In the United States Court of Federal Claims

No. 10-769C
(Filed: July 18, 2014)

****

SPA SYSPATRONIC AG,

Plaintiff,

v.

THE UNITED STATES,

Defendant,

and

GEMALTO, INC.

Third-Party Defendant.

****

Patents; Means-plus-function limitations; 35 U.S.C. § 112; Indefiniteness.

Charles P. Kennedy, Washington, DC, for plaintiff.

David M. Ruddy, United States Department of Justice, Civil Division, Commercial Litigation Branch, Washington, DC, with whom were *Stuart F. Delery*, Assistant Attorney General, and *John Fargo*, Director, for defendant.

Brian A. Rosenthal, Washington, DC, for third-party defendant.

OPINION

BRUGGINK, JUDGE.

This is a patent infringement action brought pursuant to 28 U.S.C. § 1498(a) (2012) against the United States for unlicensed use of plaintiff's patent. A third party, Gemalto, Inc., responded to our rule 14(b)(3) notice to third parties, and joined the case as a third-party defendant. Defendants moved for summary judgment, contending that certain claims of the patent are indefinite and thus invalid under 35 U.S.C. § 112. Oral argument was held on

January 14, 2014, and again after supplemental briefing on May 5, 2014. The motion is fully briefed. For the foregoing reasons, defendants' motion is granted in part and denied in part.

BACKGROUND

United States Patent No. 4,985,921 ("'921 Patent") is held by plaintiff, SPA Syspatronic AG, a Swiss company. The patent concerns a "portable carrying device containing a control unit and an additional data memory . . . as an integrated circuit." DX 1 at A3 (the '921 Patent).[1] The main application of these devices was intended to be credit cards and other small data-carrying cards. *Id.* The main feature of the device is the protection of the data stored on the device from unauthorized access. This is achieved primarily through the utilization of multiple microchips communicating with one another using codes or encryption "without participation of system parts external to the carrying device." *Id.* at A4 (claim 1).

Following proceedings before the European Patent Office concerning the corresponding European patent, plaintiff sought reexamination of claim 1 of the '921 patent by the United States Patent and Trademark Office ("PTO"). The result of that process was the cancellation of claim 1 and the addition of claims 8-13.[2] *See id.* at A5-A7 (Ex Parte Reexamation Certificate, Oct. 8, 2008). Plaintiff instituted this action against the United States in November of 2010. Plaintiff alleges infringement of claims 2, 3, 4, 7, 8, 9, 10, and 13 by the United States.

As a result of the first patent reexamination and the cancellation of claim 1, claim 8 is the only independent claim. It teaches:

> A portable data carrying device comprising a control unit and an additional data memory which are each implemented as integrated circuits, wherein the control unit is provided with

---

[1] The parties attached exhibits in support of their positions for or against defendants' motion for summary judgment. "DX" refers to "defendants' exhibit." "PX" refers to "plaintiff's exhibit."

[2] Gemalto requested a second *ex parte* reexamination of the '921 Patent. This second reexamination did not result in any changes. *See id.* at A8-A9 (Ex Parte Reexamation Certificate, Nov. 20, 2012).

> means for placing it in communication with an external read/write device characterized in that entry into the additional data memory (5) by the control unit (2) is protected by coding means which is in the carrying device and is operative to permit entry into the additional data memory (5) without participation of system parts external to the carrying device, and wherein the control unit and the additional data memory are operative to exchange information in encrypted form.

Id. at A7.

Claim 2 adds that the data memory "contains an access code region and the code means includes means within the control unit (2) for producing a code signal (C) for entry to the data memory through the access code region." *Id.* at A4 (claim 2). Claim 3 adds that "code means" "includes a processor (8) associated with the data memory (5) for a secure (coded or decoded) data exchange with the control unit (2*a*)." *Id.* (claim 3). Claim 4 further explains that the "code means includes means within the control unit (2*b*) for producing a secret microcode for communications between the control unit and the data memory." *Id.* (claim 4). Claims 5 and 6 are not at issue in this suit. Claim 7 limits the device to having the control unit, data memory, and other parts of the microchips "in a totally integrated circuit construction on the same carrier." *Id.* (claim 7). Claim 8 is the new independent claim quoted above. Claim 9 is largely duplicative of claim 2 but refers to claim 8 rather than the cancelled claim 1. Claim 10 is likewise similar to claim 4. Claims 11 and 12 are not at issue. Claim 13 is a slightly reworded version of claim 7: "the control unit, the additional data memory and further regions are implemented collectively in an integrated circuit construction on a single carrier." *Id.* at A7 (claim 13).

Paragraph 2 of section 112 of title 35 requires generally that patent specifications "conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention." 35 U.S.C. § 112 ¶ 2 (2006).[3] This is the "definiteness"

---

[3] 35 U.S.C. § 112 was amended in 2011,which changed the wording of paragraph two slightly. *See* Leahy-Smith America Invents Act, Pub. L. No. 112-29, § 4(c), 125 Stat. 284, 296 (Sept. 16, 2011). Those amendments did not take effect until after this action was filed and thus do not affect the patent in suit. We thus cite to the 2006 code containing the previous version of the statute.

requirement of patents. Paragraph 6 of the same code section allows for a special type of patent claiming known as "means-plus-function" claiming:

> An element in a claim for a combination may be expressed as a means . . . for performing a specified function without recital of structure . . . and such claim shall be construed to cover the corresponding structure . . . described in the specification and equivalents thereof.

Id. ¶ 6. "Means-plus-function" limitations disclose a function in the claim language, and the structure to achieve that function (or the "means") must be disclosed in the patent specifications. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1311 (Fed. Cir. 2005) (*en banc*). The '921 Patent employs several "means-plus-function" elements in its claims.

Defendants have identified three means-plus-function limitations as to which they assert that the '921 Patent's specifications fail to disclose any means. They are (1) "coding means which is in the carrying device and is operative to permit entry into the additional data memory . . . without participation of system parts external to the carrying device," which is found in independent claim 8; (2) "means within the control unit for producing a code signal for entry to the data memory through the access code region," which is found in dependent claims 2 and 9; and "means within the control unit for producing a secret microcode for communications between the control unit and the data memory," which appears in dependent claims 4 and 10. DX 1 at A4. Plaintiff does not dispute that these are means-plus-functions limitations.

There are four embodiments of the device contemplated by the patent as illustrated in Figures 1-4 of the patent's specifications. They appear below:

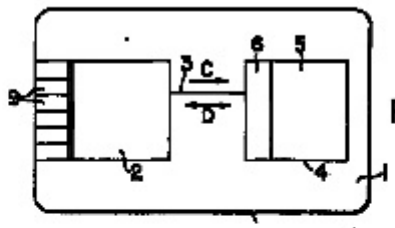

FIG. 1

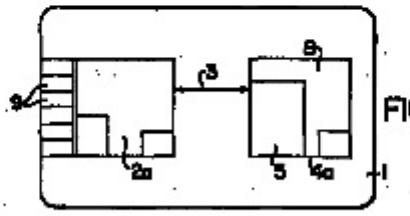

FIG. 2

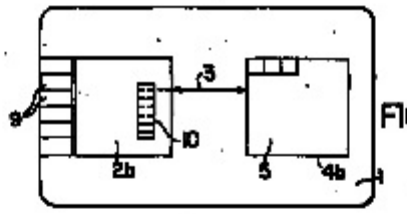

FIG. 3

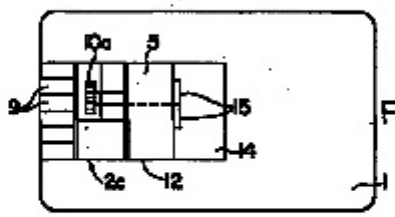

FIG. 4

Id. at A2.

The prose that follows in the patent specifications describe each of the embodiments and is comprised of a little over two columns of text. *See id.* at A3-A4 (column 2, line 23 through column 4, line 24). The first embodiment specifications read:

In FIG. 1 a plastic card is illustrated as a data carrying device in which two integrated semi-conductor - circuit components ("chips") 2 and 4 are set. The component 2 comprises the control unit of the data carrying device and is connected to an external contact 9 of the card 1 for the purpose of connecting to an external (not illustrated) read/write unit of the data exchange system. The connections for the external unit can also be produced in other manners than the galvanized contact, for example, by known means with an inductive coupling and so forth. The control unit 2 preferably comprises a microprocessor with a computer and RAM - and ROM storage areas as well as additionally a data memory region. An additional data memory 5 exists on the second component 4. The connection between the two components 2 and 4 is produced by means of a multiple conductor strip 3. For technical assembly reasons, it may be useful to combine the components 2 and 4 with the conductor strip 3 and if necessary the external contact 9 into a common module for the construction in the plastic card 1.

An external connection to the control unit 2 can only be made by means of the contact 9 so that an exchange of sensitive data between the card and the system in a known fashion can only come about after successful authentication and identification, which functions are participated in by the control unit. The data exchange is produced also however within the card between the components 2 and 4 by means of the conductor strip 3. In order to prevent manipulation and unauthorized access to the data memory 5, entry to this memory is protected by the control unit 2. For example according to FIG. 1, an access code region 6 is associated with the data memory 5 for this purpose. In this manner the memory is accessible only by means of a code signal C which is produced by the control unit 2, that is, data exchange D between the components 2 and 4 is only possible after successful decoding of the code region 6. Also, the data exchange within the component 2 between the control unit and a data memory existing there is produced in a similarly protected manner, although not further illustrated. Such protected data exchange processes are produced within the data carrying device 1 with a certain degree of self-sufficiency without participation of external system parts (naturally apart from the current supplied over the contacts 9). The access in

particular to the sensitive data in the data memory 5 is thereby protected by means of a barrier which can only be overcome by means of key codes (key lock) employed within the card. In this manner the security can substantially be enhanced so that in the microprocessor of the control unit 2 new access codes can always be generated, for example after each successful access to the additional data memory. . . . The implementation of the additional memory 5 is possible as a serial memory with comparative logic and with a minimum number of connecting conductors 3 between the components 2 and 4.

DX 1 at A3-A4.

The second embodiment of the device is explained in this way:

In the embodiment according to FIG. 2, the general construction of the data carrying card 1 with the integrated circuit components 2*a*, 4*a* interconnected by means of the conductor strip 3 is the same as in FIG. 1. The control unit 2*a* connected with the external contacts 9 similarly comprises a microprocessor and a data memory region. On the other hand, the component 4*a* contains besides the additional memory 5 likewise a microprocessor 8 Whereby still further possibilities with respect to applications and security are achieved. With the help of a microprocessor 8 it is possible not only to secure entry to the data memory 5 from the control unit 2 as in FIG. 1 and with it the unauthorized reading of data from the memory 5, but also beyond this to secure the entire data exchange over the conductors 3, that is, to accomplish this in coded or decoded form. However, the double-pass entry system is only possible after a successful cryptographic authentication from the opposite pas which again is only produced, "within the card", that is, without participation of external system parts.

Id. at A4.

The third embodiment of the device is described in this way:

The general construction in the example according to FIG. 3 with a control unit 2*b* and an additional data memory 4*b* in the form of separate integrated circuits corresponds again to

> the foregoing examples. A protected entry to the additional data memory 5 is realized in this embodiment again in another manner, namely in that the microcode of the control unit 2*b*, designated 10, is secret. Of course, a well known microprocessor can be employed in the control unit 2*b* and this microprocessor can be based upon an "uncommon" microcode 10 only known to the manufacturer and therefore secret. In this manner an unauthorized access to the data stored in the data carrier or correspondingly a decoding of the information exchanged over the conductors 3 is rendered impossible, even if there was success in getting through the multiple conductor strip 3.

Id.

The fourth embodiment differs in form from the other three in that the microchips in the card are all part of one assembly, a single circuit. It is described as containing "one individual semi-conductor component . . . on which the control unit . . . , the additional data memory . . . as well as further circuit regions are in total implemented in an integrated circuit configuration." *Id.* The specification continues:

> In a manner similar to the example according to FIG. 3, the microcode l0*a* in the microprocessor of the control unit 2*c* is secret so that entry to the additional data memory 5 is again protected ("mechanical" access on the conductors between the regions of the integrated circuit on one and the same carrier would naturally however be considerably more difficult than on the conductors 3 Which are laid within the plastic card 1 or correspondingly Within a module Which consists of the two separate components 2 and 4).
>
> With the computer in the microprocessor of the control unit 2*c* there exists further an additional computer 14 in combination With registers 15 which are likewise positioned on the carrier 12. As indicated the registers 15 are likewise coordinated With the secret microcodes l0*a* of the control unit 2c, that is, the signal exchange between the control unit 2*c* and the additional computer 14 is produced likewise on the basis of the secret codes. One such additional calculator 14 makes possible the execution of especially highly developed

> cryptographic methods within the portable data carrying device, that is, without requiring external calculating capacity and thereby particular data exchanges with external system parts. This means that the application of the secret microcodes l0*a* remains restricted to the integrated circuits of the single carrier 12 in the data carrying device whereby high level security against manipulation and unauthorized access is achieved.

Id.

The parties have exchanged competing proposed constructions of the claim terms cited above, but have not yet presented them to the court for resolution at a claim construction hearing. Instead, defendants moved for summary judgment, asking the court to hold that, as a matter of law, certain of the patent's means-plus-function claims are indefinite, making the patent invalid. The basis of the motion, as will be more fully explained below, is that the patent specifications lack sufficient structure corresponding to the functions claimed in those means-plus-function claims. Without that corresponding structure in the specifications, those claims are, according to defendants, indefinite.

DISCUSSION

Within the above quoted specifications must reside the structure that performs the functions listed in the means-plus-function limitations of the claims. The court must be able to "determine the claimed function" and "identify the corresponding structure in the written description of the patent that performs that function." *Applied Med. Res. Corp. v. U.S. Surgical Corp.*, 448 F.3d 1324, 1332 (Fed. Cir. 2006). As the Federal Circuit has explained,

> the structure disclosed in the specification is 'corresponding' structure only if the specification or prosecution history clearly links or associates that structure to the function recited in the claim. This duty to link or associate structure to function is the *quid pro quo* for the convenience of employing [means-plus-function claiming].

Saffran v. Johnson & Johnson, 712 F.3d 549, 562 (Fed. Cir. 2013) (quoting *B. Braun Med., Inc. v. Abbot Labs.*, 124 F.3d 1419, 1424 (Fed. Cir. 1997)). If that structure is missing or not sufficiently linked to the function, those claims invoking that function are indefinite. The Supreme Court recently explained

that patent claims must, "viewed in light of the specification and prosecution history, inform those skilled in the art about the scope of the invention with reasonable certainty." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).[4] This "mandates clarity, while recognizing that absolute precision is unattainable." *Id.*

When, as here, the claim employs a computer or microprocessor to accomplish the function, the structure disclosed must be more than just a reference to the microprocessor or computer generally. *See WMS Gaming Inc. v. Int'l Game Tech.*, 184 F.3d 1339, 1349 (Fed. Cir. 1999). Likewise, "simply disclosing software . . . without providing some detail about the means to accomplish the function is not enough." *Noah Sys. Inc. v. Intuit Inc.*, 675 F.3d 1302, 1312 (Fed. Cir. 2012) (citing *Finisar Corp. v. DirecTV Grp., Inc.*, 523 F.3d 1323, 1340-41 (Fed. Cir. 2008)). What must be disclosed then is a specific algorithm for accomplishing the function. *See, e.g.*, *Ergo Licensing, LLC v. CareFusion 303, Inc.*, 673 F.3d 1361,1364-65 (Fed. Cir. 2012). That is to say the specifications must disclose "a series of instructions for the computer to follow," i.e, "a step by step procedure for accomplishing a given result." *Typhoon Touch Techs., Inc. v. Dell, Inc.*, 659 F.3d 1376,1384-85 (Fed. Cir. 2011) (internal citations omitted). The law does not require disclosure of the actual coding, however. The algorithm can take the form of "any understandable terms including as a mathematical formula, in prose . . . or as a flow chart, or in any other manner that provides sufficient structure." *Finisar Corp.*, 523 F.3d at 1340 (internal citations omitted). It is important to remain conscious of the distinction between whether a structure is disclosed and whether it is adequate. In this case, because a microprocessor is employed, the first question is whether an algorithm is disclosed at all. If one is disclosed, then the court must be satisfied that it is sufficient.

Definiteness, is a question of law, *Eplus, Inc. v. Lawson Software, Inc.*, 700 F.3d 509, 517 (Fed. Cir. 2012), and can be properly resolved on summary judgment, *see, e.g., Ibormeith IP, LLC v. Mercedes-Benz USA, LLC*, 732 F.3d 1376 (Fed. Cir. 2013) (affirming district court's grant of summary judgment for defendant on the issue of indefiniteness). Although an issue of law, the court is often aided by the testimony of persons of ordinary skill in the art.

---

[4] The Court went on to explain that "[i]t cannot be sufficient that a court can ascribe *some* meaning to a patent's claims; the definiteness inquiry trains on the understanding of a skilled artisan at the time of the patent application, not that of a court viewing matters *post hoc*." *Nautilus*, 134 S. Ct. at 2130.

See, e.g., *Intel Corp. v. VIA Techs.*, 319 F.3d 1357, 1367 (Fed. Cir. 2003). The Federal Circuit has described a test for the adequacy of a disclosed structure as whether "a person of ordinary skill in the art would be []able to recognize the structure in the specification and associate it with the corresponding function in the claim." *Noah Sys.*, 675 F.3d at 1312. The disclosed structure cannot be too general, however. The patentee may not claim every possible means of accomplishing the claimed function. That is in essence a restatement of the function and is known as "purely functional claiming." *See Noah Sys.*, 675 F.3d at 1318-19.

It is defendant's burden to prove that "the specification fails to disclose sufficient corresponding structure" by clear and convincing evidence. *TecSec, Inc. v. IBM Corp.*, 731 F.3d 1336, 1349 (Fed. Cir. 2013). We grant summary judgment only when the "movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Rule 56 of the Rules of the United States Court of Federal Claims ("RCFC"). We will draw all justifiable factual inferences in favor of the non-movant. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986).

Defendants argue that the '921 patent fails to disclose a structure for the means-plus-function limitations identified.[5] Defendants believe that nowhere in the specifications is found a step-by-step set of instructions for claim 8's "coding means" limitation, the "access code" limitation of claims 2 and 9, or the "secret microcode" limitation of claims 4 and 10. Instead, the government and Gemalto argue that the language of the specifications is nothing more than a restatement of the function, an example of the prohibited "purely functional claiming." *Noah Sys.*, 675 F.3d at 1318-19. Plaintiff answers that the requirements of 35 U.S.C. § 112 are "not a high bar" and that all it must do is show "some structure corresponding to the means in the specification, as the statute states, so that one can readily ascertain what the claim means and comply with the particularity requirements of [§ 112], ¶ 2." Pl.'s Opp'n to Defs.' Mot. for Summ. J. 14 (quoting *Biomedino, LLC v. Waters Techs. Corp.*, 490 F.3d 946, 950 (Fed. Cir. 2007)). Plaintiff provides the court with citation to various lines in the specifications that it believes constitute an algorithm and testimony from its expert to buttress its position. We turn now to the specifics of the claims.

---

[5] Defendants state in their reply brief that, even were the court to find an algorithm, the specifications are inadequate as overly general. This is not, however, the thrust of their motion or their reply in support.

I. The Coding Means Limitation

Claim 8 teaches a "portable data carrying device" comprised of a "control unit" and "data memory." DX 1 at A7. The coding means limitation adds that access to the data memory by the control unit is protected by a "coding means which is in the carrying device and is operative to permit entry into the additional data memory . . . without participation of system parts external to the carrying device." *Id.* It is that protection that comprises the coding means. Plaintiff identifies what it believes are three structures, or algorithms, in the specifications, each corresponding to the first three embodiments as shown in the patent figures above. It needs only one embodiment to disclose a sufficiently linked structure in order for claim 8 to be valid. *Cardiac Pacemakers, Inc. v. St. Jude Med., Inc.*, 296 F.3d 1106, 1113-14 (Fed. Cir. 2002).

A. The First Embodiment

For the first embodiment, corresponding to figure 1, plaintiff offers the following structure and algorithm:

> A control unit or microprocessor [2] programmed with instructions to perform the algorithm of (a) producing an access code signal [C], and (b) sending the access code signal [C] to the access code region [6], which (c) allows access to the additional data memory [5] upon successful decoding of information in the access code signal [C].

Pl's Opp'n 20.[6] This is not a quotation from the '921 patent specifications themselves but is plaintiff's summary of portions of the specification relating to the first embodiment.

In its brief and at oral argument, plaintiff presented a paragraph from the specifications heavily edited with sections italicized and bolded (in its brief) or underlined and highlighted (at oral argument). From those it draws

[6] Defendants point out in their briefing that plaintiff's identification of the '921 patent's structure has not been consistent throughout the history of litigation regarding this patent in this case and in district court. We will consider the specific structures offered by plaintiff in its briefing on the motion before us.

the needed algorithm.

This language is as follows:

> In order to prevent manipulation and unauthorized access to the data memory 5, entry to this memory is protected by the control unit 2. For example according to FIG. 1, an access code region 6 is associated with the data memory 5 for this purpose. In this manner the memory is accessible only by means of a code signal C which is produced by the control unit 2, that is, data exchange D between the components 2 and 4 is only possible after successful decoding of the code region 6. . . . Such protected data exchange processes are produced within the data carrying device 1 with a certain degree of self-sufficiency without participation of external system parts . . . . The access in particular to the sensitive data in the data memory 5 is thereby protected by means of a barrier which can only be overcome by means of key codes (key lock) employed with the card. . . . in the microprocessor each of the control unit 2 new access codes can always be generated, for example after each successful access to the additional data memory. [(memories)].

Pl.'s Opp'n 22 (quoting DX 1 at A3-A4) (omitted language is that which was not bolded or italicized as it appears in plaintiff's brief). In sum, these specifications instruct that the control unit protects the device's memory by making it "accessible only by means of a code signal" produced by the control unit. It then states that data exchange between the control unit and the memory is "possible after successful decoding of the code region." The quoted language then repeats the security feature of the access code permitting the only access to the device's memory and states that "new access codes can always be generated, for example after each successful access" to the memory.

Defendants argue that this language does not explain how the code region will be decoded or what constitutes the code signal, i.e., what sort of code it is, by what means it is produced, and whether it is encrypted. This, defendants argue, is tantamount to claiming every possible type of code produced by any type of software or hardware and every possible method of decoding the code by the access code region, which they argue is prohibited pure-functional claiming.

The specification states that access to the memory is protected by the

control unit and an access code region associated with the data memory, that a "code signal" will be produced by the control unit, and that data exchange between the control unit and the memory is possible only after the code region is decoded. The corresponding drawing, figure 1, indicates a code signal being transmitted between the control unit and the memory by employing a one-way arrow and shows a two-way arrow corresponding to the data exchange between the control unit and the data memory. We agree with plaintiff that a fair reading of the quoted specification and the drawing is that the control unit (a microprocessor) is "programmed with instructions to . . . produc[e] an access code signal" and send it "to the access code region, which . . . allows access to the additional data memory" if the code is correct. Pl.'s Opp'n 20.

Defendants' point that the specification discloses no particulars as to what form the code signal should take or how the access code region will decode itself are inapposite to the general argument on which they rely. Those points might be well taken if we were considering whether the disclosed structure was adequate. Instead, we have been asked to decide whether the patent discloses a structure at all, in this context an algorithm, corresponding to the function in claim 8.[7] That is a different and more limited inquiry. We think it plainly does. Whether it is adequate is a question we leave for another day.

B. The Second Embodiment

The second embodiment, corresponding to figure 2, is laid out in the following language in the specifications:

> In the embodiment according to FIG. 2, the general construction of the data carrying card 1 with the integrated circuit components 2*a*, 4*a* interconnected by means of the conductor strip 3 is the same as in FIG. 1. The control unit 2*a* connected with the external contacts 9 similarly comprises a microprocessor and a data memory region. On the other hand,

---

[7] It is important to remember what the function claimed by the coding means limitation of claim 8 is. It claims a means for securing data access without participation of parts external to the device. The use of an access code is a particular structure disclosed in the specifications to accomplish that function. Although brief and devoid of detail, the first embodiment is thus not merely a restatement of the function.

> the component 4*a* contains besides the additional memory 5 likewise a microprocessor 8 [w]hereby still further possibilities with respect to applications and security are achieved. With the help of a microprocessor 8 it is possible not only to secure entry to the data memory 5 from the control unit 2 as in FIG. 1 and with it the unauthorized reading of data from the memory 5, but also beyond this to secure the entire data exchange over the conductors 3, that is, to accomplish this in coded or decoded form. However, the double-pass entry system is only possible after a successful cryptographic authentication from the opposite pas[s] which again is only produced, "within the card", that is, without participation of external system parts.

DX 1 at A4. This passage adopts by reference the structure of the first embodiment and adds a microprocessor to the memory chip. The feature added by the second embodiment is the "securing [of] the data exchange over the conductors," presumably by some form of encryption, though the language states it might be in "decoded form," or the use of "cryptographic authentication" and a "double-pass entry system." *Id.* The figure 2 drawing is similar to the first but the memory chip now includes a section (8) that represents the microprocessor added in this embodiment. The exchange of data between the two chips is represented by a bidirectional arrow.

Plaintiff finds in the above quoted language the following set of instructions:

> The second microprocessor 8 is programmed to perform the algorithm of (a) encrypting (or encoding) data from the additional data memory 5 and (b) sending the encrypted (or encoded) data to the first control unit or microprocessor 2*a*. The microprocessor 2*a* is programmed to perform the algorithm of (c) receiving the data from the second microprocessor 8 and (d) decrypting (or decoding) data received.

Pl.'s Opp'n 27.

Defendants again argue that all this amounts to is a restatement of the claimed function–securing access to the data memory without parts external to the device–not the means for accomplishing it. They assert again that the second embodiment is devoid of any specifics, other than mention of a "double-pass entry system" or "cryptographic authentication," about the

encryption methods to be employed. This, they believe, is evidence of a specification empty of structure and therefore indefinite.

In response to defendans' argument that the specifications are fatally devoid of structure, plaintiff offered the testimony of its expert, Dr. Steward, to provide two ways in which the second embodiment might achieve its function:

> In a first manner of operation, data between the control unit and the additional data memory is exchanged in encrypted or encoded form. In this first manner of operation, one of ordinary skill in the art would understand that a first control unit or microprocessor is programmed with instructions to encrypt and/or decrypt (or encode and/or decode) data, and a second microprocessor is programmed with instructions to encrypt and/or decrypt (or encode and/or decode) that data.
>
> In a second manner of operation, the control unit can operate in a manner similar to the Figure 1 embodiment described above and be used to produce an access code. With this second manner of operation, one of ordinary skill in the art would understand that the control unit or first microprocessor is programmed with instructions to produce an access code, and the second microprocessor operates as the access code region.

PX E ¶¶ 55, 58. As to defendants' argument that the disclosure of encryption without any specifics is insufficient, Dr. Stewart opined that

> [o]ne of ordinary skill in the art would appreciate that many different known types of encryption or encoding algorithms could be used in accordance with the '921 Patent for secure data exchange between the controller and the additional memory. Many encryption or encoding algorithms were well known and used as of 1988, including DES encryption, RSA encryption, and Diffie-Hellman encryption.

Id. ¶ 57. This testimony, plaintiff argues, is enough to meet the Federal Circuit's test of whether a person of ordinary skill in the art could recognize the claimed structure and associate it with the claimed function.

As to the limited question of whether the second embodiment discloses

any structure at all, here an algorithm, we answer in the affirmative. In light of the incorporation of the first embodiment, and some confusing surplusage aside, it is clear that the second embodiment adds a microprocessor to the data memory, which is programmed to encrypt the data exchanged between the control unit and the memory. This is not, as defendants urge, the claiming of all possible ways to secure such a data exchange. It might be overly broad or insufficiently detailed, and Dr. Stewart's opinion might be countervailed by other testimony offered by defendants as to why it is insufficient, but we reject the notion that it is a mere restatement of the claimed function and the associated argument that it is not an algorithm at all. The adequacy of the disclosed algorithm will be judged after a hearing on the issue.

C. The Third Embodiment

The third structure offered by plaintiff, corresponding to figure 3, "includes a control unit or microprocessor 2b that is programmed to perform the algorithm of (a) retrieving data from the additional data memory 5 and (b) the decrypting or decoding the data received using a secret microcode 10 (*i.e.*, secret or uncommon instructions or codes)." Pl.'s Opp'n 33. The corresponding language cited by plaintiff from the specification is as follows:

> The general construction in the example according to FIG. 3 with a control unit 2*b* and an additional data memory 4*b* in the form of separate integrated circuits corresponds again to the foregoing examples. A protected entry to the additional data memory 5 is realized in this embodiment again in another manner, namely in that the microcode of the control unit 2*b*, designated 10, is secret. Of course, a well known microprocessor can be employed in the control unit 2*b* and this microprocessor can be based upon an "uncommon" microcode 10 only known to the manufacturer and therefore secret. In this manner an unauthorized access to the data stored in the data carrier or correspondingly a decoding of the information exchanged over the conductors 3 is rendered impossible, even if there was success in getting through the multiple conductor strip 3. . . .
>
> In a manner similar to the example according to FIG. 3, the microcode 10a in the microprocessor of the control unit 2c is secret so that entry to the additional data memory 5 is again protected . . . .

DX 1 at A4. The element added by embodiment three is the use of a secret microcode. The components of the device in figure 3 are arrayed, as in the first two embodiments, with a control unit and a separate data memory chip, which in the second and third embodiments also includes a microprocessor. Access to the memory is protected in this embodiment by use of a secret microcode, a code "only known to the manufacturer." This, according to the specification, renders "decoding of the information exchanged over the conductors" impossible.

The details of how the device employs the secret microcode are not disclosed other than the statement that, without the microcode, "a decoding of the information exchanged over the conductors . . . is rendered impossible." Whether the microcode is used like an access code or whether it is used like a cipher to encrypt and decrypt the data exchange, as plaintiff posits, is also not specifically disclosed. The specification hints at both: "in this manner an unauthorized access to the data stored in the [memory] or corresponding a decoding of the information exchanged over the conductor 3 is rendered impossible." *Id.*

Defendants argue that this embodiment is wholly devoid of instructions that the microchips will be programmed to follow and thus is not a structure. We agree to this extent: it is not distinct enough from the previous embodiments to be considered an algorithm of its own.

Although arrayed in a similar way to the first two embodiments and employing the same physical makeup as the second–two microprocessors, one in the control unit and one in the data memory–the third embodiment's specifications add too little to the previous embodiments to stand on their own. These specifications instruct that the data is protected in this embodiment "in another manner, namely in that the microcode of the control unit . . . is secret" and thus "unauthorized access to the data stored in the data carrier or correspondingly a decoding of the information exchanged over the conductors 3 is rendered impossible." *Id.* Figure 3 adds nothing to the written specifications, showing only the two chips and item 10, which is simply the existence of a secret microcode in the control unit. Whether the data is meant to be protected by a secret access code or, as plaintiff's argues, by an encryption employing a secret cipher, the disclosure of the fact that the device employs an uncommon code, one that is secret, is not an algorithm. It does not change any of the steps in the instructions for retrieving data from the data memory. Simply adding the word "secret" to the structure does not make it different structure. We view the third embodiment merely as a restatement of

the first two with the word "secret" added.

Unlike the first and second embodiments, in which at least a minimal set of instructions was disclosed, the third embodiment raises only possibilities. It adds to the first two the use of a secret code but does not disclose any set of steps or instructions for the device to follow. That is insufficient.

Even if we viewed the addition of a "secret microcode" as adding something meaningful to the third embodiment, it would still be insufficient to constitute an algorithm. In *Triton Tech of Texas, LLC v. Nintendo of America, Inc.*, No. 2013-1476, 2014 WL 2619546 (Fed. Cir. June 13, 2014), the Federal Circuit recently held, in rejecting a means-plus-function claim, that "merely using the term 'numerical integration' does not disclose an algorithm . . . but is instead an entire class of different possible algorithms used to perform integration." *Id*. at *3. Thus the claim at issue did not "limit the scope of the claim to the 'corresponding structure, material, or acts' that perform the function, as required by section 112." *Id.* The same is true of the purported algorithm offered by plaintiff for the third embodiment.

D. The Fourth Embodiment

The fourth and final offered structure, corresponding to figure 4, "includes a single integrated circuit 12 with a control unit or microprocessor 2c programmed to perform the algorithm of (a) retrieving data from the additional data memory 5 and (b) decrypting or decoding the data received from the additional data memory 5 using a secret microcode 10a." Pl.'s Opp'n 36. The following is the corresponding language from the specification:

> In contrast to the above described embodiments, the data carrying device or correspondingly the plastic card 1 according to FIG. 4 contains one individual semi-conductor component 12, on which the control unit 2*c*, the additional data memory 5 as well as further circuit regions are in total implemented in an integrated circuit configuration. In a manner similar to the example according to FIG. 3, the microcode 10*a* in the microprocessor of the control unit 2*c* is secret so that entry to the additional data memory 5 is again protected ("mechanical" access on the conductors between the regions of the integrated circuit on one and the same carrier would naturally however be considerably more difficult than on the conductors 3 [w]hich are

> laid within the plastic card 1 or correspondingly [w]ithin a module [w]hich consists of the two separate components 2 and 4).
>
> With the computer in the microprocessor of the control unit 2*c* there exists further an additional computer 14 in combination [w]ith registers 15 which are likewise positioned on the carrier 12. As indicated the registers 15 are likewise coordinated [w]ith the secret microcodes 10*a* of the control unit 2*c*, that is, the signal exchange between the control unit 2*c* and the additional computer 14 is produced likewise on the basis of the secret codes. One such additional calculator 14 makes possible the execution of especially highly developed cryptographic methods within the portable data carrying device, that is, without requiring external calculating capacity and thereby particular data exchanges with external system parts. This means that the application of the secret microcodes 10*a* remains restricted to the integrated circuits of the single carrier 12 in the data carrying device whereby high level security against manipulation and unauthorized access is achieved.

DX 1 at A4.

In its initial response and opposition to defendants' motion, plaintiff claimed the fourth embodiment as a separate algorithm meeting the definiteness requirement. Later in the briefing, in response to specific questions posed by the court for supplemental briefing, plaintiff disclaimed the fourth embodiment as a separate algorithm and included it as a further example of the algorithm it propounded for the third embodiment.

The difference in the fourth embodiment is that all of the chips are arrayed as one single circuit, which, according to the specifications, provides additional security. The novelty of this embodiment is not the programming of the processors but rather their integration into one circuit, i.e., the data exchange is further secured by the physical location of the several processors in one circuit. It is thus not a separate algorithm that could meet the definiteness requirement for claim 8 and plaintiff has correctly disclaimed it as such.

II. The Dependent Claims: The Access Code Limitation and The Secret Microcode Limitation

Also at issue are two limitations found in four dependent claims. Dependant claims 2 and 9 limit the "coding means" of claim 8 by adding the following: "the code means includes means within the control unit (2) for producing a code signal (C) for entry to the data memory through the access code region." DX 1 at A4. Claim 9 is substantially similar: "coding means includes means within the control unit for producing a code signal for entry to the data memory through the access code region." *Id.* at A7. Dependent claims 4 and 10 limit the "coding means" of claim 8 through the additional language teaching that the "coding means" includes "means within the control unit (2*b*) for producing a secret microcode for communications between the control unit and the data memory." DX 1 at A4 (claim 4) (claim 10 uses almost identical language).

Defendants argue that, irrespective of whether there is any structure disclosed in the specifications for independent claim 8, no additional structure corresponding to these dependent means-plus-function limitations is disclosed. Defendants' point is that nowhere in the specification are steps or instructions disclosed for the microprocessor to follow in choosing, producing, or sending an access code signal. Thus the language offered by plaintiff is nothing more than a restatement of the function, not an algorithm for achieving the claimed function, argue defendants. Likewise, for the secret microcode limitation, defendants argue that nothing in the patent specifications discloses how the microcode will be used for encrypting or decrypting the data stored in the memory as is claimed in claims 4 and 9. Put another way, although claim 8 may disclose an algorithm for the general operation of the device, no separate instructions are disclosed for the "access code" limitation or "secret microcode" limitation.

A. The Access Code Limitation

For the access code limitation, plaintiff responds that the algorithm, limited to the first two embodiments, is "(a) producing an access code signal, and (b) sending the access code signal to the access code region, which allows access to the additional data memory upon successful decoding of information in the access code signal." Pl.'s Opp'n 38. Plaintiff argues that this is more than a restatement of the function because it includes the steps of sending the code to the access code region and the decoding of the code by the access code region.

There is no dispute that the function of the access code limitation is the production of an access code by the control unit, which will be used by the

data memory to grant access to it. The programming of the device includes the use of a pass code, produced by the control unit, and then sent to and read by the memory chip to grant access to the data in the memory chip. The problem for plaintiff is that the function and the offered algorithm amount to the same thing. Plaintiff is unable to cite to any additional lines in the specification that answer any of the questions posed by defendants in their motion for summary judgment: how will the device choose, produce, or send the access code. The patent simply does not disclose any information other than the fact that an access code will be produced and used, which is the function claimed by the access code limitation. The structure provided in the specifications for a means-plus-function limitation cannot be a simple restatement of the function; this is prohibited as purely functional claiming. *See Blackboard Inc. v. Desire2Learn, Inc.*, 574 F.3d 1371, 1384 (Fed. Cir. 2009). The access code limitation of claims 2 and 9 is indefinite because the patent specifications do not disclose an algorithm for achieving the claimed function of the access code limitation.

B. The Secret Microcode Limitation

For the secret microcode limitation, plaintiff contends that the following algorithm is present in the specifications for the third and fourth embodiments: "(a) retrieving data from the additional data memory and (b) decrypting (or decoding) data received from the additional data memory with or using a secret microcode." Pl.'s Opp'n 39. Plaintiff argues that this is something more than a restatement of the function of producing a secret microcode because it includes the steps of retrieving the data from the memory and then decoding or decrypting it using the code.

The function of the limitation is producing a secret microcode to be used for the exchange of data between the control unit and the memory chip. As we noted in our analysis regarding the third embodiment, the patent does not disclose how the microcode will be used; it hints at the use of a pass code or cipher for decryption.[8] As quoted above, plaintiff's proposed algorithm

[8] "[A] well known microprocessor can be employed in the control unit [] and . . . can be based on an 'uncommon' microcode [] only known to the manufacturer . . . . In this manner an unauthorized access to the data stored in the data carrier or correspondingly a decoding of the information exchange over the conductors [] is rendered impossible . . . ." DX 1 at A4 (quote from specifications for the third embodiment).

would clear that ambiguity by offering that the secret microcode is used for decrypting data received from the memory chip. Plaintiff's algorithim also adds to the limitation the steps of retrieving the data from the memory and then decoding or decrypting it.

Setting aside the question of whether the specifications offer even that minimal level of clarity,[9] beyond producing a secret microcode that will protect from unauthorized access to the memory or unauthorized decryption of it, nothing further is disclosed by the specifications. The secret microcode limitation claims a means for producing and utilizing a secret microcode. The specifications add nothing other than that such a code will be produced and utilized by the device for preventing unauthorized access or decryption. This is merely a restatement of the function and thus cannot constitute the needed structure. Each function of a claimed means must have a corresponding structure, here an algorithm, in the specifications.[10] *See Noah Sys.*, 675 F.3d at 1313-14 (The court found that the limitation in question contained two functions and that the cited specifications did not address the second function. Thus, the limitation was held to be indefinite.). Because no structure is disclosed, the secret microcode limitation is indefinite.

C. The *Katz* Exception Does Not Apply

For the first time, in its supplemental brief, plaintiff argues that the access code and secret microcode limitations do not require separate algorithms because the functions associated with these limitations are inherently performed by a computer processor or microprocessor. Plaintiff relies on the Federal Circuit's decision in *In re Katz Interactive Call Processing Patent Litigation*, 639 F.3d 1303, 1316 (Fed. Cir. 2011). We do not think *Katz* controls the outcome here.

---

[9] Were we to agree with plaintiff that its algorithm was sufficient, we would still be faced with the question of whether it was actually disclosed in the specifications. We take no position on that question.

[10] Plaintiff also makes the novel claim in its supplemental brief that neither the access code nor the secret microcode limitations require separate algorithms because they "serve to limit the structures and algorithms for the coding means of the independent claims." Pl.'s Supp. Br. 6. Plaintiff does not cite any authority for that proposition, and we are unable to find any.

In *Katz*, the Federal Circuit reversed the district court's holding that the patent in suit was devoid of an algorithm for general computer functions such as "processing, receiving and storing" data. *Id.* (internal quotations omitted). The court held that the patentee was only claiming the general purpose functions of a computer and thus no disclosure of an algorithm was required. The disclosure of a computer processor itself was sufficient structure. *Id.* A specific algorithm for a processor to achieve the claimed function is thus only required when the claim involves "specific functions that would need to be implemented by programming a general purpose computer to convert it into a special purpose computer capable of performing those specified functions." *Id.* (citing *Aristocrat Techs. PTY Ltd. v. Int'l Game Tech.*, 521 F.3d 1328, 1333-34 (Fed. Cir. 2008).

The function of producing an access code by one chip and then the utilization of it by another chip to grant access to its stored data goes beyond storing or retrieving data. It is the securing of data from unauthorized access that is claimed in this case. The patentee clearly intends for the chips to be used in a specific way for a special function, unlike in *Katz*.

Likewise, the production and use of a secret microcode to limit access or for decryption goes beyond a general purpose function of a processor. The use of the term "secret" is enough to distinguish from the generic use of a processor. The secret microcode limitation requires an algorithm for achieving that function. *Katz* does not save claims 2, 4, 9, and 10 from the definiteness requirement of 35 U.S.C. § 112 paragraph 2.

CONCLUSION

We find that an algorithm for the coding means limitation of claim 8 is disclosed in the first and second embodiments of the specifications. Whether these algorithms are sufficient to meet the definiteness requirement will be addressed after the court has heard testimony from persons of ordinary skill in the art. The third and fourth embodiments do not present an algorithm for carrying out the coding means limitation of claim 8. We also find that no algorithm is disclosed for the access code and secret microcode limitations of claims 2, 4, 9, and 10 because the specifications merely recite the claimed function. Those claims are therefore indefinite. Accordingly, defendants' motion for summary judgment is granted in part and denied in part. The court will convene a status conference to discuss further proceedings.

s/ Eric G. Bruggink
ERIC G. BRUGGINK
Judge