation can be standalone with all data collected and stored locally*, or otherwise [the workstation can be] connected to a local area network or an intranet . . . with data stored in a central database server." '732 patent col. 14 ll.

[7] The Court finds the '732 patent's disclosures on the apparatus or software application are available as intrinsic evidence to the '844 patent because the '732 patent is the '844 patent's parent. *See* '732 patent col. 9 l. 40–col. 13 l. 25; *see also E.I. du Pont de Nemours & Co. v. Unifrax I LLC*, 921 F.3d 1060, 1070 (Fed. Cir. 2019). The '732 patent discloses elements of the method claimed by the '844 patent.

27–31 (emphasis added). The '732 patent specification further clarifies "[t]he functional intent of this apparatus is to provide a means for automatically recovering information from standardized identification cards and processing the data *through an internal processor and communicating the output to a computer system or network application.*" *Id.* at col. 7 ll. 3–8 (emphasis added). Viewing the patents together, a "standardized credential reader means" processes and stores the credential data internally—at least for a temporary period before the data is extracted and stored on the central database server.

The '732 and '844 patents also disclose the process of building real time records: the "standardized credential reader means" first decodes data and then encrypts sensitive data. *See* '732 patent fig.7; '844 patent col. 3 ll. 39–41 ("The system decodes the encoded data and encrypts the sensitive information before displaying it on the work-station monitor for verification by the station guard."). A software application, designed for recovering information from the standardized credential reader, extracts the encoded data before the system "display[s the data] on the work-station monitor for verification by the station guard." '844 patent col. 3 ll. 40–41. The phrase "for recovering information from" is used several times in the '732 patent to describe the standardized credential reader's acquisition of information "from standardized personal identification credentials." *See, e.g.*, '732 patent col. 13 ll. 27–28, 47–48, 57–58. The credential reader is separate from the credential, so the inventor's consistent usage between familial patents implies the software application is also separate from the credential reader. *See* '844 patent col. 1 ll. 37–41. Accordingly, the intrinsic evidence suggests the process of "build[ing] individual real time records" occurs exclusively on the credential reader. *Id.* col. 5 ll. 1–6. The Court preliminarily found the process requires the system to read information off a credential, and then immediately: (1) save the information on the credential reader; (2) decode the information; (3) encrypt any sensitive personal information; and (4) display the information for verification by the gate employee. *See* '732 patent fig.7, col. 13 ll. 27–28, 47–48, 57–58; *see also* '844 patent col. 3 ll. 39–41, col. 5 ll. 1–6. The description of prior art in the '732 patent, where plaintiff distinguished U.S. Patent No. 6,394,356 ("Zagami") (filed June 4, 2001), further supports the Court's preliminary construction: (1) the Zagami system "does not claim reading encoding available on the driver['s] license"; and (2) without reading this information, the Zagami system "at most" scans credentials as a picture, saving sensitive information in an unencrypted format, which "fails to protect individual information." '732 patent col. 2 ll. 34–37, 49–52.

The Court, by clearly demarcating the bounds of the '844 patent claim term "build[ing] individual real time records," rejected defendants' indefiniteness arguments because the '844 patent combined with the '732 patent allow "a skilled artisan to know the scope of the claimed invention with reasonable certainty." *See Presidio*, 875 F.3d at 1376–77. Defendants' indefiniteness contention of "how [records are built] in 'real time'" is irrelevant because a patent claim need not answer every conceivable question to be found definite. *Id.* at 1376 (citing *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 909–10 (2014)). Defendants' alternative construction fares no better, for nothing in the claims or the specification limits what information must be stored from the read data. *See* '732 patent col. 11 ll. 30–32 ("Each data item . . . can be saved in the system data store or ignored at the end of an admission process"), col. 11 ll. 28–29 ("Data shown in the collection form can be customized for viewing and saving as specified by the system administrator."), col. 10 ll. 43–47 ("[D]igital images . . . [of a potential visitor] are

saved or stored in the system only if the individual is actually admitted into the facility."). Limitations from preferred embodiments are not read "into the claims absent a clear indication in the intrinsic record that the patentee intended the claims to be so limited." *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 913 (Fed. Cir. 2004). Defendants offered no indication in the intrinsic record that these limitations were intended, so the Court declined to read them into the claims and rejected defendants' alternative construction.

Plaintiff's broad proposed constructions must also be rejected. Zagami discloses a "basis for providing an access control system," to "generate[] a data record in real time" and "stor[e] data received by a credential reader," which means either relevant portions of the '844 patent are fully disclosed in the art, or "build[ing] individual real time records" requires additional disclosure. '732 patent col. 1 l. 64–col. 2 l. 52. Plaintiff distinguishes Zagami because of the '844 patent's usage of decoding and encrypting, so decoding and encrypting must be a necessary part of "build[ing] individual real time records."

In sum, the Court preliminarily found the intrinsic evidence to support the following construction: "the credential reader immediately generates a digital record after decoding information from the credential and encrypting sensitive personal information." *See* '844 patent col. 3 ll. 39–41 ("The system decodes the encoded data and encrypts the sensitive information before displaying it on the work-station monitor for verification by the station guard."); '732 patent fig.7, col. 14 ll. 27–31 ("[T]he system workstation can be standalone with all data collected and stored locally, or otherwise connected to a local area network or an intranet . . . with data stored in a central database server . . . .").

2. The Court's Final Construction

At the *Markman* hearing, the parties agreed with the Court's preliminary construction with certain modifications. *See* Tr. at 60:9–69:10. Defendants requested the language "stored within the system for access by a operator at any time" be added as the language was supported by the specification. Tr. at 63:15–66:6; '844 patent col. 4 ll. 10–11 ("At any time, the gate attendant is able to review the records that have been collected during the entry process."). Plaintiff agreed to this modification and suggested use of the term "user" instead of "operator." Tr. at 65:19. The Court's final construction is: "The credential reader immediately generates a digital record after decoding information from the credential and encrypting sensitive personal information. The digital record is then stored within the system for access by a user at any time."

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning. The system generates a data record in real time. The data and entry decision are displayed to the operator but not accessed by the system operator. Accessing data means ability to edit, update and make changes, which is not the case here."	"Indefinite. To the extent the term is construed, Defendants propose: Create and store a record of information obtained from each credential reading, including at least the individual's photo and all information extracted from the machine-

	readable magnetic stripe or bar code, which may be accessed by the system operator at any time"
Court's Construction	
The credential reader immediately generates a digital record after decoding information from the credential and encrypting sensitive personal information. The digital record is then stored within the system for access by a user at any time.	

VI. Disputed Claim Term #4: "credential collected information match"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning. As an illustration, checks can be made against TSA lists, employee lists if employee, or traveler lists, if traveler." Pl.'s Resp. Cl. Constr. Br. at 8.	"Indefinite. To the extent the term is construed, Defendants propose: A match between the individual real time record created for the presented credential and any previously collected and stored individual real time record containing the same name, or information extracted from the same credential." Defs.' Cl. Constr. Br. at 10.

The disputed term is used in claim 1:

> real time records are checked searching for a *credential collected information match*; individual suspicious status is checked against a security list stored in a system database; employee records are checked to determine if the individual is an employee; the type of entry, visitor, employee, contractor, supplier, or vendor, is determined; and admission is processed as entry or re-entry of the individuals,

'844 patent col. 5 ll. 8–15.

A. Parties' Arguments

Defendants argue this term is indefinite. Defs.' Cl. Constr. Br. at 10. Defendants contend the list of functions (including the contested term) require the "software application [to perform] three separate and distinct functions, creating ambiguity as to how" the contested term differs from what is covered by the second and third recited functions. *Id.* at 11–12 (identifying the second phrase to include matches found by "comparing data read by the reader device *against an airport employee database* to verify employee status" and the third phrase to include "comparing data read by the reader device *against a suspect individual list* obtained from an outside source"). Moreover, defendants argue plaintiff's "suggested interpretation of [function

1] as a 'catchall' would clearly render [functions 2 and 3] superfluous." Defs.' Reply Cl. Constr. Br. at 6. If the Court does not find the term indefinite, defendants propose the term be construed as: "[a] match between the individual real time record created for the presented credential and any previously collected and stored individual real time record containing the same name, or information extracted from the same credential." Defs.' Cl. Constr. Br. at 10.

To rebut defendants' indefiniteness argument, plaintiff offers an illustration of potential databases where the collected information may be "matched": "TSA lists, employee lists[,] if employee, or traveler lists, if traveler." Pl.'s Resp. Cl. Constr. Br. at 8. Plaintiff reasons the preamble to the contested term, "'wherein one or more of the following process[es] is performed,'" contextualizes the subsequent clauses as part of a list. *Id.* at 9 (quoting '844 patent col. 5 ll. 6–7). More specifically, plaintiff argues the term is a "catchall phrase in the midst of much more specific types of matches, only one of which needs to be performed by the accused process to infringe this claim." *Id.* If found to be definite, plaintiff argues "credential collected information match" should be given its plain and ordinary meaning. *Id.* at 8.

B. Analysis

1. The Court's Preliminary Construction

Before the *Markman* hearing, the Court provided the parties with the Court's preliminary construction after considering both parties' claim construction briefs and all referenced materials in full. Tr. at 8:15–19. The '844 patent specification discloses the elements for a "credential collected information match," including three main prerequisite steps: (1) the standardized credential reader means decodes the credential; (2) the standardized credential reader means encrypts sensitive personal information; and (3) the station guard views the resulting "real time record" after the standardized credential reader means presents the record for verification. *See* '844 patent col. 3 ll. 35–41. After station guard verification, the system "checks database information to determine whether the individual is an employee, contractor, vendor, supplier or a visitor." '732 patent col. 10 ll. 32–34; *see also* '844 patent col. 5 ll. 12–13 ("the type of entry, visitor, employee, contractor, supplier, or vendor, is determined"). If the individual is an employee who is "recognized using the employee pre-selected alternative credential," the system displays the employee's picture, which is verified by the station guard. '732 patent col. 10 ll. 35–39; *see also* '844 patent col. 5 ll. 30–31 ("other alternative credentials"). If the individual is "recognized as a visitor, then the system acquires a digital image of the individual" using a camera, which is "saved or stored in the system only if the individual is actually admitted into the facility." '732 patent col. 10 ll. 41–47. The system then "checks existing records for possible matches. If a match is found, the archived record is displayed with the contemporaneous record . . . to facilitate visual confirmation by the station guard." *Id.* col. 10 ll. 48–52; *see also* '844 patent col. 5 ll. 29–30 ("checked against a security list"). In addition, the system "further checks for known and suspected criminal, saboteurs, and terrorists using lists as delivered by the US Department of Homeland Security." '732 patent col. 10 ll. 55–58; *see also* '844 patent col. 5 ll. 29–30 ("checked against . . . TSA NO-FLY list, SELECTEE list"). If all checks are negative, "the system searches for previous visitor records," and if found, the system displays the previous image for visual confirmation by the station guard. '732 patent col. 10 ll. 64–67; *see also* '844 patent col. 5 ll. 14–15 ("admission is processed as entry or re-entry of the

individuals"). In sum, the disclosure identifies four potential matches: (1) an employee match; (2) a Department of Homeland Security list match; (3) an archived record match; and (4) a current visitor match (for entry/re-entry).

Turning to the parties' proposed constructions, the Court agreed with plaintiff the plain meaning is sufficiently clear within context of the specifications but disagreed the "credential collected information match" is a "catchall" provision. *See* Pl.'s Resp. Cl. Constr. Br. at 8–9. Defendants' attempt to limit this "match" to a "collected and stored individual real time record containing the same name, or information extracted from the same credential" is unsupported by the intrinsic record. *See* Defs.' Cl. Constr. Br. at 10. Accordingly, the Court preliminarily construed "credential collected information match" according to its plain and ordinary meaning. *See Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (citing *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1580 (Fed. Cir. 1996)). Insofar as a specific definition is useful, the Court offered the following preliminary construction: "when the data collected from a currently presented credential is equal or similar to an existing record." *See Match*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/match (last visited Jan. 10, 2023) ("a person or thing equal or similar to another); *Information*, Webster's Third New International Dictionary (2002) ("facts of figures ready for communication or use as distinguished from those incorporated in a formally organized branch of knowledge: DATA").

2. The Court's Final Construction

At the *Markman* hearing, both parties agreed to the Court's preliminary plain meaning construction. Tr. at 67:1–9. The Court adopts its preliminary construction as final: plain meaning, "when the data collected from a currently presented credential is equal or similar to an existing record."

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning. As an illustration, checks can be made against TSA lists, employee lists if employee, or traveler lists, if traveler."	"Indefinite. To the extent the term is construed, Defendants propose: A match between the individual real time record created for the presented credential and any previously collected and stored individual real time record containing the same name, or information extracted from the same credential."
Court's Final Construction	
Plain meaning: "when the data collected from a currently presented credential is equal or similar to an existing record."	

VII. Disputed Claim Terms #5: "system database"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**

"Plain meaning. A database is a database and yes there is a system involved but all databases involve some type of system. Currently, that hardly means it is connected to a [local access network ('LAN')] and generally its not given improvement in WiFi and cellular technologies like 5G." Pl.'s Resp. Cl. Const. Br. at 9–10.	"A central database server, connected to the automated access control system over a local area network, that stores at least individual real time records and a security list for multiple automated access control systems." Defs.' Cl. Constr. Br. at 13.

The disputed term in used claims 1, 5, and 6. '844 patent col. 5 ll. 7–15, col. 6 ll. 9–14, 15–19. The following claim limitations highlight selected usage of the term in context:

> real time records are checked searching for a credential collected information match; individual suspicious status is checked against a security list stored in a *system database*; employee records are checked to determine if the individual is an employee; the type of entry, visitor, employee, contractor, supplier, or vendor, is determined; and admission is processed as entry or re-entry of the individuals,

id. col. 5 ll. 5–7,

> 5. An automated access control system as claimed in claim 1, wherein the *system database* includes one or more interrelated group of records: the airport employee as ESCORTER, the DMV vehicle registration card information, the driver identification record and the passengers' identification records.

id. col. 6 ll. 9–14,

> 6. An automated access control system as claimed in claim 1, includes: a wireless barcode reader, a *system database*, a suitable camera, a color plastic card printer, a keyboard, a laser printer, an intranet package and a display monitor.

id. col. 6 ll. 15–19.

A. Parties' Arguments

Defendants argue "system database" in the context of the '844 patent requires the combination of a central server, the automated access systems, and a local area network. Defs.' Cl. Constr. Br. at 14. According to defendants, the embodiment described in the '844 patent makes use of a network and limits the breadth of the term because a single embodiment can be appropriately used to limit patent scope. *Id.* at 13 (citing *Medicines Co. v. Mylan, Inc.*, 853 F.3d 1296, 1309 (Fed. Cir. 2017)).

Plaintiff argues patent scope can only be limited by a single embodiment when the term has no generally accepted technical meaning and intrinsic evidence is required to construe the

term. Pl.'s Resp. Cl. Constr. Br. at 10. Plaintiff further argues "the term 'system database' is being used in its conventional manner to simply describe a conventional component used in the invention." *Id.* The "'system database' . . . has a well understood meaning to one of ordinary skill in the art," so plaintiff argues "plain meaning should . . . control." *Id.* at 10–11.

B. Analysis

1. The Court's Preliminary Construction

Before the *Markman* hearing, the Court provided the parties with the Court's preliminary construction after considering both parties' claim construction briefs and all referenced materials in full. Tr. at 8:15–19. The Court first determined whether defendants' proposed construction was supported in the patent. Defendants' preferred construction imposes multiple limitations on the construction of the term. *See* Defs.' Cl. Constr. Br. at 13. Defendants construe "system database" to require a centralized server and a connection through a LAN from the server to the automated control system, while the "system database" stores real time records and a security list. *Id.* Defendants draw these limitations from language in the specification describing the "Airport Vehicular Gate Entry system" as an "enterprise platform." *Id.* at 14 (quoting '844 patent col. 2 ll. 40–47). In the system:

> multiple airport vehicular gates comprise one workstation each, interconnected in a network configuration, controlled by a central database server. All workstations collect and store data in the central database server. In such a network, all data is immediately available at all workstations. Such a strategy permits vehicles entering from one particular gate to exit from another gate.

'844 patent col. 2 ll. 40–47. The stated configuration does not explicitly correspond to a "system database" as used in claim 1. *Compare id.*, *with id.* col. 5 l. 12, col. 6 l. 10, col. 6 l. 16. Defendants conflate "central database server" as used in the specification with "system database" as used in the claims; however, these are not necessarily the same. The section of the specification cited by defendants refers to storage of information *collected by* the individual workstations. '844 patent col. 2 ll. 40–47. "All workstations collect and store data in the *central database server*[,]" so "all data is immediately available at all workstations" and the system can stay up to date when a vehicle "exit[s] from another gate." *Id.* (emphasis added). By contrast, the "system database" referenced in claim term 1 stores a "security list." *Id.* col. 5 ll. 12. The specification indicates the invention—the Airport Vehicular Gate Entry system—"incorporates critical data" from security lists which "could be supplied by . . . the US Department of Homeland Security, the Federal Bureau of Investigation and other security agencies." '844 patent col. 1 ll. 54–59. In other words, the "central databases server" is not necessarily the same as the "system database." Consequently, the "system database" in claim 1 could be a separate repository of information and is not limited by the methods for storing information collected by each workstation in a central database server.

Moreover, a particular embodiment described in the specification should not limit the scope of the claims. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1323–24 (Fed. Cir. 2005) (noting that the Federal Circuit "expressly reject[s] the contention that if a patent describes only a single

embodiment, the claims of the patent must be construed as being limited to that embodiment"). Even if the language cited by defendants were relevant to the definition of system database as used in claim 1, the scope of the claim term should not be so limited. *Id.* Defendants cite *Medicines* for the proposition a single embodiment can be used to provide a limited definition for claim construction. Defs.' Cl. Constr. Br. at 13 (citing *Medicines*, 853 F.3d at 1309). *Medicines* is inapposite to the facts in this case. First, in *Medicines*, the court was required to construct a term—"efficient mixing"—which did not "carr[y] an accepted meaning to one of ordinary skill in the art." *Medicines*, 853 F.3d at 1308. Second, in *Medicines*, construction of the term in a manner consistent with the specification was necessary to overcome the prior art. *Id.* at 1303–05. The patent's novelty was based on its "batch consistency," and the specification taught "efficient mixing as a necessary and sufficient condition for achieving batch consistency." *Id.* at 1305. Therefore, constructing "efficient mixing" based on the specification was necessary to cabin the scope of the patent. In this case, "system database" is a common term of art and the novelty of the patent does not depend on this term's construction. *See* Pl.'s Resp. Cl. Constr. Br. at 10–11. Therefore, the Court did not preliminarily construe "system database" with the limitations of the embodiment described in the '844 patent specification. *See* '844 patent col. 2 ll. 40–47.

As plaintiff neither disavows claim scope or acts as his own lexicographer, the Court preliminarily construed the term according to its plain and ordinary meaning. *Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (citing *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1580 (Fed. Cir. 1996)). Insofar as a specific definition is useful, the Court offered the following: "a collection of data organized for retrieval by a computer, and accessible by an automated access control system." *See Database*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/database, (last visited Jan. 10, 2023) ("a usually large collection of data organized especially for rapid search and retrieval (as by a computer)").

2. The Court's Final Construction

At the *Markman* hearing, both parties agreed to the Court's preliminary plain meaning construction. Tr. at 67:20–68:11. The Court adopts its preliminary construction as final: plain meaning, "a collection of data organized for retrieval by a computer, and accessible by an automated access control system."

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning. A database is a database and yes there is a system involved but all databases involve some type of system. Currently, that hardly means it is connected to a LAN and generally its not given improvement in WiFi and cellular technologies like 5G."	"A central database server, connected to the automated access control system over a local area network, that stores at least individual real time records and a security list for multiple automated access control systems."
Court's Construction	
Plain meaning: "a collection of data organized for retrieval by a computer, and accessible by an automated access control system."	

VIII. Disputed Claim Term #6: "the type of entry, visitor, employee, contractor, supplier, or vendor, is determined"

Plaintiff's Proposed Construction	Defendants' Proposed Construction
"Plain meaning. Visitor is a well understood term. So is an employee. Contractor. Supplier. And Vendor." Pl.'s Resp. Cl. Constr. Br. at 11.	"Indefinite. To the extent the term is construed, Defendants propose: The system is capable of categorizing the individual presenting the credential as each one of the following and categorizes the individual as one of the following: visitor, employee, contractor, supplier, or vendor." Defs.' Cl. Constr. Br. at 14.

The disputed term is used in claim 1:

> real time records are checked searching for a credential collected information match; individual suspicious status is checked against a security list stored in a system database; employee records are checked to determine if the individual is an employee; *the type of entry, visitor, employee, contractor, supplier, or vendor, is determined*; and admission is processed as entry or re-entry of the individuals,

'844 patent col. 5 ll. 8–15.

A. Parties' Arguments

Defendants argue the disputed term is indefinite. Defs.' Cl. Constr. Br. at 14–15. Defendants concede the terms visitor, employee, contractor, supplier, and vendor are "well understood terms," but not well understood in the context of the claim. *Id.* Defendants state the patent is "silent with respect to how the system determines who is in the other four distinct categories of visitor, contractor, supplier, or vendor." *Id.* at 15–17. Defendants argue "the claim creates a zone of uncertainty as to what activity is encompassed under the claim term," and "the claim term remains indefinite." *Id.* In the alternative, defendants argue the term should be construed to "properly parse[] the potentially confusing use of passive voice and an 'or'-joined list." *Id.* at 17.

Plaintiff argues the terms "visitor, employee, contractor, supplier, [and] vendor" all have a well understood plain meaning. *See* Pl.'s Cl. Constr. Br. at 11. Plaintiff claims "the system would determine whether someone is a contractor, supplier or vendor: just as with their employees, an airport maintains a database of such individuals." *Id.* Plaintiff further claims defendants' proposed construction should be rejected because defendants' "definition that the

system must be both capable of and actually perform this step" is contrary to the claim's language stating "one or more of the following processing is performed." *Id.* at 12.

B. Analysis

1. The Court's Preliminary Construction

Before the *Markman* hearing, the Court provided the parties with the Court's preliminary construction after considering both parties' claim construction briefs and all referenced materials in full. Tr. at 8:15–19. The '844 patent details the process followed when "standardized personal identification credentials" are presented to the reader by the attendant. *See* '844 patent col. 3 ll. 35–64. When the information is presented, "[t]he system checks database information to determine whether the individual is an employee." *Id.* col. 3 ll. 42–43. The system then proceeds to validate the credentials by comparing them to separate "TSA NO-FLY and SELECTEE" lists. *Id.* col. 3 ll. 47–48. Following the comparison, the system prompts the attendant to insert the credential ID into an "authenticator apparatus" which verifies "physical aspects" of the ID by comparing it to stored templates. *Id.* col. 3 ll. 54–60. "If all checks are negative, . . . [t]he system . . . prints a time sensitive encoded pass." *Id.* col. 3 ll. 61–64. The specification focuses heavily on the procedure used to identify employees, but it also mentions the system's capability to "automatically collect[] data and build visitor records." *Id.* col. 1 ll. 61–62. The parent patent specification also states "[t]he system checks database information to determine whether the individual is an employee, contractor, vendor, supplier or a visitor." '732 patent col. 10 ll. 33–35. Even though the process detailed in the specification does not describe how the system would verify other individuals such as visitors, the Court is "cautioned against limiting the claimed invention to preferred embodiments or specific examples in the specification." *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1328 (Fed. Cir. 2002) (citing *Comark Comm'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1186 (Fed. Cir. 1998)). The use of the system for other categories of individuals is implied because when construing claims the Court looks "to the words of the claims themselves . . . to define the scope of the patented invention," and the specification allows one to extend the use of the system to other categories of individuals. *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996). The '844 patent describes two key components in the process of authenticating credentials, i.e., building records (employees and visitors) and comparing the credentials to the records, so the patent "need not explicitly include information [on how the comparison occurs] that is already well known in the art." *Presidio Components, Inc. v. Am. Tech. Ceramics Corp.*, 875 F.3d 1369, 1376 (Fed. Cir. 2017). The '844 patent contains sufficient disclosure to rebut defendants' indefiniteness arguments because the "general approach [of scanning credentials and comparing to a database is] sufficiently well established in the art and referenced in the patent." *Id*. at 1377. The detailed description of the comparison process and the development of databases for people other than employees makes it reasonable to expect a "skilled artisan to know the scope of the claimed invention with reasonable certainty." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 910 (2014). Accordingly, when the authentication process is "read in the view of the specification," describing the building of visitor records, the process is reasonably applied to other categories of individuals such as vendors, contractors, suppliers, and visitors. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995).

Defendants note the terms "contractor" and "supplier" appear "nowhere outside their use in the claim at issue." Defs.' Cl. Constr. Br. at 15. Similarly, the term "vendor" is only used once "outside of the claim term issue." *Id.* Although "visitor" is frequently used, the term is not explicitly defined. *See* '844 patent. Accordingly, none of the terms are defined, so the patentee did not "set[] out a definition and act[] as his own lexicographer." *Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (citing *Vitronics*, 90 F.3d at 1580). Similarly, the patentee did not disavow the claim scope in the specification. *Id.; see* '844 patent. The patentee neither set a definition nor disavowed the full scope of a claim term in the specification, so the ordinary and customary meanings of the terms visitor, employee, contractor, supplier, vendor apply. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005). The Court preliminarily construed "the type of entry, visitor, employee, contractor, supplier, or vendor, is determined" as: "Using the individual real time record built from the presented personal identification credentials, the software application checks the system database stored information to ascertain whether the individual presenting the credential is one of the following: visitor, employee, contractor, supplier, or vendor."

2. The Court's Final Construction

At the *Markman* hearing, both parties agreed to the Court's preliminary construction. *See* Tr. at 68:11–69:10. The Court adopts it preliminary construction as final: "Using the individual real time record built from the presented personal identification credentials, the software application checks the system database stored information to ascertain whether the individual presenting the credential is one of the following: visitor, employee, contractor, supplier, or vendor."

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning. Visitor is a well understood term. So is an employee. Contractor. Supplier. And Vendor."	"Indefinite. To the extent the term is construed, Defendants propose: The system is capable of categorizing the individual presenting the credential as each one of the following and categorizes the individual as one of the following: visitor, employee, contractor, supplier, or vendor."
Court's Construction	
"Using the individual real time record built from the presented personal identification credentials, the software application checks the system database stored information to ascertain whether the individual presenting the credential is one of the following: visitor, employee, contractor, supplier, or vendor."	

IX. Disputed Claim Term #7: "an ID authenticator"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**

"An ID authenticator is a device that scans a personal identification document (including, but not limited to, a U.S. State driver's license or a U.S. passport) and determines the authenticity of the identification document using one or more embedded security features." Pl.'s Resp. Cl. Constr. Br. at 12.	"Indefinite. To the extent the term is construed, Defendants propose: A commercial identification card authentication device, separate from the standardized credential reader device, which further includes 'means to read non-encoded credentials.'" Defs.' Cl. Constr. Br. at 17.

The disputed term is used in claim 1:

> an *ID authenticator*, wherein a credential to be authenticated is presented, a credential physical aspect and embedded security features are analyzed to determine the possibility of any tempering or forgery and provide an authenticity risk rating, said *ID authenticator* comprises means to read non-encoded credentials, whereas said *ID authenticator* generates an authentication data record comprising presented credential information and authentication rating,

'844 patent col. 5 ll. 16–23.

A. Parties' Arguments

Defendants argue "ID authenticator" is indefinite because it is not supported by sufficient structure or detail.[8] Defs.' Cl. Constr. Br. at 17. According to defendants, within the context of the claims, the patent defines multiple "who's" of the "ID authenticator": (1) a mechanism or apparatus which automatically analyzes an ID for authentication issues; and (2) a human attendant who uses a device to perform authentication. *Id.* at 18. Defendants also argue the specification is silent on "what" the "ID authenticator" authenticates or "how" the "ID authenticator" performs the relevant analysis. *Id.* at 18–19. The patent suggests either the process may require the mechanism perform the analysis automatically or the mechanism may merely assist a human operator in analyzing the ID. *Id.* at 18–19. Accordingly, defendants assert the claim is indefinite. *Id.*

Defendants also argue, citing *Becton*, based on the structure of the '844 patent, the "ID authenticator" and credential reader device must necessarily be separate. Defs.' Reply Cl. Constr. Br. at 8 (citing *Becton, Dickinson & Co. v. Tyco Healthcare Grp.*, 616 F.3d 1249, 1254 (Fed. Cir. 2010)). Defendants note "Claim 1 separately lists 'a standardized credential reader means for reading a credential encoded with personal identification' and 'an ID authenticator' that 'comprises means to read non-encoded credentials.'" *Id.* at 8 (quoting '844 patent col. 5 ll. 1–2, 16–21). Defendants argue the distinction creates a presumption the devices are separate,

[8] Defendants argue the claim term is indefinite but do not invoke a specific paragraph under § 112 in their briefing.

and nothing in the intrinsic record contemplates practice of the functions in a single device. *Id.* at 8. Defendants also argue the specification outlines multiple purposes for the ID authenticator, and therefore the exact function is unclear. Defs.' Cl. Constr. Br. at 18. If the Court finds the term not indefinite, defendants assert the term should be limited to non-encoded credentials and a "commercial" product as described in certain embodiments. *Id.* at 19.

Plaintiff argues "ID authenticator" is not inherently ambiguous because the '844 patent specifically references "a commercial ID card authenticator." Pl.'s Resp. Cl. Constr. Br. at 12 (citing '844 patent fig.1). According to plaintiff, the number of suitable devices is limited, and, therefore, the boundary of the claims is not indefinite. *Id.* at 12–13. Moreover, plaintiff contends the claims need not define the operator and device relationship as the specific device chosen will define the relationship. Pl.'s Surreply Cl. Constr. Br. at 8. The patent does not differentiate the functions of the standardized credential reader and "ID authenticator," so plaintiff argues the claim encompasses a machine performing both functions. *Id.* at 9–10. "Plaintiff concedes, however, that plain meaning will indeed not suffice for this Claim" and instead invokes means-plus-function claim interpretation. Pl.'s Resp. Cl. Constr. Br. at 13–14. Under a means-plus-function construction, plaintiff asserts the patent contains sufficient structure to define the meaning of "ID authenticator." *Id.* at 14.

B. Analysis

1. The Court's Preliminary Construction

Before the *Markman* hearing the Court provided the parties with the Court's preliminary construction after considering both parties' claim construction briefs and all referenced materials in full. Tr. at 8:15–19. The patent references a commercial identification card authentication device. '844 patent fig.1, element 4. While a question exists as to which specific model the patent contemplates, the options are limited, and a skilled artisan would understand the boundaries of the claim with reasonable certainty. *Presidio Components, Inc. v. Am. Tech. Ceramics Corp.*, 875 F.3d 1369, 1376 (Fed. Cir. 2017). Disclosure of a specific device, or specific characteristics of a suitable device, is not the type of information that must be explicitly included as it "is already well known in the art." *Id.* Therefore, the Court did not preliminarily find the term to be indefinite.

The parties agree the term refers to a commercial identification card authentication device if the term is not indefinite. *See* Pl.'s Resp. Cl. Constr. Br. at 12; Defs.' Cl. Constr. Br. at 19. Given the device must be a standard commercial product, the Court found no reason to hold the term indefinite or to provide a unique construction in its preliminary construction. The patentee did not act as his own lexicographer, nor did patentee clearly disavow claim scope; neither exception to use of the plain and ordinary meaning is triggered. *See Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (citing *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1580 (Fed. Cir. 1996)); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005).

While "ID authenticator" should be given its plain and ordinary meaning, the parties dispute whether the authentication device is necessarily separate from the standardized credential

reader. *See* Pl.'s Resp. Cl. Constr. Br. at 14; Defs.' Reply Cl. Constr. Br. at 8. The '844 patent provides several reasons why the two devices would be considered separate and no reasons as to why they should be considered as one machine. First, Figure 1 of the '844 patent shows them as separate machines (#4–Commercial ID card Authenticator; #3–Apparatus for Recovering Information from standardized personal identification Credentials). '844 patent fig.1, elements 3, 4. Figure 1 is consistent with the claim language, which divides the functions between the standardized credential reader, *id.* col. 5 ll. 1–15, and the "ID authenticator," *id.* col. 5 ll. 16–23. Second, the '732 patent, which covers the standardized credential reader, does not contemplate or enable a device capable of ID authentication. *See* '732 patent. The "ID authenticator" is accordingly a new disclosure in the '844 patent, which does not teach the combination of "ID authentication" into the standardized credential reader. The intrinsic record provides support for two separate devices but does not provide support for combining these two devices into one; the Court therefore considered the devices separately. *See* '844 patent.

In sum, the Court preliminarily found "ID authenticator" should be given its plain meaning, with the caveat the device must be separate from the "standardized credential reader means." Insofar as a specific definition is clarifying, the Court offered the following: "a commercial identification card authentication device, separate from the standardized credential reader device."

2. The Court's Final Construction

At the *Markman* hearing, plaintiff argued the authentication device need not be separate from the credential reader but otherwise was satisfied with the Court's construction. Tr. at 70:10–17. ("THE COURT: [T]he question is whether or not the ID authenticator necessarily has to be separate from the credential reader. Is that right? [PLAINTIFF]: Yes, that's the issue . . . . The rest of it, obviously, we have no issue."). Plaintiff stated the claims support a combined device. Tr. at 72:18–20. ("THE COURT: [W]hat describes them as the same thing? [PLAINTIFF]: I think the party's claims ultimately."). Plaintiff was unable to point to any claim suggesting the two devices could be combined into a single device and agreed there were a number of instances where separate devices were described throughout the specification and the claims. *See* Tr. at 72:1–74:25. Plaintiff's only explanation was the devices "could possibly be separate, they could possibly be combined." Tr. at 74:14–15. Defendants reasserted the claims and specification "uniformly and exclusively treats ["the standardized credential reader means" and "ID authenticator"] as separate from one another" and agreed with the Court's preliminary construction. Tr. at 75:19–76:18, 79:14–15. Plaintiff failed to provide any support from the intrinsic record for a combined credential reader and ID authenticator; accordingly, the Court adopts its preliminary construction of "ID authenticator": "A commercial identification card authentication device, separate from the standardized credential reader device."

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"An ID authenticator is a device that scans a personal identification document (including, but not limited to, a U.S. State driver's license or a U.S. passport) and determines the authenticity of the identification document	"Indefinite. To the extent the term is construed, Defendants propose:

using one or more embedded security features."	A commercial identification card authentication device, separate from the standardized credential reader device, which further includes 'means to read non-encoded credentials.'"
Court's Construction	
"A commercial identification card authentication device, separate from the standardized credential reader device."	

X. Disputed Claim Term #8: "means to read non-encoded credentials"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning. Any automated ID authentication systems also includes means to read the non-encoded aspects of the identification." Pl.'s Resp. Cl. Constr. Br. at 14.	"Indefinite." Defs.' Cl. Constr. Br. at 20.

The disputed term is used in claim 1.

> an ID authenticator, wherein a credential to be authenticated is presented, a credential physical aspect and embedded security features are analyzed to determine the possibility of any tempering or forgery and provide an authenticity risk rating, said ID authenticator comprises *means to read non-encoded credentials*, whereas said ID authenticator generates an authentication data record comprising presented credential information and authentication rating,

'844 patent col. 5 ll. 16–23.

A. Parties' Arguments

Defendants argue the term is a means-plus-function claim and should be construed under 35 U.S.C. § 112, ¶ 6. Defs.' Cl. Constr. Br. at 20. According to defendants, the word "means" creates a rebuttable presumption § 112, ¶ 6 applies, and when construed as a means-plus-function claim, the specification fails to provide sufficient structure to disclose the function. *Id.* As a result, defendants assert the term is indefinite. *Id.*

Plaintiff avers the specification discloses sufficient structure to perform the function in its entirety. Pl.'s Resp. Cl. Constr. Br. at 14–15. Plaintiff points to the language from the specification, related to vehicle tracking, which suggests the patent discloses image acquisition and character recognition. *Id.* (citing '844 patent col. 3:25–29). According to plaintiff, the PHOSITA would recognize these requirements for vehicle tracking are applicable structure for "means to read non-encoded credentials." *Id.*

B. Analysis

1. The Court's Preliminary Construction

Before the *Markman* hearing, the Court provided the parties with the Court's preliminary construction after considering both parties' claim construction briefs and all referenced materials in full. Tr. at 8:15–19. The Court first considered whether the disputed term overcomes the presumption of a means-plus-function construction. Ordinarily, the word "means" in a claim creates a rebuttable presumption § 112, ¶ 6 applies. *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1348 (Fed. Cir. 2015). Using the term "means to read non-encoded credentials" creates a rebuttable presumption of means-plus-function construction, which can be overcome if the patent recites sufficient structure for performing the function in its entirety. *Skky, Inc. v. MindGeek, S.A.R.L.*, 859 F.3d 1014, 1019 (Fed. Cir. 2017); *see Biomedino, LLC. v. Waters Techs. Corp.*, 490 F.3d 946, 950 (Fed. Cir. 2007) (discussing the inclusion of "means" in claim language creates a presumption of § 112, ¶ 6); *Altiris, Inc. v. Symantec Corp.*, 318 F.3d 1363, 1375 (Fed. Cir. 2003) ("[T]his presumption can be rebutted where the claim, in addition to the functional language, recites structure sufficient to perform the claimed function in its entirety."). The claim language indicates "ID authenticator" is the structure which performs the function. *See* '844 patent col. 5 ll. 16–23. The key language from claim 1 of the'844 patent is the term "comprises" which links "ID authenticator" to "means to read non-encoded credentials," therefore implying "ID authenticator" provides the structure for the claimed functionality. *Id.* Given the Court's finding that "ID authenticator" is sufficiently specific when interpreted by the PHOSITA, the overall claim term "ID authenticator comprises means to read non-encoded credentials" provides adequate structure to implement the function in its entirety. *See supra* at Section IX. The Court preliminarily found the term overcame the presumption of a means-plus-function construction because there was adequate structure for the claimed functionality; accordingly, the Court preliminarily found the term to be definite. *See Williamson*, 792 F.3d at 1351–52.

The Court preliminarily found "means to read non-encoded credentials" should be construed as a function of the "ID authenticator." When construed in this manner, the phrase should be given its plain and ordinary meaning: "an apparatus capable of image acquisition and taking in the sense of letters and symbols." *See Read*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/read, (last visited Jan. 10, 2023) ("to receive or take in the sense of (letters, symbols, etc.) especially by sight or touch").

2. The Court's Final Construction

At the *Markman* hearing, the parties disputed whether the rebuttable presumption is overcome. Plaintiff argued the application of § 112, ¶ 6 is rebutted for this term. Tr. at 86:12–21. Defendants claimed the term "means to read non-encoded credentials" invokes means-plus-function construction and does not overcome the rebuttable presumption as the claim has "no structure disclosed for performing that process of reading non-encoded credentials." Tr. at 77:14–15, 78:2–4. Defendants argued, "[T]here's a disconnect between what the specification teaches and what the claims require." Tr. at 78:6–7. The disconnect, according to defendants, is because "the claim requires the ID authenticator box scans the non-encoded credential, does [optical character recognition ('OCR')] and generates a data record" whereas "[t]he specification teaches that the ID authenticator takes a picture . . . then sends that to the system for doing the

character recognition." Tr. at 78:12–18. Defendants claimed the discrepancy between the specification and the claim results in indefiniteness. *See* Tr. at 89:24–90:6. Defendants, however, were unable to point to any location in the patent where the claim mandates OCR of the credential information. *See* Tr. at 84:9–90:5 ("THE COURT: So your argument is that from the claim, presented credential information must be an OCR-converted digital file? [DEFENDANTS]: The authentication data record includes presented credential information which necessarily is OCR . . . . That's our position. . . . THE COURT: I just don't see where that conversion is mandated in the claim. [DEFENDANTS]: . . . I can't point to anything that specifically says the personal information in the authentication data record constitutes post-OCR data.").

The parties misunderstood the Court's preliminary construction to include OCR. Defendants understood the Court's preliminary construction to include OCR, which is in line with the claim but not the specification. Tr. at 88:23–89:2 ("[DEFENDANTS]: [W]e agree generally with [the preliminary definition] capturing the notion of reading a non-encoded credential, because you're doing an OCR process."). Plaintiff also misunderstood the Court's construction to include OCR. Tr. at 89:20–23. Plaintiff initially required the "ID authenticator" be capable of doing OCR in plaintiff's brief but later changed position and agreed the Court's construction does not and should not include OCR. Tr. at 91:13–15 ("[PLAINTIFF]: I agree. I mean, certainly, I've changed my position from that brief at this point, based on [the preliminary construction], as well as this discussion."). The Court's preliminary definition, however, did not convey the capability of OCR because the key term in the disputed claim is "read" which is defined as "to receive or take in the sense of (letters, symbols, etc.) especially by sight or touch." *Read*, Merriam-Webster Dictionary. The process of OCR requires the further recognition of these letters and symbols as alphanumeric and conversion into digital data, which was not described in the Court's preliminary construction. Tr. at 88:20–22. As defendants have not persuaded the Court OCR should be included in its construction, the Court retains its preliminary construction of the claim term: "An apparatus capable of image acquisition and taking sense of letters and symbols."

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning. Any automated ID authentication systems also includes means to read the non-encoded aspects of the identification."	"Indefinite."
Court's Construction	
"An apparatus capable of image acquisition and taking sense of letters and symbols."	

XI. Disputed Claim Term #9: "authentication data record"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning." Pl.'s Resp. Cl. Constr. Br. at 15.	"Indefinite. To the extent the term is construed, Defendants propose:

	A record, separate from any individual real time record, containing both information extracted from a scanned image of the credential and an 'authentication rating.'" Defs.' Cl. Constr. Br. at 21.

The disputed term is used in claim 1:

> an ID authenticator, wherein a credential to be authenticated is presented, a credential physical aspect and embedded security features are analyzed to determine the possibility of any tempering or forgery and provide an authenticity risk rating, said ID authenticator comprises means to read non-encoded credentials, whereas said ID authenticator generates *an authentication data record* comprising presented credential information and authentication rating,

'844 patent col. 5 ll. 16–23.

A. Parties' Arguments

Defendants argue the ID authenticator generates two types of records: (1) the image of the vehicle registration card; and (2) the data captured and analyzed when the ID authenticator performs ID checks against stored templates. Defs.' Cl. Constr. Br. at 21–22. According to defendants, "[b]ecause one of ordinary skill is left in a zone of uncertainty as to which type(s) of record would be encompassed by the claim term, the term should be held indefinite." *Id.* at 22. In the alternative, defendants propose "authentication data record" should refer only to information extracted from the scan of a vehicle registration card. *Id.* Defendants argue plaintiff's interpretation is overbroad as it would include any information extracted from a credential, regardless of the method of extraction. *Id.*

Plaintiff argues there is no ambiguity in the claims. Pl.'s Resp. Cl. Constr. Br. at 16. Plaintiff explains "authentication data record" comprises information extracted when the ID authenticator reads credential information and the authentication rating. *Id.* Plaintiff's construction excludes any DMV or vehicle registration records because such records are not credentials as defined by the claims. *Id.* at 15–16. Rather, the claims refer to personal credentials. *Id.* Plaintiff asserts the term should be given it plain and ordinary meaning. *Id.* at 15.

B. Analysis

1. The Court's Preliminary Construction

Before the *Markman* hearing, the Court provided the parties with the Court's preliminary construction after considering both parties' claim construction briefs and all referenced materials in full. Tr. at 8:15–19. The Court first determined the scope of "authentication data record." Neither party contests the "authentication data record" includes at least an image of the presented

credential. *See* Defs.' Cl. Constr. Br. at 21–22; Pl.'s Resp. Cl. Constr. Br. 15–16. The '844 specification supports this notion: "[t]he authenticator acquires an image of the registration card and sends the image to the system for proceeding with character recognition." '844 patent col. 3 ll. 27–29. "The system picks up the individual photo provided by the authenticator returned record . . . ." *Id.* col. 3 ll. 61–63. "[T]he automated access control system picks up the individual photo provided by the authentication data record . . . ." *Id.* col. 5 ll. 41–42.

The parties dispute whether "authentication data record" is separate from other data records. Defs.' Cl. Constr. Br. at 21; Pl.'s Resp. Cl. Constr. Br. at 16. Different terms in a claim are construed to have different meanings, and meaning should be given to all terms in a claim. *MicroStrategy Inc. v. Bus. Objects Americas*, 238 F. App'x 605, 609 (Fed. Cir. 2007) ("[D]ifferent claims terms are presumed to have different meanings."); *see Merck & Co. v. Teva Pharm. USA, Inc.*, 395 F.3d 1364, 1372 (Fed. Cir. 2017). The Court preliminarily construed claim term 7, "ID authenticator," as necessarily separate from the "standardized credential reader means." *See supra* Section IX. Consequently, the record generated by the ID authenticator must also necessarily be a separate record from the record created by the "standardized credential reader means." In other words, an individual real time record must be different from an "authentication data record." Paralleling the Court's construction of claim term 3—deriving the "individual real-time record" from "standardized credential reader means"—the "authentication data record" must come from the "ID authenticator." The derivation is explicitly supported by the claim language: "whereas said ID authenticator generates an authentication data record comprising presented credential information and authentication rating . . . ." '844 patent col. 5 ll. 21–23; *see supra* Section V.

The specification also suggests "authentication data record" should include an authentication rating. *Compare* '844 patent col. 3 ll. 26–30 ("The authenticator acquires an image of the registration card and sends the image to the system for proceeding with character recognition. This data becomes the second record in the entry group."), *with id.* col. 3 ll. 56–60 ("The authentication process provides a mean [sic] of determining and rating ID physical aspects security risks. The authenticator matches the ID against stored templates, and looks for the ID security features to determine the possibility of any ID tampering."). While the registration card has an image captured and stored, the credential has its unique security features analyzed to create an authentication rating. *See id.* col. 3 ll. 26–30, 56–60. The patent claim, therefore, refers to the credential ID and the information captured from the credential ID when describing an "authentication data record" comprising presented credential information and authentication rating. *See supra* Section IX. As such, the Court preliminarily construed the "authentication data record" to be "[a] record, separate from any individual real time record, containing both an authentication rating and information extracted from a scanned image of the credential."

2. The Court's Final Construction

At the *Markman* hearing, plaintiff agreed to the Court's preliminary construction. Tr. at 91:24–25. ("[PLAINTIFF]: Yeah, I have no [problem] with [the Court's] construction [of term 9]."). Defendants requested clarification as to the use of "information extracted from a scanned image of the credential." Tr. at 92:2–7. Consistent with the term 8 arguments, defendants argued disputed term 9 also "include[s] post-OCR information" Tr. at 94:7–15. This was

defendants' only disagreement with the preliminary construction. Tr. 97:5–8. For all the reasons the Court notes in term 8, *supra*, there is no OCR requirement. The Court modifies its preliminary construction and adopts the following final construction: "A record, separate from any individual real time record, containing both an authentication rating and a digital image of the credential."

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning."	"Indefinite. To the extent the term is construed, Defendants propose: A record, separate from any individual real time record, containing both information extracted from a scanned image of the credential and an 'authentication rating.'"
Court's Construction	
"A record, separate from any individual real time record, containing both an authentication rating and a digital image of the credential."	

XII. Disputed Claim Term #10: "authenticity risk rating" / "authentication rating" / "ID forgery risks rating"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"An authentication rating is either a numerical scale based on various authentication criteria, or a narrative or message relating to authenticity that is delivered to the end user of a device that can determine authenticity. Many numerical scales are, in fact, simply a series of different narrative or message choices that can be converted into a number." Pl.'s Resp. Cl. Constr. Br. At 16–17.	"Indefinite." Defs.' Cl. Constr. Br. At 23.

The disputed term is used in claim 1:

> an ID authenticator, wherein a credential to be authenticated is presented, a credential physical aspect and embedded security features are analyzed to determine the possibility of any tempering or forgery and provide an *authenticity risk rating*, said ID authenticator comprises means to read non-encoded credentials, whereas said ID authenticator generates an authentication data record comprising presented credential information and *authentication rating* . . .
>
> wherein, upon a credential reading, the automated access control system automatically determines the source of the credential data record, and

> automatically extracts personal information to be checked against a security list, TSA NO-FLY list, SELECTEE list, other alternative credentials; whereas upon the credential authentication, the automated access control system automatically extracts authentication information from the authentication data record, and subsequently displays a warning window, as a result of the individual credentials match and *ID forgery risks rating* contained in the authentication data record.

'844 patent col. 5 ll. 16–37.

A. Parties' Arguments

Defendants argue the patent uses "authenticity risk rating," "authentication rating," and "ID forgery risks rating" interchangeably. Defs.' Cl. Constr. Br. At 23. Defendants argue, however, *Merck* dictates the claim terms must be construed to have unique and distinct meanings. *Id.* (citing *Merck & Co. v. Teva Pharm. USA, Inc.*, 395 F.3d 1364, 1372 (Fed. Cir. 2005)). The patent cannot support a construction whereby all three terms have a different meaning, so defendants argue the patent must fail for indefiniteness. *Id.* At 24.

Plaintiff argues the patent language makes clear the authenticity risk rating, authentication rating, and ID forgery risks rating are all produced by the "standardized credential reader means." Pl.'s Resp. Cl. Constr. Br. At 17–18. Plaintiff asserts a limited number of devices are commercially available; therefore, the analytical outputs of such machines are familiar in the industry and the claim is sufficiently definite. *Id.* Plaintiff rejects defendants' reliance on *Merck*, and argues *Merck* suggests unique definitions are preferred but not required. *Id.* At 17. Plaintiff further argues a PHOSITA would understand all three terms refer to the same output, and, therefore, the claim is sufficiently definite. *Id.* 17–18.

B. Analysis

1. The Court's Preliminary Construction

Before the *Markman* hearing, the Court provided the parties with the Court's preliminary construction after considering both parties' claim construction briefs and all referenced materials in full. Tr. At 8:15–19. Patent claim interpretation preferably presumes different claim terms have different meanings. *MicroStrategy Inc. v. Bus. Objects Americas*, 238 F. App'x 605, 609 (Fed. Cir. 2007); *see Merck*, 395 F.3d at 1372. This presumption can be "overcome where . . . the evidence indicates that the patentee used the . . . terms interchangeably." *Baran v. Med. Device Techs., Inc.*, 616 F.3d 1309, 1316 (Fed. Cir. 2010) (citing *Tehrani v. Hamilton Med., Inc.*, 331 F.3d 1355, 1361 (Fed. Cir. 2003)). In *Baran*, the Federal Circuit construed the descriptors "detachable" and "releasably" to have the same meaning based on the overall context of the claim language. *Id.*

The present case, like *Baran*, uses three terms interchangeably. Each of the three variations of the term "rating" occur when describing the same process (ID authentication) by the same apparatus (ID authenticator) evaluating the same aspects (an ID's physical aspects and

embedded security features) to produce the same output (authentication data record), suggesting interchangeability of the terms. *Compare* '844 patent col. 5 ll. 16–21 ("ID authenticator . . . a credential physical aspect and embedded security features are analyzed to . . . *provide an authenticity risk rating* . . . [which] generates *an authentication data record comprising presented credential information and authentication rating*") (emphasis added), *with id.* Col. 5 ll. 31–37 ("whereas upon the credential authentication . . . [the ID authenticator] automatically extracts *authentication information from the authentication data record,* and subsequently displays a warning window, as a result of the individual credentials match *and ID forgery risk rating contained in an authentication data record.*") (emphasis added). The claim begins by describing how "an ID authenticator . . . [is used to] determine the possibility of any tempering [sic] and forgery and provide an authenticity risk rating" for a presented credential. *Id.* Col. 5 ll. 16–19. The claim then contrasts this process with the functioning of the same ID authenticator when "non-encoded" credentials are presented which results in the generation of an "authentication data record comprising [of] presented credential information and [an] authentication rating." *Id.* Col. 5 ll. 20–23. The claim continues describing how a "central processing unit" receives the "authentication data record" and "automatically extracts authentication information from the authentication data record." *Id.* Col. 5 ll. 24–34. The central processing unit then "displays a warning window" based on its comparison of the authentication information and "ID forgery risks rating" extracted from the authentication data record. *Id.* Col. 5 ll. 34–37. No specific definition of each of the terms exists in the intrinsic record to suggest the terms are not interchangeable, so the "evidence [and context of the terms] indicates that the patentee used the [three] terms interchangeably." *Baran*, 616 F.3d at 1316. When viewed within context, a skilled artisan would know the scope of the claimed invention with reasonable certainty—these rating descriptors refer to the same output and are interchangeable. *See Presidio Components, Inc. v. Am. Tech. Ceramics Corp.*, 875 F.3d 1369, 1376 (Fed. Cir. 2017). Accordingly, the Court rejected defendants' indefiniteness arguments. *See id.*

Given the language of the claim, and the general purpose of the ID authenticator in relation to the overall process, the Court preliminarily construed all three "rating" terms to mean: "[a] grade of an ID's security risks provided by the ID authenticator by analyzing physical aspects and embedded security features to determine the possibility of any tampering or forgery by matching with stored templates." *See* '844 patent col. 5 ll. 16–19 ("ID authenticator . . . [is used to] determine the possibility of any tempering [sic] and forgery"), col. 3 ll. 56–60 ("The authentication process provides a means of determining and rating ID physical aspects security risks. The authenticator matches the ID against stored templates, and looks for ID security features to determine the possibility of any ID tempering [sic]").

2. The Court's Final Construction

At the *Markman* hearing, defendants argued the term is indefinite because the terms are presumed to have "three different meanings" and the specification does not support or define even one of the terms. Tr. At 98:13–23. Defendants further argued the specification does not support "how [the rating] is used." *Id.* In response, plaintiff stated the terms are interchangeable, and a PHOSITA would understand the terms are interchangeable. Tr. At 100:5–11. Regarding the Court's preliminary construction, defendants stated "grade" is not defined and might lead to future litigation. *See* Tr. At 98:24–99:9. Plaintiff claimed a PHOSITA

would understand the term "grade" as a percentage in the industry; for example, "TSA uses the percentage between a certain point and another point as being high risk, low risk, medium risk. There is no set risk . . . for everyone. It's just relative to the client." Tr. At 106:9–13 (plaintiff explaining "percentage of risk"). Further, plaintiff suggested at the *Markman* hearing defendants' argument—"[n]othing's taught in the specification about what a rating looks like"—is an enablement argument, not an indefiniteness argument. Tr. At 99:1–106:25; 25:18–24 (defendants stating if disputed terms are definite "we have some written description and enablement issues to grapple with, but that will be down the road").

Although enablement and indefiniteness may conceptually overlap, the legal standards are distinct. *See, e.g.*, *Augme Techs., Inc. v. Yahoo! Inc.*, 755 F.3d 1326, 1340 (Fed. Cir. 2014) ("Appellants' arguments appear to be based on the wrong legal standard, i.e., written description or enablement as opposed to indefiniteness."); *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1358 n.2 (Fed. Cir. 1999) ("[D]efiniteness and enablement are analytically distinct requirements [of validity], even though both concepts are contained in 35 U.S.C. § 112."). The Federal Circuit has held validity arguments, such as lack of enablement and lack of written description, are not proper to address during claim construction; therefore, the Court will not address defendants' enablement argument here. *See Philips v. AWH Corp.*, 415 F.3d 1303, 1327 (Fed. Cir. 2005) ("[W]e have certainly not endorsed a regime in which validity analysis is a regular component of claim construction."). Accordingly, the Court adopts its preliminary construction as final: "A grade of an ID's security risks provided by the ID authenticator by analyzing physical aspects and embedded security features to determine the possibility of any tampering or forgery by matching with stored templates."

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"An authentication rating is either a numerical scale based on various authentication criteria, or a narrative or message relating to authenticity that is delivered to the end user of a device that can determine authenticity. Many numerical scales are, in fact, simply a series of different narrative or message choices that can be converted into a number"	"Indefinite."
Court's Construction	
"A grade of an ID's security risks provided by the ID authenticator by analyzing physical aspects and embedded security features to determine the possibility of any tampering or forgery by matching with stored templates."	

XVIII. Disputed Claim Term #11: "automatically determines the source"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning, and as an example, the type of entry, visitor, employee, contractor, supplier, or vendor."	"Indefinite" or "Using common storage to verify that a submitted unique identifier has not already been assigned to another physical device."

Pl.'s Resp. Cl. Constr. Br. At 18.	Defs.' Cl. Constr. Br. At 24.

The disputed term is used in claim 1:

> wherein, upon a credential reading, the automated access control system *automatically determines the source* of the credential data record, and automatically extracts personal information to be checked against a security list, TSA NO-FLY list, SELECTEE list, other alternative credentials; whereas upon the credential authentication, the automated access control system automatically extracts authentication information from the authentication data record, and subsequently displays a warning window, as a result of the individual credentials match and ID forgery risks rating contained in the authentication data record.

'844 patent col. 5 ll. 26–37.

A. Parties' Arguments

Defendants argue the term "automatically determines the source" must be read in relation to the subsequent term "credential data record" and is therefore ambiguous. Defs.' Cl. Constr. Br. At 24. Assuming "credential data record" refers to information extracted from IDs processed by the system, the source could be: (1) the actual terminal device which originally processed the data record; or (2) the original source of the ID, such as the state agency which produced and issued the credential. *Id.* Defendants contend the term is ambiguous because "source" never appears anywhere else in the language of the patent. *Id.* Defendants argue the first interpretation stems naturally from the construction of the sentence, but the second interpretation is also plausible because a determination of the original source is likely necessary to determine which template should be used for evaluation of the authenticity risk rating. *Id.* Accordingly, defendants argue the term is indefinite. *Id.*

Plaintiff rejects defendants' interpretation and instead argues the source is a reference to the type of prospective entrant presenting the credential. Pl.'s Resp. Cl. Constr. Br. At 18. Plaintiff contends "automatically determin[ing] the source" is an extension of the process described in claim term 1, where the type of entry is determined. *Id.* At 18–19 (citing '844 patent col. 5 ll. 12–13). In support, plaintiff argues "automatically determin[ing] the source" is a necessary step because different types of entrants utilize different credentials, and the central processing unit must analyze each credential. *Id.* (citing '844 patent col. 5 ll. 27–31) ("automatically determines the source [or type of entrant] of the credential data record and automatically extracts personal information to be checked against a security list, TSA NO-FLY list, SELECTEE list, other alternative credentials [because based on the type of entrant the list to compare would vary.]"). Therefore, the system must determine the type of entrant presenting the credential. *Id.* Accordingly, plaintiff argues the term should be given its plain meaning. *Id.*

B. Analysis

1. The Court's Preliminary Construction

Before the *Markman* hearing, the Court provided the parties with the Court's preliminary construction after considering both parties' claim construction briefs and all referenced materials in full. Tr. At 8:15–19. The Court first determined whether "source" must refer to the "type of entrant," as plaintiff argues.[9] *See* Pl.'s Resp. Cl. Constr. Br. At 18. Reading the specification, "type of entry," however, has multiple potential meanings as argued by defendants including: (1) the physical location of the credential, *see* '844 patent col. 5 ll. 12-13 ("[A]dmission is processed as entry or re-entry of the individuals . . . ."); and (2) the issuing authority of the credential, *see id.* ("[E]mployee records are checked to determine if the individual is an employee; the type of entry, visitor, employee, contractor, supplier, or vendor, is determined . . . ."). *See also* Defs.' Cl. Constr. Br. At 24. Replacing either meaning of "type of entrant" with the plain meaning of "source" indicates plaintiff's interchangeability argument is inapplicable. The patentee further did not consistently interchange "type of entry" and "source" in the specification. *See id.*; *see also Baran v. Med. Device Techs., Inc.*, 616 F.3d 1309, 1316 (Fed. Cir. 2010). Additionally, the ordinary meaning of "source" does not naturally lend itself to be understood as "type of entrant." *See Source*, Webster's Third New International Dictionary, (2002) ("A point of origin or procurement"). As such, the Court preliminarily construed "source" and "type of entry" to have different meanings. *MicroStrategy Inc. v. Bus. Objects Americas*, 238 F. App'x 605, 609 (Fed. Cir. 2007); *see Merck & Co. v. Teva Pharm. USA, Inc.*, 395 F.3d 1364, 1372 (Fed. Cir. 2005).

When construing the term, the Court looked "to the words of the claims themselves, both asserted and nonasserted, to define the scope of the patented invention"; however, equating "source" to "type of entry" is not supported by asserted and nonasserted aspects of the specification. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (citing *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)). Although a patent need not answer every conceivable question to be found definite, the '844 patent specification does not define "automatically determines the source," even when read within the context of the claims. *See Presidio Components, Inc. v. Am. Tech. Ceramics Corp.*, 875 F.3d 1369, 1377 (Fed. Cir. 2017); *Baran*, 616 F.3d at 1316. Without a clear definition for "source" in the specification, a skilled artisan could not know the scope of the claimed invention with reasonable certainty. *See Presidio*, 875 F.3d at 1375 (citing *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 910 (2014)).

Noting this term may be indefinite, the Court provided the parties with three potential preliminary constructions for "automatically determines the source": (1) "the process by which the system understands the physical location from which the credential data record originated"; (2) "the process by which the system understands the type of entry of the credential (employee, visitor, etc.)"; or (3) "the process by which the system determines the issuing authority of the credential."

2. The Court's Final Construction

[9] In briefing, plaintiff uses "type of entry" to describe the "type of entrant." *See* Pl.'s Resp. Cl. Constr. Br. at 18 (arguing "source" means "type of entry" or entrant, i.e., visitor, employee, contractor, supplier or vendor).

At the *Markman* hearing, defendants maintained "automatically determines the source" was indefinite because the term is prone to multiple constructions, and a skilled artisan would not know the scope of the term with reasonable certainty. *See* Tr. At 117:24–118:1 (defendants arguing "we have multiple intrinsic references all supplying multiple potential interpretations . . . ."). Plaintiff admitted the term "source" was not defined in the specification and stated, "[I]t could be a lot of different things." Tr. At 109:12–14 ("[PLAINTIFF]: [I]t's our view that a source check . . . there's no definition of it. It could be a lot of different things."). Plaintiff agreed the specification does not provide any detail as to the meaning of the term "source." Tr. At 112:19–22. ("THE COURT: And you agree that the specification does not provide any detail of what source is? [PLAINTIFF]: That's correct."). When asked how the patent informs the PHOSITA with reasonable certainty as to what "source" is "automatically determined," plaintiff stated "source" "reasonably" could refer to the type of person presenting the credential ("visitor versus employee") or "reasonably does incorporate another sense of the word [depending on] where it is." *See* Tr. At 115:20–116:14. Defendants agreed, citing supporting intrinsic evidence for all the possible different meanings of "source." Tr. At 117:3–118:11 ("[DEFENDANTS]: . . . It's not enough for us to come up with an interpretation. We've come up with four or five. We have to know, with reasonable certainty, which one it is, and we just don't know here. There's nothing to discern that from and so it can't be valid. . . . [T]he word 'source' doesn't even appear in the specification.").

As plaintiff concedes, "source" means "a lot of different things," Tr. At 109:12–14, and therefore does not inform "those skilled in the art about the scope of the claimed invention with reasonable certainty." *Sonix Tech. Co. v. Publ'ns Int'l, Ltd.*, 844 F.3d 1370, 1377 (Fed. Cir. 2017) (citing *Nautilus*, 572 U.S. at 901). As such, "automatically determines the source" fails § 112, ¶ 2 and renders the term indefinite. *Nautilus*, 572 U.S. at 901.

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning, and as an example, the type of entry, visitor, employee, contractor, supplier, or vendor."	"Indefinite" or "Using common storage to verify that a submitted unique identifier has not already been assigned to another physical device."
Court's Construction	
Indefinite.	

XIV. Disputed Claim Term #12: "credential data record"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning." Pl.'s Resp. Cl. Constr. Br. At 19.	"Indefinite." Defs.' Cl. Constr. Br. At 25.

The disputed term is used in claim 1:

> wherein, upon a credential reading, the automated access control system automatically determines the source of the *credential data record*, and

> automatically extracts personal information to be checked against a security list, TSA NO-FLY list, SELECTEE list, other alternative credentials; whereas upon the credential authentication, the automated access control system automatically extracts authentication information from the authentication data record, and subsequently displays a warning window, as a result of the individual credentials match and ID forgery risks rating contained in the authentication data record.

'844 patent col. 5 ll. 26–37.

A. Parties' Arguments

Defendants argue "credential data record" is ambiguous because claim 1 contains no antecedent basis for the term. Defs.' Cl. Constr. Br. At 25. According to defendants, the claim identifies multiple types of records, including real time records generated from the ID reader, authentication data records generated by the ID authenticator, and entry records when vehicles are admitted. *Id.* (citing '844 patent col. 5 ll. 1–24). Defendants argue the "credential data record" could be a combination of any of the records. *Id.* Given the patent identifies multiple types of records but does not specify type here, defendants contend the claim is indefinite. *Id.*

Plaintiff argues "credential data record" encompasses all entrant data derived from presented credentials, as recorded by the access system as a whole, including both the real time data generated by the credential reader and authentication data records generated by the ID authenticator. Pl.'s Resp. Cl. Constr. Br. At 19–20. Plaintiff argues a term encompassing both types of system data is required because some types of identification do not receive an authentication rating, but all data records are subject to evaluation against a relevant list. *Id.* At 20. Plaintiff therefore argues "credential data record" encompasses all data extracted during the process of admitting an entrant and is not indefinite. *Id.* At 20–21. Plaintiff asserts the term should be given its plain and ordinary meaning. *Id.* At 19.

B. Analysis

1. The Court's Preliminary Construction

Before the *Markman* hearing, the Court provided the parties with the Court's preliminary construction after considering both parties' claim construction briefs and all referenced materials in full. Tr. At 8:15–19. The Court first addressed whether the term clearly marks the bounds of the claim. When a claim term has no express antecedent basis, the claim term is indefinite unless the context of the claim provides information to sufficiently clarify the boundary of the claim. *See Energizer Holdings, Inc. v. Int'l Trade Comm'n*, 435 F.3d 1366, 1370 (Fed. Cir. 2006). To avoid indefiniteness, a "person of ordinary skill in the art [should be able] to read ['credential data record'] . . . in the context of the entire patent" and ascertain the clear boundaries of the claim. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005); *see Energizer Holdings*, 435 F.3d at 1370–71. The term "credential data record" appears for the first and only time in the '844 patent on column 5, line 28. When read within the local context of the claim, "credential data record" has at least two possible meanings: (1) "authentication data record"; and (2) "the

real time record" generated by reading the credential. *See* '844 patent col. 5 ll. 21–37. When viewed within the context of the entire patent, however, "credential data record" must be a new, third record comprising both the "real time record" and the "authentication data record." *Id.* The term "credential data record" is therefore prone to multiple interpretations within the context of the patent, so "the bounds of the invention are [not] sufficiently demarcated." *ePlus, Inc. v. Lawson Software, Inc.*, 700 F.3d 509, 517 (Fed. Cir. 2012). The term is boundless, and "a skilled artisan [could not] know the scope of the claimed invention with reasonable certainty." *Sonix Tech. Co. v. Publ'ns Int'l, Ltd.*, 844 F.3d 1370, 1377 (Fed. Cir. 2017) (citing *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014)). As a skilled artisan cannot "know the scope of the claimed invention with reasonable certainty[,]" "credential data record" fails under § 112, ¶ 2 and is indefinite. *Nautilus*, 572 U.S. at 901. Preliminarily noting this term may be indefinite, the Court offered the parties the following alternative construction in addition to those the parties already presented: "a record comprising of the individual real-time record and the authentication data record."

2. The Court's Final Construction

At the *Markman* hearing, plaintiff faltered from the arguments made in its brief—"credential data record" encompasses all entrant data derived from presented credentials, as recorded by the access system as a whole. Pl.'s Resp. Cl. Constr. Br. at 19–20. Plaintiff argued "credential data record" only includes the real time record. Tr. at 120:11–14. ("[PLAINTIFF]: . . . So ['credential data record'] looks like it really actually should be just the real time record . . . ."). Plaintiff then changed course and agreed the term could be construed to include both real time data record and authentication data record when asked why the Court's alternative construction of "a record comprising of the individual real-time record and the authentication data record" was incorrect. Tr. at 121:13–15 ("THE COURT: So explain to me why it's not both. [PLAINTIFF]: Well, because I think . . . it certainly could be both, and I think that was why I originally wrote that . . . ."). Plaintiff also conceded neither the '732 nor the '844 patent described "credential data record." Tr. at 123:22–25 ("THE COURT: [D]oes either the '844 patent or the '732 patent describe and use the language 'credential data record" anywhere? [PLAINTIFF]: I don't believe so."). Plaintiff agreed the plain meaning of "credential data record" favored the Court's alternative construction. Tr. at 123:16–21. ("THE COURT: . . . [W]hat is the plain meaning of 'credential data record'? [PLAINTIFF]: Well, it is more encompassing, and I think that pushes in favor of [the preliminary construction]."). Plaintiff further argued the antecedent basis for the term was "the authentication device and the standardized credential reader . . . are the only sources of data that are present," which in turn supported the Court's alternative construction. Tr. at 124:1–21. At the same time, plaintiff stated "credential data record" "probably is just real time records," but because "it's a different term, it should be given a different meaning . . . [so], overall, I think it actually encompasses both." Tr. at 123:9–125:5. By changing positions between two separate constructions, and deviating from the construction in plaintiff's own briefs, plaintiff demonstrated the term is prone to multiple constructions. *See, e.g.*, Tr. at 120:7–125:14. The multiple constructions show "the bounds of the invention are [not] sufficiently demarcated." *ePlus, Inc.*, 700 F.3d at 517. The claim term lacks clear antecedent basis and does not "inform those skilled in the art about the scope of the claimed invention with reasonable certainty." *Sonix Tech. Co.*, 844 F.3d at 1377 (citing *Nautilus*, 572 U.S. at 901); *Energizer Holdings*, 435 F.3d at 1370–71. The term fails

under § 112, ¶ 2 and is indefinite. *Nautilus*, 572 U.S. at 901; *Energizer Holdings*, 435 F.3d at 1370–71.

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning."	"Indefinite."
Court's Construction	
Indefinite.	

XV. Disputed Claim Term #13: "to be checked against a security list, TSA NO-FLY list, SELECTEE list, other alternative credentials"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning. All airports maintain a security list, the TSA maintains a NO-FLY list, as well as a SELECTEE list." Pl.'s Resp. Cl. Constr. Br. at 21.	"Indefinite." Defs.' Cl. Constr. Br. at 26.

The disputed term is used in claim 1:

> wherein, upon a credential reading, the automated access control system automatically determines the source of the credential data record, and automatically extracts personal information *to be checked against a security list, TSA NO-FLY list, SELECTEE list, other alternative credentials*; whereas upon the credential authentication, the automated access control system automatically extracts authentication information from the authentication data record, and subsequently displays a warning window, as a result of the individual credentials match and ID forgery risks rating contained in the authentication data record.

'844 patent col. 5 ll. 26–37.

A. Parties' Arguments

The parties primarily dispute the meaning of "other alternative credentials." According to defendants, "other alternative credentials" appears at the end of a list and could reasonably be read in light of the characteristics of the other listed elements. Defs.' Cl. Constr. Br. at 26. Reading the term alongside the "security list, TSA NO-FLY list, SELECTEE list," defendants suggest "alternative credentials" refers to a type of list. *Id.* Defendants alternatively assert, using the '732 patent, the term could refer to an alternative backup form of ID for employees unable to present their main credential. *Id.* at 26–27. Defendants argue the term is indefinite because the claim term has two plausible readings. *Id.* Defendants further argue if the term is construed to mean an alternative employee ID, the claim term does not adequately describe what type of comparison the system would make between: (1) the personal information extracted from the presented credential; and (2) the personal information extracted from the alternative credential. *Id.* Accordingly, defendants assert the term is indefinite. *Id.* at 26.

Plaintiff argues if a separate alternative credentials "list" was contemplated, as suggested by defendants, the claim would have expressly described the list as an "alternative credentials list." Pl.'s Resp. Cl. Constr. Br. at 21. The lack of the word "list," according to plaintiff, suggests "alternative credentials" should be construed without consistency with the characteristics of the other elements in the list. *Id.* Plaintiff contends "to be checked against" should receive its ordinary meaning, contemplating a process where the system compares personal data from the presented credential to various lists maintained by the facility or to an alternative credential. *Id.* at 21–22.

B. Analysis

1. The Court's Preliminary Construction

Before the *Markman* hearing, the Court provided the parties with the Court's preliminary construction after considering both parties' claim construction briefs and all referenced materials in full. Tr. at 8:15–19. The Court first looked to determine if the '844 defines alternative credential. The '844 patent does not reference or provide an independent definition of "alternative credentials." *See* '844 patent. The '732 patent, on the other hand, describes "an alternative credential" in dependent claim 3 as a credential used when an employee's main credential is unavailable. '732 patent col. 10 l. 36, col 11 l. 20, col. 14 l. 54. In the context of airport security, the '732 patent's definition coincides with the term's plain meaning. *See Alternative*, Oxford Dictionary of English, (3d ed. 2010) ("available as another possibility or choice"). "When a parent application includes statements involving 'common subject matter' with the terms at issue, those statements are relevant to construction of the terms in the child patent." *E.I. du Pont De Nemours & Co. v. Unifrax I LLC*, 921 F.3d 1060, 1070 (Fed. Cir. 2019). The '732 parent patent includes a definition of "an alternative credential" consistent with the term's plain meaning in context, so the '732 patent is relevant to construing the term within the '844 patent. Accordingly, the Court preliminarily construed this term indefinite or plain meaning for the enumerated lists, with "alternative credentials" as defined in dependent claim 3 of the '732 patent.[10]

2. The Court's Final Construction

At the *Markman* hearing, defendants agreed the '282 application (the predecessor to the '732 patent) is part of the intrinsic record and therefore resolved any indefinite issues for the disputed term. Tr. at 128:24–25, 129:1 ("THE COURT: And you would agree that ['282 application, now '732 patent is] in the intrinsic record? [DEFENDANTS]: Yes . . . ."). Defendants also agreed the definition of "alternative credentials" from the '732 patent can be used in construing the term in the current claim at issue. Tr. at 136:1–7 ("THE COURT: You got to agree that the parent patent does seem to go into some discussions about alternative credential. So there's explanation there in the spec[ification]. [DEFENDANTS]: . . . [G]iven that this is in the intrinsic record, I think the Court has a basis for [the preliminary] construction

[10] The Court preliminarily construed the term as indefinite based on the differences between the '282 application and '732 issued patent; however, these discrepancies were resolved during the *Markman* hearing.

under *Phillips*.”). For clarity, defendants requested the Court remove reference to the parent patent and define “alternative credential” within the construction itself as “a credential used when the employee loses or misplaces a regular company credential.” Tr. at 131:10–19. Plaintiff agreed to the modification. Tr. at 132:15–17. Accordingly, as agreed by the parties, the Court adopts as final the construction: “Plain meaning as to the enumerated lists, with ‘alternative credentials’ meaning a credential used when an employee loses or misplaces a regular credential.”

Plaintiff’s Proposed Construction	**Defendants’ Proposed Construction**
“Plain meaning. All airports maintain a security list, the TSA maintains a NO-FLY list, as well as a SELECTEE list.”	“Indefinite.”
Court’s Construction	
“Plain meaning as to the enumerated lists, with ‘alternative credentials’ meaning a credential used when an employee loses or misplaces a regular credential.”	

XVI. Disputed Claim Term #14: “warning window[, as a result of the individual credentials match and ID forgery risks rating contained in the authentication data record]”

Plaintiff’s Proposed Construction	**Defendants’ Proposed Construction**
“Plain meaning. All airports maintain a security list, the TSA maintains a NO-FLY list, as well as a SELECTEE list.” Pl.’s Resp. Cl. Constr. Br. at 22.	“Indefinite. To the extent the term is construed, Defendants propose: An alert to the system operator, notifying the system operator that the individual should be denied access without human intervention, based on the credential data record generated using information from the standardized credential means and the authentication data record generated using information from the ID authenticator.” Defs.’ Cl. Constr. Br. at 27.

This disputed term is used in claim 1:

> wherein, upon a credential reading, the automated access control system automatically determines the source of the credential data record, and automatically extracts personal information to be checked against a security list, TSA NO-FLY list, SELECTEE list, other alternative credentials; whereas upon the credential authentication, the automated access control system automatically extracts authentication information from the authentication data record, and subsequently displays a *warning*

window, as a result of the individual credentials match and ID forgery risks rating contained in the authentication data record.

'844 patent col. 5 ll. 26–37.

A. Parties' Arguments

Defendants contend the term is indefinite because the patent does not describe the information displayed upon appearance of the warning window or the additional actions the system takes once the warning window is triggered. Defs.' Cl. Constr. Br. at 27–28. Defendants point to the '844 patent specification describing a potential embodiment where the warning window requires a security manager to enter a predefined security code in order to override the warning. *Id.* (citing '844 patent col. 3 ll. 37–53). Defendants assert the language of claim 1 does not describe the content of the warning window or the potential actions taken by the security system to prevent unauthorized access prior to intervention by the security manager. *Id.* at 28. According to defendants, the '844 patent's lack of detail renders the claim indefinite. *Id.* Alternatively, if the claim is not indefinite, defendants argue the term must be construed to clarify the relationship with the system operator when the warning window is triggered. *Id.*

Plaintiff argues "warning window" has a plain and ordinary meaning in the field. Pl.'s Resp. Cl. Constr. Br. at 22–23. Plaintiff further argues defendants are inappropriately reading limitations from an illustrative embodiment into the construction of the claim term. *Id.* at 23.

B. Analysis

1. The Court's Preliminary Construction

Before the *Markman* hearing, the Court provided the parties with the Court's preliminary construction after considering both parties' claim construction briefs and all referenced materials in full. Tr. at 8:15–19. The Court first determined whether an embodiment should limit the claim. The '844 patent provides an illustration of the system operating as a vehicle gate entry system. '844 patent col. 3 ll. 31–64. The embodiment explains when a "warning window" is displayed, intervention and a security code from a manager are required. *Id.* Such an illustrative embodiment, however, should not limit this term's construction. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (the Federal Circuit "has repeatedly warned against confining the claims to [very specific] embodiments"). As such, the Court did not preliminarily adopt a requirement where a security manager must intervene with a security access code because claim 1 does not expressly state the limitation. Furthermore, the patentee did not adopt an independent definition, act as his own lexicographer, or disavow any claim scope. *See* '844 patent; '282 application; *Phillips*, 415 F.3d at 1312–13 (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)); *Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (citing *Vitronics*, 90 F.3d at 1580). The Court therefore preliminarily adopted a plain and ordinary meaning. *See Phillips*, 415 F.3d at 1312–13. Insofar as a definition is helpful, the Court preliminarily offered: "any of various rectangular boxes appearing on a computer screen that display files or program output to call something to an operator's attention." *Warn*, Webster's Third New International Dictionary (2002) ("to notify or apprise

esp[ecially] in advance: call to one's attention: make aware: INFORM"); *Window*, Merriam-Webster's Dictionary, https://www.merriam-webster.com/dictionary/window (last visited Jan. 10, 2023) ("any of various rectangular boxes appearing on a computer screen that display files or program output, that can usually be moved and resized, and that facilitate multitasking").

2. The Court's Final Construction

At the *Markman* hearing, defendants argued the term is indefinite because the specification fails to detail a test for when the warning window would be displayed. Tr. at 137:11–23. Defendants also questioned if "the warning window [is] triggered to display or [if the warning window] is . . . always displayed to show the operator information." Tr. at 139:21–23. Applying broader patent policy arguments, defendants stated, because "[t]here's zero information about when this warning window appears, . . . if it always has to appear, [or] what that rating looks like," designing around the patent is more difficult. *See* Tr. at 146:6–12. Defendants' argument, however, focuses on enablement rather than indefiniteness. *See Enzo Life Sciences, Inc. v. Roche Molecular Sys., Inc.*, 928 F.3d 1340, 1345 (Fed. Cir. 2019) ("The enablement requirement asks whether 'the specification teach[es] those in the art to make and use the invention without undue experimentation.'"). The legal standards of enablement and indefiniteness are distinct despite a conceptual overlap between both statutory requirements, and defendants improperly conflate enablement and indefiniteness. *See, e.g.*, *Augme Techs., Inc. v. Yahoo! Inc.*, 755 F.3d 1326, 1340 (Fed. Cir. 2014) ("Appellants' arguments appear to be based on the wrong legal standard, i.e., written description or enablement as opposed to indefiniteness."); *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1358 n.2 (Fed. Cir. 1999) ("[D]efiniteness and enablement are analytically distinct requirements [of validity], even though both concepts are contained in 35 U.S.C. § 112."). The Federal Circuit has held validity arguments, such as lack of enablement and lack of written description, are not relevant during claim construction; therefore, the Court will not address an enablement argument here. *See Philips*, 415 F.3d at 1327 ("[W]e have certainly not endorsed a regime in which validity analysis is a regular component of claim construction."). Defendants alternatively agreed with the Court's construction of this term. Tr. at 139:10–20. Accordingly, the Court adopts its preliminary construction as final: "Plain meaning, 'any of various rectangular boxes appearing on a computer screen that display files or program output to call something to an operator's attention.'"

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning. All airports maintain a security list, the TSA maintains a NO-FLY list, as well as a SELECTEE list."	"Indefinite. To the extent the term is construed, Defendants propose: An alert to the system operator, notifying the system operator that the individual should be denied access without human intervention, based on the credential data record generated using information from the standardized credential means and the authentication data

	record generated using information from the ID authenticator."
Court's Construction	
Plain meaning: "any of various rectangular boxes appearing on a computer screen that display files or program output to call something to an operator's attention."	

XVII. Disputed Claim Term #15: "individual credentials match"

Plaintiff's Proposed Construction	Defendants' Proposed Construction
"Plain meaning. As an illustration, checks can be made against TSA lists, employee lists if employee, or traveler lists, if traveler." Pl.'s Resp. Cl. Constr. Br. at 24.	"Indefinite." Defs.' Cl. Constr. Br. at 28.

The disputed term is used in claim 1:

> wherein, upon a credential reading, the automated access control system automatically determines the source of the credential data record, and automatically extracts personal information to be checked against a security list, TSA NO-FLY list, SELECTEE list, other alternative credentials; whereas upon the credential authentication, the automated access control system automatically extracts authentication information from the authentication data record, and subsequently displays a warning window, as a result of the *individual credentials match* and ID forgery risks rating contained in the authentication data record.

'844 patent col. 5 ll. 26–37.

A. Parties' Arguments

Defendants argue the term is indefinite because the patent does not describe whether the system checks against various predetermined databases or against previously collected ID information to detect a match. Defs.' Cl. Constr. Br. at 28–29. Defendants further argue if the system checks against predetermined databases, the patent does not specify which databases are contemplated as the patent describes a non-exhaustive list of potential databases. *Id.* at 29.

Plaintiff argues the term is intended as a catch-all and should describe a match against any list utilized by the system and is not indefinite. Pl.'s Resp. Cl. Constr. Br. at 24. Plaintiff asserts the term should be given its plain and ordinary meaning. *Id.*

B. Analysis

1. The Court's Preliminary Construction

Before the *Markman* hearing, the Court provided the parties with the Court's preliminary construction after considering both parties' claim construction briefs and all referenced materials in full. *See* Tr. at 8:15–19. In multiple instances, the '844 patent describes a system comparing personal information against different types of predefined lists. *See* '844 patent col. 1 l. 66 (terrorists lists), col. 3 l. 13 (NO-FLY and SELECTEE lists), col. 3 l. 46 (NO-FLY and SELECTEE lists), col. 5 ll. 29–30 (security list, TSA NO-FLY and SELECTEE list). A PHOSITA would therefore read the term against a backdrop of these references and understand "individual credentials match" to refer to predefined lists similar to those illustrated in the patent. As for "match," neither of the *Thorner* exceptions are met, and therefore, the Court preliminarily construed based on ordinary meaning. *See* '844 patent; '282 application; *Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (citing *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1580 (Fed. Cir. 1996)). Based on the lists described by the '844 patent and the ordinary meaning of "match," the Court provided the following preliminary construction: "The result when the extracted personal information is equal or similar to an entry in a security list, TSA NO-FLY list, SELECTEE list, or other alternative credentials."

2. The Court's Final Construction

At the *Markman* hearing, defendants generally agreed to the Court's construction but wanted "further clarity . . . where the extraction of personal information comes from." Tr. at 149:18–24. Plaintiff stated the information comes from the authentication data record. Tr. at 151:5. Both parties then agreed with the Court's construction of the term with the added clarification. *See* Tr. at 151:12–21. Accordingly, the Court adopts the following final construction: "The result when the extracted personal information from the authentication data record is equal or similar to an entry in a security list, TSA NO-FLY list, SELECTEE list, or other alternative credentials."

Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
"Plain meaning. As an illustration, checks can be made against TSA lists, employee lists if employee, or traveler lists, if traveler."	"Indefinite."
Court's Construction	
"The result when the extracted personal information from the authentication data record is equal or similar to an entry in a security list, TSA NO-FLY list, SELECTEE list, or other alternative credentials."	

XXIII. Conclusion

The disputed terms are interpreted by the Court in this Claim Construction Opinion and Order. The Court accordingly adopts the constructions of the disputed terms as set forth herein.

Term #	**Disputed Term**	**The Court's Construction**
1	"standardized credential reader means"	Indefinite.

2	"credential encoded with personal identification"	Plain meaning: "a driver's license, passport, boarding pass, airport ID, or other standardized documents containing information relating to a particular individual converted from one system of communication into another."
3	"build individual real time records"	"The credential reader immediately generates a digital record after decoding information from the credential and encrypting sensitive personal information. The digital record is then stored within the system for access by a user at any time."
4	"credential collected information match"	Plain meaning: "when the data collected from a currently presented credential is equal or similar to an existing record."
5	"system database"	Plain meaning: "a collection of data organized for retrieval by a computer, and accessible by an automated access control system."
6	"the type of entry, visitor, employee, contractor, supplier, or vendor, is determined"	"Using the individual real time record built from the presented personal identification credentials, the software application checks the system database stored information to ascertain whether the individual presenting the credential is one of the following: visitor, employee, contractor, supplier, or vendor."
7	"an ID authenticator"	"A commercial identification card authentication device, separate from the standardized credential reader device."
8	"means to read non-encoded credentials"	"An apparatus capable of image acquisition and taking sense of letters and symbols."
9	"authentication data record"	"A record, separate from any individual real time record, containing both an authentication rating and a digital image of the credential."
10	"authenticity risk rating" / "authentication rating" / "ID forgery risks rating"	"A grade of an ID's security risks provided by the ID authenticator by analyzing physical aspects and embedded security features to determine the possibility of any tampering or forgery by matching with stored templates."
11	"automatically determines the source"	Indefinite.
12	"credential data record"	Indefinite.
13	"to be checked against a security list, TSA NO-FLY list, SELECTEE list, other alternative credentials"	Plain meaning as to the enumerated lists, with "alternative credentials" meaning a credential used when an employee loses or misplaces a regular credential.
14	"warning window[, as a result of the individual credentials match and	Plain meaning: "any of various rectangular boxes appearing on a computer screen that

	ID forgery risks rating contained in the authentication data record]"	display files or program output to call something to an operator's attention."
15	"individual credentials match"	"The result when the extracted personal information from the authentication data record is equal or similar to an entry in a security list, TSA NO-FLY list, SELECTEE list, or other alternative credentials."

The Court began this claim construction analysis with a presumption "patents are presumed to be valid" and the USPTO "only grants those patent applications that meet the statutory patentability requirement[s]." *See supra* Section I.A. Defendants have proven their case and overcome the presumption of validity with clear and convincing evidence regarding three disputed terms. As discussed *supra* Sections III, XIII, and XIV, claim terms 1, 11, and 12 are indefinite under 35 U.S.C. § 112 and as a result independent claim 1 is rendered invalid. As the only independent claim in the '844 patent, the entire '844 patent is invalid under § 112. *See Horizon Pharma, Inc. v. Dr. Reddy's Labs., Inc.*, No. CV 15-3324 (SRC), 2018 WL 6040265, at *9 (D.N.J. Nov. 19, 2018) (finding the patents-in-suit invalid after finding the sole independent claims invalid for indefiniteness), *aff'd*, 839 F. App'x 500 (Fed. Cir. 2021); *see also Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 902 ("A lack of definiteness renders invalid 'the patent or any claim in suit.'") (quoting 35 U.S.C. § 282, ¶ 2(3)). Although three terms were found indefinite, rendering the entire '844 patent invalid, the Court construed all disputed terms the parties raised. *See O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1360 (Fed. Cir. 2008) ("When the parties raise an actual dispute regarding the proper scope of these claims, the court . . . must resolve that dispute.").

The '844 patent—the only patent asserted as infringed—is now invalid. Plaintiff no longer presents a valid patent viable for patent infringement adjudication in this Court. Rule 12(h)(3) of the Rules of the Court of Federal Claims ("RCFC") provides "[i]f the court determines at any time that it lacks subject matter jurisdiction, the court must dismiss the action." The Court therefore **ORDERS** plaintiff to **SHOW CAUSE** as to why this case should not be dismissed pursuant to RCFC 12(h)(3) **on or before 20 February 2023**. In responding to this order, plaintiff must identify which source or sources of law he is invoking and explain why this Court has jurisdiction over this case. Defendants **SHALL FILE** a response **on or before 6 March 2023.**

IT IS SO ORDERED.

s/ Ryan T. Holte
RYAN T. HOLTE
Judge