United States District Court,
M.D. Florida, Tampa Division.

TIMECERTAIN, LLC,
Plaintiff.
v.
AUTHENTIDATE HOLDING CORPORATION, et al,
Defendants.

No. 8:05-CV-1559-T-23EAJ

Dec. 22, 2006.

Christopher M. Faucett, Houston, TX, Corby R. Vowell, Edward W. Goldstein, Goldstein, FAUCETT & PREBEG, LLP, Houston, TX, Stacy Delayne, Blank Holland & Knight, LLP, Tampa, FL, for Plaintiff.

Alexander J. Hadjis, David Ziskind, Michael W. Maas, Robert W. Giles, Yan Wang, Sonnenschein, Nath, & Rosenthal, LLP, Washington, DC, Andrew C. Greenberg, Carlton Fields, P.A., Tampa, FL, David B. Newman, Sonnenschein, Nath & Rosenthal, New York, NY, Joel N. Bock, Sonnenschein Nath & Rosenthal, LLP, Short Hills, NJ, for Defendants.

ORDER

STEVEN D. MERRYDAY**, United States District Judge.**

The plaintiff sues (Doc. 1) the defendants for alleged infringement of United States Patent Numbers 6,792,536 ("the 536 Patent") and 6,898,709 ("the 709 Patent"), which patents protect certain aspects of the plaintiff's invention for "time-stamping" a digital data file. On July 27, 2006, the parties submitted a "Joint Chart of Claim Terms and Proposed Constructions" (Doc. 56), in which the parties dispute the meaning of nineteen claim terms and three "means plus function" terms. A September 15, 2006, order (Doc. 72) granted the parties' joint motion (Doc. 65) for a claim construction hearing pursuant to Markman v. Westview Instruments, Inc., 517 U.S. 370 (1996), which hearing occurred following the submission of briefs on the disputed claim terms (Docs.60, 62). On November 27, 2006, each party presented both a technology tutorial and oral argument on claim construction (Doc. 98).

BACKGROUND

The plaintiff's patents claim a unique technology for "time-stamping" a digital file created or copied by the user of a personal computer ("PC"). Simply put, a "time-stamp" enables others to verify the time that a PC's user creates, accesses, modifies, receives, or transmits any given digital file. Time-stamping permanently records the precise time at which a certain event occurs during the life-cycle of that file, and enables a PC's user to represent credibly to others the time at which a given life-cycle event occurred.

Ordinarily, a PC time-stamps a digital file upon the file's creation, access, modification, receipt, or transmission by the PC's user. Unlike the prior art disclosed in the plaintiff's patents, the standard time-stamp issued by a PC is neither unalterable nor reliable. Because the PC's system-clock generates the standard time stamp, the PC's user easily may alter the system-clock to attest a bogus time or date and, if the PC's system clock is inaccurate, the standard time-stamp is concomitantly inaccurate.

In response to these systematic deficiencies of standard time-stamping (and before the issuance of the plaintiff's patents), alternative methods for time-stamping a digital file developed to ensure easy detection of any modification to the time or date assigned to a given file. As required, the plaintiff's patents include disclosure of pre-existing, alternative time-stamping technology, which pre-date (by years) the plaintiff's patented technology (536 Patent at 11:28-12:11; 709 Patent at 11:18-67). The specifications of the plaintiff's patents seek to distinguish the plaintiff's technology over prior art, designated by the patentee as "conventional digital time-stamping services" ("DTS") (536 Patent at 11:30-32; 709 Patent at 11:19-43).

In a conventional DTS, an initial "hash function" is performed on a file that a PC's user desires to time-stamp. "Hashing" subjects a file's digital contents to an algorithm that effectively chops and mixes (i.e., "hashes") those contents to create a unique string of characters, which string is called a "digest" and which serves as a sort of digital "fingerprint" for that file. Hashing the same file with the same hashing algorithm produces the same digest. Hashing a different file produces a unique and different digest. Although a digest identifies a specific file, a digest is not the file and cannot be used to access or retrieve the file.

Once a file is hashed and a digest created, the PC's user electronically transmits the digest (but not the original file) to a secure third party remote from the user, which party cryptographically bundles the digest with a verified date and time by "signing" those two components. This signing process time-stamps the bundle and produces a "digital identity certificate," which identifies the DTS (the entity signing both the digest and the date and time) for later reference. The DTS next transmits to the user (1) the user's original digest; (2) the date and time generated by the DTS upon receipt of the user's digest; (3) a hash of the cryptographic bundle created by the DTS's digital signing process (combining the digest and the DTS-generated date and time); and (4) a digital identity certificate. The original file and the certified time-stamped digest prove the file's existence at the time the digest was time-stamped.

The plaintiff's patent addressed two perceived drawbacks of conventional DTS. First, "because the DTS is located remotely relative to the user, there is no reliable way to provide a digital time-stamp locally at the user's site" (536 Patent at 12:8-11, 45-54; 709 Patent at 11:64-67, 12:33-43). Second, conventional DTS's bundling of the date and time with the digest instead of the original file created "the possibility that two individuals may collude to falsely state the value of a hash" (536 Patent at 11:40-46, 12:52-60; 709 Patent at 11:29-35, 12:40-49). Accordingly, the plaintiff's patent creates a time-stamping technology that resides on the user's PC and time-stamps files locally, rather than remotely. Further, the plaintiff's patented technology time-stamps the file itself, not a digest of the file. These time-stamping features are embodied in the claims of the plaintiff's patents.

ANALYSIS

In the claims of his patent, a patentee is required to "define precisely what his invention is." Phillips v. AWH Corp., 415 F .3d 1303, 1312 (Fed.Cir.2005). A patent's claims notify the interested public, including potential competitors, of the scope of the patentee's invention. Johnson & Johnson Assoc. v. R.E. Service Co., 285 F.3d 1046, 1052 (Fed.Cir.2002) (en banc). The construction of a patent claim is solely a question

of law. Cybor Corp. v. FAS Techs., Inc., 138 F.3d 1448, 1454-56 (Fed.Cir.1998) (en banc).

A patent claim's words "are generally given their ordinary and customary meaning." Phillips, 415 F.3d at 1312. A disputed term should enjoy the same meaning that a "person of ordinary skill in the art in question" would assign "at the time of the invention ." Innova/ Pure Water, Inc. v. Safari Water Filtration Sys., Inc., 381 F.3d 1111, 1116 (Fed.Cir.2004). To ascertain the ordinary meaning of a term, a court should consult the same resources as a person of ordinary skill in the art, which resources include "the words of the claims themselves, the remainder of the specification, the prosecution history, and extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art." Innova/Pure Water, Inc., 381 F.3d at 1116. In construing a patent claim, "[t]he sequence of steps used by the judge in consulting various sources is not important; what matters is for the court to attach the appropriate weight to be assigned to those sources in light of the statutes and policies that inform patent law." Phillips, 415 F.3d at 1324.

A patent's claims "must be read in view of the specification of which they are a part." *Markman,* 52 F.3d at 979. "[T]he single best guide to the meaning of a disputed term," a patent's specification usually is dispositive of a disputed claim's construction. Phillips, 415 F.3d at 1312. "The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction." Reinshaw PLC v. Marposs Societa' per Azioni, 158 F.3d 1243, 1250 (Fed.Cir.1998); *On* Demand Mach. Corp. V. Ingram Indus., Inc., 442 F.3d 1331, 1344 (Fed.Cir.2006) (holding that "each term must be construed to implement the invention described in the specification").

Claims also may be limited by a patent applicant's arguments to the United States Patent and Trademark Office during the applicant's "prosecution" of the patent application. Phillips, 415 F.3d at 1317. In addition to consulting the specification, a court should consider a patent's prosecution history, which may reveal "how the inventor understood the invention and whether the inventor limited the invention in the course of prosecution." Phillips, 415 F.3d at 1317. However, the prosecution history "often lacks the clarity of the specification and thus is less useful for claim construction purposes." Phillips, 415 F.3d at 1317.

In its discretion, a court also may rely on extrinsic evidence, which constitutes "all evidence external to the patent and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises." *Markman,* 52 F.3d at 980. Although perhaps useful, extrinsic evidence is "less significant than the intrinsic record in determining 'the legally operative meaning of claim language.' " Phillips, 415 F.3d at 1317 (quoting C.R. Bard, Inc. V. U.S. Surgical Corp., 388 F.3d 858, 862 (Fed.Cir.2004)). Generally, extrinsic evidence is "less reliable than the patent and its prosecution history in determining how to read claim terms." Phillips, 415 F.3d at 1318.

Although claim construction is the province of the court (and not the jury), *Markman* requires a district court neither to hold a hearing nor to follow any particular procedure for claim construction. Ballard Medical Products v. Allegiance Healthcare Corp., 268 F.3d 1352, 1358 (Fed.Cir.2001) (holding that a court may approach the task of claim construction "in any way that it deems best"). The instant parties dispute the meaning of nineteen claim terms and three "means plus function" terms (Doc. 55). However, the parties' presentations at the November 27, 2006, *Markman* hearing focused on fewer than half of the disputed claim terms. Consistent with the parties' presentations, this order construes only those claim terms most likely to advance resolution of the present controversy. FN1

FN1. "District courts have wide latitude in how they conduct the proceedings before them, and there is nothing unique about claim construction that requires the court to proceed according to any particular

protocol." Ballard Medical Products v. Allegiance Healthcare Corp., 268 F.3d 1352, 1358 (Fed.Cir.2001). *Markman* requires a court to construe a patent's claims "only to the extent necessary to resolve the controversy." Biovail Corp. v. Andrx Pharms, Inc., 239 F.3d 1297, 1301 (Fed.Cir.2001); Ballard Medical Products, 268 F.3d at 1358 (holding that a district court "need not exhaustively discuss" all claim construction issues raised by the parties).

"Trusted Time Source"

"Trusted time source" appears in each disputed patent claim (536 Patent: 1,6; 709 Patent: 1,17). The defendants contend that the phrase "trusted time source" means "a non-resettable and tamper-proof real time clock that is installed on or as part of the computer of a user who desires to time-stamp a digital data field" (Doc. 62 at 14). The plaintiff argues that the phrase "trusted time source" means simply "a source from which a time value that is trustworthy may be obtained" (Doc. 60 at 12). However, the latter definition contradicts the patents' express identification of a "local source of trusted time" as an important aspect of the invention. One of the express objectives of the plaintiff's invention is to "provide such systems, apparatus, methods, and articles of manufacture for time-stamping digital data files, which do not continually rely on a remote trusted source of time" (536 Patent at 14:14-18; 709 Patent at 14:2-6).

The plaintiff's proposed construction also contradicts the express teachings of the patents' specifications. In attempting to distinguish his invention over existing prior art, the patentee expressly defines a "trusted time source" as "a real time clock, which is not resettable, is independent of any system clock of the PC, and is installed locally relative to the PC" (709 Patent, Abstract). A patentee may act as his own lexicographer to specially define a word or phrase used in his patent. Markman v. Westview Instruments, Inc., 52 F.3d 967, 979-80 (Fed.Cir.1995), *aff'd,* 517 U.S. 370 (1996). If a patentee provides a definition to distinguish his invention over prior art, he may not later attempt to recapture the disclaimed meaning. Astrazeneca AB v. Mutual Pharmaceutical Co., 384 F.3d 1333, 1340 (Fed.Cir.2004).

Further, both patents repeatedly distinguish the patented invention over prior art on the basis that conventional DTS used a time source remote from the user. In distinguishing his invention from conventional DTS, the patentee states "because the DTS is located remotely relative to the user, there is no way to provide a digital time-stamp locally at the user's site" (536 Patent at 11:58-67; 709 Patent at 11:64-67). "It would be much more desirable to provide systems and methods of time-stamping digital data files locally and without continuing reliance on a remote time source" (536 Patent at 13:36-43; 709 Patent at 13:23-30). This crucial distinction throughout the patent between a "remote" versus a "local" time source necessarily informs any construction of "trusted time source."

Finally, the plaintiff's urged construction of "trusted time source" as "a source from which a time value that is trustworthy may be obtained" (Doc. 60 at 12) is mere tautology and would render the patent indefinite. Because a "trustworthy" time value may vary widely with context, the plaintiff's proposed construction fails to provide the public adequate notice (as required by law FN2) of the patentee's claimed invention. If "one of ordinary skill would not know from one [context] to the next whether a particular composition standing alone is within the claim scope or not ... [t]hat is the epitome of indefiniteness." *Geneva Pharmaceuticals, Inc. v. GlaxoSmithKline PLC,* 346 F.3d 1373, 1384 (Fed.Cir.2003). The law requires definiteness "to guard against unreasonable advantages to the patentee and disadvantages to others arising from uncertainty as to their rights." General Electric Co. v. Wabash Appliance Corp., 304 U.S. 364, 369 (1938); Athletic Alternatives Inc. v. Prince Mfg. Inc., 73 F.3d 1573, 1581 (Fed.Cir .1986).

FN2. 35 U.S.C. s. 112 requires a patentee to include "one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention." 35 U.S.C. s. 112, para. 2 (2006).

In sum, the patents' express identification of a "local source of trusted time" as an important aspect of the invention (536 Patent at 14:14-18; 709 Patent at 14:2-6), the patentee's express definition of a "trusted time source" (709 Patent, Abstract), the patents' repeated disavowal of a remote time source as used in prior art (536 Patent at 11:58-67, 13:36-43; 709 Patent at 11:64-67, 13:23-30), and the requirement of definiteness disfavor decisively the construction urged by the plaintiff. Accordingly, "trusted time source" means "a real time clock, which is not resettable, is independent of any system clock of the PC, and is installed locally relative to the PC." FN3

FN3. This definition comports with the patents' prosecution history. Indeed, during prosecution of the 536 Patent, the U.S. Patent and Trademark Office amended the applicant's claims. The amendment expressly requires a "trusted time source" that is local to the user's PC (Doc. 99). Likewise, the examiner's "Notice for Allowability" for the 709 Patent explains that the "trusted time source" is installed on or as part of the user's PC (Doc. 99).

"Digital Data File"

"Digital data file" appears in each disputed patent claim (536 Patent: 1,6; 709 Patent: 1,17). The defendants contend that "digital data file" means "a self-contained electronic representation of information, *i.e.,* a document, graphic, or database record, created by a user or copied by a user from another source, which has a unique file name by which it can be accessed by a user" (Doc. 62 at 10). The plaintiff argues that one of ordinary skill in the art would understand "digital data file" to mean merely "an aggregate of digital data" (Doc. 60 at 18).

The plaintiff's interpretation of "digital data file" presumably encompasses the digest or digital fingerprint that results from a hashed file, which digest is next transmitted to a third party for time-stamping in a conventional DTS. However, this construction contradicts the use of "digital data file" in the patents' claims, which repeatedly depict "digital data file" and "digest" as distinct. For example, the disputed claims of the 709 Patent describe "hashing said digital data file to produce a digest" (709 Patent: 1, 17). If a "digital data file" is a digest (as urged by the plaintiff), the phrase "hashing said digital data file to produce a digest" becomes unintelligible. Also, the disputed claims of the 536 patent distinguish a "saved file" from a digest (536 Patent: 1,6). Likewise, as the defendants persuasively argue (Doc. 70 at 11), the plaintiff's proposed construction ("an aggregate of digital data") impermissibly renders the word "file" superfluous within the phrase "digital data file," which phrase preposterously becomes, under the plaintiff's definition, a "file file." *See* Primos, Inc. v. Hunter's Spec., Inc., 451 F.3d 841, 847-48 (Fed.Cir.2006).

Further, both patents repeatedly distinguish the patented invention over prior art on the basis that a conventional DTS time-stamps the digest of a digital file but not the file itself (Patent 536 at 12:4-8; Patent 709 at 11:60-64). Highlighting the advantages of his invention over a conventional DTS, the patentee discloses a means to avoid "counterfeiting" problems by time-stamping the actual digital data file as opposed to time-stamping merely the digest that results from the hashed file (Patent 536 at 12:52-64; Patent

709 at 12:40 -52). The patentee also observes that time-stamping a digest, as opposed to time-stamping a file, certifies the date the DTS received the digest but not the date the actual document was accessed, created, modified, or transmitted (536 Patent at 12:4-9; 709 Patent at 11:60-64). Having disclaimed in the specifications the time-stamping of a digest, the patentee's claims may not be read to construe "digital data file" to encompass a digest.

Finally, the patents' prosecution history reveals that a "digital data file" is either created by a user or copied by a user from another source. The Examiner's Amendment, distinguishing prior art, explains that the applicant's time-stamp confirms the time at which "said file" is "accessed, created, modified, received, or transmitted by the user" (Doc. 99). This language confirms that time-stamping a digest reveals when the file associated with the digest existed but not when the file was accessed, created, modified, received, or transmitted by the user. This written description further distinguishes time-stamping a "digital data file" from the conventional DTS practice of merely time-stamping a digest.

Nothing in the patents' language or history supports equating a "digital data file" to a mere "aggregate of digital data." The patents' consistent use of "digital data file" and "digest" as distinct terms (536 Patent: 1,6; 709 Patent: 1, 17), the patents' express disavowal of the time-stamping of digests as an important aspect of the invention (536 Patent at 12:4-9; 709 Patent at 11:60-64), and the patents' prosecution history decisively disfavor the broad construction urged by the plaintiff. Accordingly, "digital data file" means "a collection of digital data stored as a self-contained unit, either created by a user or copied by a user from another source, and containing a unique file name by which it can be accessed by a user."

"Signing," "Key," and "Signed File"

As used in the patent claims' language and specifications, the definitions of "signing," "key," and "signed file" are closely related. "Signing" appears in each disputed patent claim (536 Patent: 1, 6; 709 Patent: 1,17). The defendants contend that "signing" means "the process of hashing input to compute a hash result and using a cryptographic function with a private key to transform the hash result into a digital signature" (Doc. 62 at 12). The plaintiff argues "signing" means simply "applying a unique identifying characteristic of a unique entity" (Doc. 60 at 12). The plaintiff's significantly elastic definition admittedly encompasses "a lawyer signing a brief" and "an illiterate person marking their X" (Doc. 60 at 11). However, the intrinsic evidence directly contradicts the plaintiff's unbounded construction.

Attempting to distinguish his invention over prior art, the patentee, in the specifications in both patents, expressly and unambiguously defines "signing":

To sign a document, or for that matter any other digital data file, a "signer" must first delimit the borders of the digital data file to be signed. As used herein, the term signer refers to any person who creates a digital signature for a message, such as message 110. The information delimited by the signer, in turn, refers to that message 110. A hash function 120 in the signer's software is used to compute a hash result 130, which is unique for all practical purposes to the message 100. Thereafter, a signing function 140 is used to transform the hash result 130 into a digital signature 160, but only after input of the signer's private key 150.

(536 Patent at 8:9-20; 709 Patent at 8:5-16). The patentee expressly defines signing as "creat[ing] a digital signature" by hashing a document or "any other digital data file" (536 Patent at 8:9-20; 709 Patent at 8:5-16). This definition reveals that "signing" does not encompass a physical, written signature.

Further, the patents' claims ubiquitously speak of "maintaining trust in the content of a digital data file" by "signing said digital data file," "hashing said signed file to produce a digest," and "signing said digest with a key to produce a certificate" (536 Patent at 40:22-41:21; 709 Patent at 43:4-43:67). The patent's use of "sign" consistently depicts "digital data" as the recipient of a signature, and the patent is unconcerned with the unlimited application of "a unique identifying characteristic of a unique entity." In this context, "signing" obviously means the signing of digital data and the creation of a digital signature. "The claims of a patent define the invention to which the patentee is entitled the right to exclude." Phillips v. AWH Corp., 415 F.3d 1303, 1312 (Fed.Cir.2005). Nothing in the patents' claims supports the plaintiff's suggestion that "signing" encompasses a non-digital, handwritten signature.

Because the claims of both patents' limit "signing" to digital signing, the plaintiff's proposed construction is inconsistent with the written descriptions' express definition. As the defendants persuasively argue, one of ordinary skill in the art understands "signing" (as used in the patents) to mean creating a digital (but not a written) signature. Consistent with the patent and its specifications, "signing" means "the process of computing a hash result, which result is converted into a digital signature using a cryptographic function and the signer's private key."

The patents' definition of "signing" contemplates the use of a signer's private "key" (536 Patent at 8:9-20; 709 Patent at 8:5-16). The patents expressly state that a key is not used for encryption:

Thereafter, a signing function 140 is used to transform the hash result 130 into a digital signature 160, but only after input of the signer's private key 150. This transformation is sometimes referred to as a process of encryption. However, such a characterization would be inaccurate, because message 110 itself may, or may not be, confidential.

Further, the specifications state "[s]ystems that generate and employ a secure key pair (i.e., a 'private key' for creating the 'digital signature' and a 'public key' for verifying that digital signature) are typically known as asymmetric cryptographic systems" (536 Patent at 7:48-51; 709 patent at 7:45-49). Consistent with the language of the patents, "key" means "a unique sequence used to create or verify a digital signature."

Finally, the defendants propose that a "signed file" is "a file with its digital signature" (Doc. 62 at 17). The plaintiff argues that a "signed file" means simply "a file with its signature" (Doc.. 60 at 16). However, the patents' claims specify that a digital file joined with a date and time is signed to create a "signed file" (536 Patent at 40:37-40, 41:15-18). Accordingly (and perforce the above constructions), a "signed file" means "a file with its digital signature."

"User"

"User" appears in each disputed patent claim (536 Patent: 1,6; 709 Patent: 1,17). The defendants contend that the phrase "user" means "a human who issues commands to the computer on which a digital data file was created or copied" (Doc. 62 at 14). The plaintiff argues that "user" means "an entity that issues requests to a system on which digital data exists" (Doc. 60 at 20). The plaintiff's urged construction avowedly encompasses a computer program or application as a "user" (Doc. 60 at 19-20). However, an examination of the intrinsic evidence reveals no "entity" other than a human being as performing the tasks of a "user."

In support of the construction of "user" as any human or non-human "entity" (including a computer program), the plaintiff argues that the specifications distinguish a "user" from an "end user," which "end

user" the plaintiff concedes is a human (Doc. 60 at 19). Yet, in the paragraph on which the plaintiff relies, "user" and "end user" are employed interchangeably:

This removes the burden of the request process from the end user of the certificate. Certificates in this model can be issued in a centrally managed bulk process on behalf of the user, and any keys that will be used to encrypt data can be securely backed up in case the issued key gets lost.

(536 Patent at 33:22-27). Obviously, "end user" in the first sentence and "user" in the second sentence denote the identical user.

Throughout the patents and their specifications, the patentee repeatedly attributes human attributes to a "user." For example, "User B wants to send User A an offer to purchase a piece of property that User A owns and an authorization to his bank to transfer money if a user accepts the offer" (536 Patent at 10:1-3; 709 Patent at 9:60-62). Similarly, "Verification means 580 may comprise any biometric device (e.g., iris scan, retinas scan, hand geometry, voice verification, and dynamic signature verification devices, etc.) that may be used in order to further verify the identity of a user" (709 Patent at 42:50-55). Finally, "This operation may take 0.5 to 2.0 seconds, which could be annoying to a user" (536 Patent at 25:7-8). A non-human "entity" (1) has no desire to sell property, (2) lacks eyes, fingers, hands, or a voice susceptible to "biometric" verification, and (3) is incapable of "annoyance."

Further, the specifications repeatedly depict a "user" as a human manipulating the computer toward some end. For example, "Hypothetically, a user at a computing means 400 signs a document and wants it time stamped" (536 patent at 11:42-43; 709 Patent at 11:30-32). Also, "Indeed, it is quite trivial for a user to reset the [local time clock] to any desirable date and time" (536 Patent at 6:24-25; 709 Patent at 6:24-25). Similarly, "[a] trusted date and time is programmed within real time clock 1000, such that it cannot be changed by a user of the PC system 700" (709 Patent at 28:6-8). Nothing in these statements permits a non-human "user."

In sum, the patentee's consistent use of "user" in the claims and specifications favors the construction urged by the defendants. The intrinsic evidence reveals that a "user" is a human who creates, time-stamps, and publicly verifies the moment of a file's creation. A "user" possesses an array of attributes unavailable to a computer program or other inanimate "entity." Accordingly, "user" means "a human who issues a command to the computer on which a digital data file was created or copied."

"Personal Computer"

"Personal computer" or "PC" appears in Claims 1 and 17 of the 709 Patent (709 Patent: 1, 17). The plaintiff contends that "personal computer" means "a computer system" (Doc. 60 at 18). Emphasizing the word "personal" in "personal computer," the defendants argue that "personal computer" means "a computer designed for use by one person at a time and designed to be independent of a mainframe or other computer. Personal computers have their own operating systems, software, and peripherals so that they can be set up and operated without additional equipment" (Doc. 62 at 19-20). Presumably, the plaintiff's urged construction includes any computer system, mainframe, or server. The defendants contend that the plaintiff's urged construction ignores "personal" while impermissibly inserting the "system" to include a server, mainframe, or "computer means."

The patentee's use of "personal computer" ' in the claims distinguishes a "personal computer" from a server

or mainframe. The specification describes a "personal computer" as a general purpose computer that utilizes input devices such as a keyboard, mouse, or touchpad (709 Patent 15:44-55; 15 :64-16 :8). The specification further provides: "Many varied computing means pervade today's society. PCs, web browsers, e-mail clients, e-mail servers, network file servers, network messaging servers, mainframes...." (536 Patent at 5:51-59; 709 Patent at 5:52-59). This specification reveals that "PC" or "personal computer" denotes one species of "computer means" but not all "computer means."

The patentee also distinguishes between a "stand-alone PC" and a "server" in the 709 Patent's specification: "Finally, the PC system 700 according to the present invention may simply comprise a stand-alone PC, a server, a PC or workstation coupled to a server" (709 Patent at 42:61-63. This specification reveals that a "personal computer" cannot encompass a server. In addition, one of ordinary skill in the art distinguishes a "personal computer" from a mainframe or server (Doc. 62 at 17). The plaintiff's construction of "personal computer" as "a computer system" (which "system" apparently could encompass the entire "world wide web") is unsupported by the intrinsic evidence. Accordingly, "personal computer" or "PC" means "a computer capable of operation without additional equipment, independent of a mainframe or other computer, and designed for use by one person."

ORDERED.

M.D.Fla.,2006.
Timecertain, LLC v. Authentidate Holding Corp.