United States District Court,
D. Delaware.

**PRISM TECHNOLOGIES LLC,**
Plaintiff.
v.
**VERISIGN, INC., RSA Security, Inc., Netegrity, Inc., Computer Associates International, Inc., and Johnson & Johnson Services, Inc,**
Defendants.

Civil Action No. 05-214-JJF

**April 2, 2007.**

**Background:** Patent holder brought action for infringement of patent on subscription access security system for use with untrusted computer networks.

**Holdings:** After Markman hearing, the District Court, Joseph J. Farnan, J., held that:
(1) the patent did not anticipate that all subscribers would pay for access to protected content;
(2) "operating session" was period of communication between the subscriber client computer and the first server computer that followed successful initial authentication and ended upon termination of authorized access;
(3) hardware key connected to the subscriber client computer was external hardware device;
(4) "subscriber client computer" was computer that subscriber used to access selected computer resources of the first server computer;
(5) "adapted to" language in claim that subscriber client computers were adapted to forward identity data to first server computer did more than precede the recited function and was a part of the recited function;
(6) means-plus-function interpretation did not apply to the phrase "at the beginning of an operation session in which access to selected computer resources is requested"; and
(7) claim of method of controlling access to selected computer resources comprising the steps of the claimed elements, including clearinghouse means, did not state means-plus-function or a step-plus-function limitation.

Ordered accordingly.

6,516,416. Construed.

Dirk D. Thomas, Robert A. Auchter, Jason R. Buratti, Andre J. Bahou, and Chandran B. Iyer, of Robbins, Kaplan, Miller & Ciresi, L.L.P., Washington D.C., Richard D. Kirk, Ashley B. Stitzer, of The Bayard Firm, Wilmington, DE, for Plaintiff.

Edward F. Mannino, Jason A. Snyderman, John D. Simmons, Akin Gump Strauss Hauer & Feld LLP,

Philadelphia, PA, Frank C. Cimino, Daniel E. Yonan, Akin Gump Strauss Hauer & Feld LLP, Washington, D.C., Patricia Smink Rogowski, Connoly Bove Lodge & Hutz LLP, Wilmington, DE, for Defendant VeriSign, Inc.

William F. Lee, David B. Bassett, Mark D. Selwyn, Gregory P. Teran, Wilmer Cutler Pickering Hale and Dorr LLP, Boston, MA, Frederick L. Cottrell, III, Steven J. Fineman of Richards, Layton & Finger, P.A., Wilmington, DE, for Defendant RSA Security Inc.

David M. Schlitz, Esquire of Baker Botts L.L.P., Washington D.C., Samir A. Bhavsar, Esquire and Jeffery D. Baxter, Esquire of Baker Botts L.L.P., Dallas, TX, Richard L. Horowitz, Esquire, and David E. Moore, Esquire of Potter Anderson & Corroon LLP, Wilmington, DE, for Defendant Netegrity, Inc. and Computer Associates International.

John M. DiMatteo, Esquire, Neal K. Feivelson, Esquire and Leslie M. Spencer, Esquire of Willkie Farr & Gallagher, New York, NY, Steven J. Balick, Esquire, John G. Day, Esquire and Tiffany Geyer Lydon, Esquire of Ashby & Geddes, Wilmington, DE, for Defendant Johnson & Johnson Services, Inc.

***MEMORANDUM OPINION***

JOSEPH J. FARNAN**, District Judge.**

This action was brought by Plaintiff, Prism Technologies, LLC ("Plaintiff") against Defendants Verisign, Inc., RSA Security Inc., Netegrity, Inc., Computer Associates International, Inc., and Johnson & Johnson Services, Inc. (collectively "Defendants") alleging infringement of United States Patent No. 6,516,416 (the "'416 Patent"). The parties briefed their respective positions on claim construction, and the Court conducted a Markman hearing on November 9, 2006 regarding the disputed terms in the '416 Patent. This MemorandumOpinion presents the Court's construction of the disputed terms.

## I. Preliminary Matters

Following the Markman Hearing, Plaintiff moved this Court to allow supplementation of the hearing record. (D.I.376). Plaintiff sought to introduce an expert declaration to counter allegedly new arguments presented by Defendants at the hearing. The Court finds that Defendants did not adopt new positions for the affected terms. Accordingly, Plaintiff's Motion For Leave To Supplement The Markman Hearing Record (D.I.376) will be denied.

## II. Background

The patent-in-suit relates to a subscription access security system for use with untrusted computer networks. The patented system provides secure access, subscriber and server authentication, subscriber usage tracking, and information rights management. The system seeks to solve problems such as how to generate revenue when users access content on untrusted networks, and how to protect information rights.

## III. Legal Standard

### A. *General Claim Construction Principles*

Claim construction is a question of law. Markman v. Westview Instruments, Inc., 52 F.3d 967, 977-78 (Fed.Cir.1995), *aff'd,* 517 U.S. 370, 388-90, 116 S.Ct. 1384, 134 L.Ed.2d 577 (1996). When construing the claims of a patent, a court considers the literal language of the claim, the patent specification and the prosecution history. Markman, 52 F.3d at 979. Of these sources, the specification is considered the single best guide for discerning the meaning of a claim. Phillips v. AWH Corporation, 415 F.3d 1303, 1312-1317 (Fed.Cir.2005).

[1] A court may consider extrinsic evidence, including expert and inventor testimony, dictionaries, and learned treatises, in order to assist it in understanding the underlying technology, the meaning of terms to one skilled in the art and how the invention works. Phillips, 415 F.3d at 1318-19; Markman, 52 F.3d at 979-80 (citations omitted). However, extrinsic evidence is considered less reliable and less useful in claim construction than the patent and its prosecution history. Phillips, 415 F.3d at 1318-319 (discussing "flaws" inherent in extrinsic evidence and noting that extrinsic evidence "is unlikely to result in a reliable interpretation of a patent claim scope unless considered in the context of intrinsic evidence").

[2] [3] In addition to these fundamental claim construction principles, a court should also interpret the language in a claim by applying the ordinary and accustomed meaning of the words in the claim. Envirotech Corp. v. Al George, Inc., 730 F.2d 753, 759 (Fed.Cir.1984). If the patent inventor clearly supplies a different meaning, however, then the claim should be interpreted according to the meaning supplied by the inventor. Markman, 52 F.3d at 980 (noting that patentee is free to be his own lexicographer, but emphasizing that any special definitions given to words must be clearly set forth in patent). If possible, claims should be construed to uphold validity. In re Yamamoto, 740 F.2d 1569, 1571 & n. * (Fed.Cir.1984) (citations omitted).

**B.** ***Claim Construction Of Means-Plus-Function and Step-Plus-Function Claim Elements***

[4] Under 35 U.S.C. s. 112, para. 6, a claim limitation may be expressed as a "means or step for performing a specified function without the recital of structure, material, or acts in support thereof." 35 U.S.C. s. 112, para. 6. When interpreting claims expressed in this manner, "structure" and "material" are associated with means-plus-function claim limitations, whereas "acts" or "steps" are associated with step-plus-function claim limitations. Seal-Flex, Inc. v. Athletic Track & Court Constr., 172 F.3d 836, 843 (Fed.Cir.1999) (citing O.I. Corp. v. Tekmar Co. Inc., 115 F.3d 1576, 1583 (Fed.Cir.1997)).

[5] [6] [7] In determining whether a claim element is subject to Section 112, para. 6, a court considers the phrasing of the element. Use of the word "means" creates the presumptions that a claim is employing means-plus-function language, and therefore, that Section 112, para. 6 applies. Its absence creates a presumption to the contrary. Mas-Hamilton Group v. LaGard, Inc., 156 F.3d 1206, 1213 (Fed.Cir.1998). In the context of step-plus-function limitations, the same can be said if the element includes the word "step for." St. Clair Intellectual Prop. Consultatns, Inc. v. Canon Inc., 2004 WL 1941340, *10, 2004 U.S. Dist. LEXIS 17489 at (D.Del.2004)(citing Seal-Flex, Inc. v. Athletic Track & Ct. Constr., 172 F.3d 836, 849 (Fed.Cir.1999)). A presumption that Section 112, para. 6 applies can be overcome by showing that (1) there is no corresponding function for the "means" or (2) the claim recites sufficient structure, material, or acts to perform the function. Sage Prods. v. Devon Indus., 126 F.3d 1420, 1427-28 (Fed.Cir.1997).

[8] [9] If Section 112, para. 6 does apply, a court must first determine the function that is being performed, "staying true to the claim language and the limitations expressly recited by the claims." Omega Eng'g v. Raytek Corp., 334 F.3d 1314, 1322 (Fed.Cir.2003). Second, a court must determine what structure, material,

or acts provided in the written description correspond to the function performed. Id. A claim governed by section 112, para. 6 does not encompass every structure, material, or act that can possibly perform the specified function. Laitram Corp. v. Rexnord, 939 F.2d 1533, 1535 (Fed.Cir.1991). Rather, the limitation must be construed to cover the "corresponding structure, material, or acts described in the specification and equivalents thereof." 35 U.S.C. s. 112, para. 6; Odetics, Inc. v. Storage Tech. Corp., 185 F.3d 1259, 1266-67 (Fed.Cir.1999). The claim limitation covers only the structure, material, or acts necessary to perform the function. Omega Eng'g, 334 F.3d at 1322 (Fed.Cir.2003).

**IV. The Meanings Of The Disputed Terms In The** '416 Patent

Though Plaintiff asserts that Defendants infringe independent claims 1 and 24 and dependent claims 4, 5, 15, 16, and 25 of the '416 Patent, the terms that the Court must construe all appear in independent claims 1 and 24. In full, with disputed terms and phrases emphasized, these claims recite:

1. A system for controlling the operation of and access to selected computer resources of at least a *first server computer* by at least one *subscriber client computer* via an *untrusted network* in an *operating session,* without necessarily controlling access to other computer resources provided by the *first server computer* and by other server computers and nonsubscriber client computers, comprising:

*clearinghouse means* for storing identity data of said *first server computer* and the *identity data of each of said subscriber client computers;*

*server software means* installed on said *first server computer adapted to forward its identity data* and *identity data* of each *subscriber client computer* to said *clearinghouse means* at the beginning of an *operating session* in which access to selected computer resources of said *first server computer* is requested;

*client software means* installed on each of said *subscriber client computers adapted to forward its identity data* to said *first server computer* at the beginning of an *operating session* in which access to selected computer resources is requested;

at least one *hardware key* connected to the *subscriber client computer,* said key being adapted to generate a *predetermined digital identification,* which identification is *part of said identity data;*

said *server software means* installed on the *first server computer* being adapted to selectively request the *subscriber client computer* to forward said *predetermined digital identification* to the *first server computer to thereby confirm that said hardware key is connected to said subscriber client computer;*

said *clearinghouse means* being adapted to authenticate the identity of said *subscriber client computer* responsive to a request for selected computer resources of said *first server computer* by a subscriber client computer;

said *clearinghouse means* being adapted to authenticate the identity of said *first server computer* responsive to said *subscriber client computer* making the request for selected computer resources of said *first server computer;* and,

said *clearinghouse means* being adapted to permit access to said selected computer resources responsive to successful initial authentication of said *first server computer* and of said *subscriber client computer* making

first [sic] request.

24. A method of controlling access to selected computer resources of at least a *first server computer* by at least one *subscriber client computer* via an *untrusted network* during an *operating session,* without necessarily controlling access to other computer resources provided by the *first server computer* and by other server computers and nonsubscriber client computers, comprising the steps of:

registering *identity data* of said *first server computer* and the *identity data of each of said subscriber client computers* and storing the registered *identity data* in a *clearinghouse means* associated with said *first server computer* and said *subscriber client computers;*

requiring a *subscriber client computer* to forward its *identity data* to said *clearinghouse means* at the beginning of an *operating session* in which access to selected computer resources is requested;

requiring a subscriber client computer to forward a *predetermined digital identification* to said *first server computer to thereby confirm that a hardware key is connected to said subscriber client computer;*

attempting to authenticate the identity of said *subscriber client computer* from said *clearinghouse means* responsive to a request for selected computer resources of said *first server computer* by a *subscriber client computer;*

attempting to authenticate the identity of said *first server computer* from said *clearinghouse means* responsive to said *subscriber client computer* making the request for selected computer resources; and,

*permitting access* to said selected computer resources responsive to successful initial authentication of said *first server computer* and of said *subscriber client computer* making said request.

('415 Patent, col. 35, line 25-col. 26, line 2; col. 28, lines 36-67).

The parties have agreed upon definitions, which the Court adopts, for the following terms:

**"Authenticate"** means "to determine that something is, in fact, what it purports to be" (D.I.207, pg.20); **"Adapted to forward"** means "capable of transmitting" ( Id. at pg. 22); **"Requiring ... to forward"** means "requiring that certain information be transmitted" ( Id.); and **"Its" in the context of "its identity data"** has two meanings: the first occurrence of "its," in Column 35, line 36, refers to the identity data of a first server computer and the second occurrence of "its," in Column 35, line 42, refers to the identity data of a subscriber client computer. ( Id. at pg. 24).

For the reasons that follow, the Court construes the disputed terms and phrases as follows:

**A. Untrusted Network**

[10] The parties agree that the patentee explicitly defined the term "untrusted network" in the specification of the '416 Patent. However, they disagree as to whether the patentee's definition comprises one or two sentences. The relevant part of the specification reads:

As used herein, an untrusted network is defined as a public network with no controlling organization, with

the path to access the network being undefined and the user being anonymous. A client-server application running over such a network has no control over the transmitted information during all the phases of transmission.

('416 Patent, col. 3, ll. 59-64). Plaintiff contends that "untrusted network" is defined by only the first sentence, whereas Defendants contend that the patentee intended "untrusted network" to be defined by both sentences. (D.I. 266, pg. 25; D.I. 305, pg. 26; D.I. 268, pg. 39; D.I. 306, pg. 17). Defendants contend that the patentee clearly intended to limit the scope of the term "untrusted network" to "control" over transmitted information, and that desired scope is only apparent when both sentences are read together. (D.I. 268 at 39).

After reviewing the claim language and the specification, the Court concludes that the second sentence explains how an untrusted network acts upon a client-server application, while the first sentence contains the patentee's definition of the term. Accordingly, the Court agrees with Plaintiff, and construes "untrusted network" to mean "a public network with no controlling organization, with the path to access the network being undefined and the user being anonymous."

**B. Subscriber**

[11] Defendants contend that because the claims distinguish between "subscriber client computers" and "non-subscriber client computers," thereby describing some users as subscribers, and some users as non-subscribers, the terms "user" and "subscriber" cannot, as Plaintiff contends, be interchangeable. Moreover, Defendants contend that payment for access to content is a necessary component of the invention, noting that "a prominent feature of the system of the present invention is that it provides a secure platform [to publish protected resources] in a way that assures revenue generation." (D.I. 268 at 20 citing '416 Patent, col. 35, ll. 10-14.). Therefore, Defendants contend, the patent teaches that information providers only provide information to subscribers who pay for access to the content, and deny that right to all other users. (D.I. 268 at 20).

Plaintiff acknowledges that the '416 Patent provides the possibility that information providers could collect payment from those who seek access to the providers' content. However, Plaintiff contends, collecting fees is not a requirement of the patent, and a user does not become a subscriber only upon paying for access to providers' content. Rather, Plaintiff contends, the terms "subscriber" and "user" are used interchangeably throughout the specification and drawings to refer to someone who has applied, and been approved, to access protected content, with or without paying a fee to do so. (D.I. 266, citing '416 Patent col. 1, ll. 63-67, col. 7, ll. 48-53, and Figs. 3, 17, 18).

After reviewing the term "subscriber" in the context of the specification and other claims, the Court agrees with Plaintiff that the '416 Patent does not anticipate that all subscribers pay for access to protected content. FN1 The opening paragraphs of the specification suggest that one function of a subscription access system is to help generate revenue, as Defendants point out. (' 416 Patent, col. 1, l. 13). However, there are other functions, such as to provide protection of information assets. ( Id., col. 1, ll. 13-15).

FN1. The parties have submitted definitions for the word "user" and "subscriber" from various dictionaries. However, because the Court concludes that the meaning of "subscriber" can be sufficiently construed from the intrinsic evidence, it will not consider which party's dictionary of choice is most appropriate.

Also, the specification never requires that the invention be associated with generating revenue, even though the invention provides for such a possibility. ( Id. at col. 4, l. 4-5). The specification teaches that each information provider establishes its *own* criteria for accepting subscribers, and that some possible prerequisites can include "things like collecting payment, demographic checks, etc." ( Id. at col. 14, ll. 43-44). While it does provide this list of possible criteria, the specification never requires information providers to include any particular prerequisites for their subscribers.

Moreover, it appears that the patentee intended the terms "user" and "subscriber" to have the same meaning throughout the patent. For example, Column 8, lines 30-33 read: "The functions in the shared object 66 insures that the *subscriber* is operating as a valid session. If it is not a valid session, the functions redirect the *user* to the login process so that a new session can be created for the *subscriber*." ('416 Patent, col. 8, ll. 30-33)(emphasis added). The Court's interpretation does not imply that "subscribers" are synonymous with *any* computer user. Rather, the Court's reading of the terms "subscriber" and "user" is consistent with the patent specification in distinguishing those who are allowed access to protected content, whether they paid for that access or not, (subscribers/users of the system) from those who are not allowed to access protected content (non-subscribers, who do not use the system).

**C. First Server Computer and the "Selected Computer Resources of at least a [or said] first server computer ..."**

[12] Plaintiff contends that the first server computer, or "subscription access server," does not need to actually store all of the selected computer resources it makes available to subscribers. Rather, Plaintiff contends, the first server computer can act as a gatekeeper, controlling access to those resources by instructing a "Service Function" to make those services, applications or content available. (D.I. 266 at 27; D.I. 305 at 17-18).

Defendants contend that the claim language and specification of the '416 Patent require that the first server computer physically store all of the protected content it communicates to subscribers, pointing to language in the specification stating that the invention "control[s] access to selected computer resources *of* at least a first server computer." (D.I. 306 at 20, citing '416 Patent, col. 35, ll. 26, 29-31)(emphasis added). Defendants contend that the use of the word "of" implies possession of resources by the first server. ( Id. at 20). However, reading the claim in the context of the entire patent, the Court concludes that Defendants' contentions rely on an overly restrictive concept of possession, and that, given a broader reading, the language cited by Defendants is consistent with the specification.

The specification discusses a system whereby various web sites are hosted through web servers operating in conjunction with first server computers that protect the contents of the sites. ( *See e.g.* col. 5, ll. 14-16, col. 27, ll. 3-4). Figure 3 shows the protected contents residing outside of the first server computer, with the path over which protected contents can be sent crossing through the "Service Function" block rather than the server. ( Id., Fig. 3). Likewise, in Figure 4, the protected content resides outside the first server, and is accessed by the server through the "Service Function," which also resides outside the first server computer. ( Id., Fig. 4). Thus, the Court concludes that the system disclosed in the specification and corresponding figures does not require the first server computer to store the resources it communicates to subscribers. Rather, it allows the server to act as a gatekeeper, accessing selected computer resources protected by the invention either itself or through a "Service Function" block, and communicating those resources to subscribers.

[13] Accordingly, the Court construes "First Server Computer" to mean "a computer that makes available information or other resources." The Court also construes "selected computer resources of at least a [or said] first server computer" to mean "computer services, applications, or content that can be accessed by (either directly or indirectly) said first server computer."

**D. Operating Session**

[14] The parties agrees that the term "operating session" refers to communications between the subscriber client computer and the server. Their main point of disagreement is over when it begins and ends.

Plaintiff contends that the language of Claims 1 and 24 provides that an operating session begins when the subscriber client computer's identity data is forwarded to the clearinghouse. (D.I.266, pg.27). Plaintiff contends that a subscriber is authenticated during an operating session, and authentication cannot be completed without identity data. Id. Plaintiff further contends that the inventors intended "beginning" to have its conventional meaning of "the time or place of starting." ( Id. citing *Webster's New Twentieth Century Dictionary* (1983)).

Defendants contend that Plaintiff's proposed construction is overly broad, in that an "operating session" would inappropriately cover communications that never result in a successful log in or never grant access to the requested protected content. (D.I.268). Defendants point to the patent abstract, which states that user/subscriber authentication is completed before an operating session occurs. ( *See* '416 Patent, Abstract). Defendants note that the patent uses the terms "operating session" interchangeably with the terms "session" and "active session," to discuss something that is not started until after successful authentication. (D.I. 268, pg. 18-19 citing '416 Patent 7:48-53, 8:27-30, 10:17-21 and Figs. 17, 18). Finally, Defendants contend that an "operating session" ends when the user logs off or when the website forcibly logs the user off for lack of use. *Id*. at 19:26-37 and Figs 20, 22.

Reviewing the claim language in light of the specification, the Court concludes that "Operating Session" means "a period of communication between the subscriber client computer and the first server computer that follows successful initial authentication and ends upon termination of authorized access, such as upon a log-out or time-out due to prolonged inactivity."

Plaintiff does not contest Defendants' assertion that "session" and "active session" are used synonymously throughout the specification to refer to what the claim language calls an "operating session." Instead, Plaintiff relies upon Figure 18 to support its position that an operating session begins when identity data is transmitted during a login attempt. (D.I.207, pg.19). However, the description of Figure 18 refers to login, authentication and session initiation as three distinct, sequential, phases of a single process. ('416 Patent, 3:20-22). Moreover, the figure details that a user must input its identity data, which is encrypted before being sent to the login enforcer. The login enforcer then sends the encrypted identity data and an "Initiate Session" message to the Session Initiator. ('416 Patent, Fig. 18). At this point, with no session yet begun, the Session Initiator sends an "authenticate login" message to the clearinghouse, and the clearinghouse authenticates the login parameters. Id. It is only after the user's login parameters are authenticated that the "User Authentication Server" sends a successful "Authentication Response" to the Session Initiator, prompting the Session Initiator to create a new active session with a unique session ID. Id. Moreover, the specification states several times, "[i]f the login is successful, the subscription access server initiates a session[.]" ('416 Patent, col 7, ll. 48-53; *see also* Abstract("The clearinghouse authenticates the subscriber and server computers before an operating session begins."), col, 5, ll. 21-22 ("A session manager is provided

which builds sessions for every valid subscriber"), col. 8 ll. 27-30 ("When the CGIs get the login parameters sent by the subscriber software, they send a request to the session manager to authenticate the subscriber and start a new session."), col. 13, ll. 42-53 and col. 17, ll. 45-50). Further, the invention has several features, such as the usage server and the URL tracking server, that are set to track what protected content is visited during an active session, so that information providers can keep a record of how, when, and how often users are accessing the information that has been made available to them. (See e.g. '416 Patent, col. 4, ll. 55-59).

Therefore, in light of the process described in Figure 18, the language of the specification, and the described purpose of the operating session, the Court disagrees with Plaintiff that an "operating session" includes the transmission of identity data. Moreover, Plaintiff does not dispute that an operating session ends when a user is no longer authorized to access protected content. Accordingly, the Court concludes that an operating session follows successful initiation, and ends upon termination of authorized access.

**E. Hardware Key and Connected**

[15] Claim 1 recites that the invention is comprised of "at least one hardware key connected to the subscriber client computer," and Claims 1 and 24 require that the subscriber client computer "forward [a] predetermined digital identification to [the] first server computer to thereby confirm that [the] hardware key is connected to said subscriber client computer." The parties agree that "hardware key" is used synonymously with the terms "access key" and "hardware access key" in the specification. (D.I. 266 at 27, D.I. 268 at 7). However, they disagree over whether the specification uses the term "connected" interchangeably with "attached."

Plaintiff contends that the hardware key does not need to be an external device, but could also be built into the subscriber client computer. Plaintiff further contends that "connected," as used in the '416 Patent, means only that the access key interface can read the digital ID from the access key. Plaintiff contends that the patent does not require any specific kind of connection between the hardware key and the access key interface.

Defendants contend that a "hardware key connected to the subscriber client computer," as used in the context of the specification, is an external device that physically attaches to the subscriber client computer. (D.I. 268 citing ' 416 Patent at col. 21, ll. 39-45, col. 7, ll. 61). They further argue that Plaintiff's proposed construction, that the hardware key can be built into the computer, would eliminate the need for the invention to verify the presence of the access key.

After reviewing the term "hardware key" in the context of the specification, the Court concludes that the specification requires that the hardware key be an external hardware device. ('416 Patent, col. 21, l. 40). The Court declines to adopt Plaintiff's proposal that the key can be built into the computer, because the "major function of the [hardware key] is to uniquely identify a user," and the specification teaches that the key should be something "which is known to have been assigned and given to a specific person." FN2 ( Id., col. 21, ll. 45-46, col. 22, ll. 4-5). A hardware key built in to a computer is computer-specific, not user-specific.

FN2. Plaintiff also supports its argument that the hardware key can be built into the computer by pointing to the following language in the specification: "Generally, two factor authentication provides that something is known, such as the name and password and something is held, such as the physical key that is attached to the computer, or built into the computer." (D.I. 266 at 28, citing '416 Patent, col. 21, ll. 49-53; *see also*

Transcript of Markman Hearing, held November 9, 2006 at Pg. 44, l. 5).

This sentence, however, is a general description of two-factor authentication. As such, the sentence explains to the reader of the patent that two factor authentication is comprised of something which is known and something which is either held or built into the computer. By using the descriptive phrase "such as the physical key that is attached to the computer," in this sentence, the patentee indicated that this invention uses the combination of something held and something known-the physical key attached to the computer that had been referenced throughout the paragraph. (See id., col. 21, l. 37-col. 22, l. 5).
[16] After reviewing the term "connected" in the context of the specification, the Court concludes that it is not synonymous with physical attachment. Though the invention's preferred embodiment involves a hardware key that is physically attached to the subscriber client computer via a port interface, the specification also lists acceptable alternatives to the preferred embodiment which need not be physically attached, including "a credit card, a key, an ATM card, or the like which is known to have been assigned and given to a specific person." ( Id., col. 22, ll. 1-5). Therefore, the Court finds that the specification anticipates hardware keys which are not physically attached.

Moreover, even though the inventors did not describe any embodiment of a hardware key that connects wirelessly to the computer, patent claims are not limited to only those features described in the specification, and later-developed technology is commonly allowed to be covered by broad claim terms. Varco, L.P. v. Pason Sys. USA Corp., 436 F.3d 1368, 1375-76 (Fed.Cir.2006)(citing SRI Int'l v. Matsushita Elec. Corp. Of Am., 775 F.2d 1107, 1121 (Fed.Cir.1985)("The law 'does not require than an applicant describe in his specification every conceivable and possible future embodiment of his invention.' ")( *en banc* )). Thus, wireless devices are anticipated by the broad language in the claims and specification. Accordingly, the Court construes "connected" to mean "in communication with, inserted in, or attached to."

**F. Predetermined Digital Identification**

[17] Plaintiff contends that the "predetermined digital identification" can be known in advance or calculated at the moment it is verified. Conversely, Defendants argue that the "predetermined digital identification" cannot be calculated at the moment because it must be a unique preassigned data string that cannot be shared with others. (D.I. 268 at 11).

Defendants base their contention on language in the specification calling for the "predetermined digital identification" to be microcoded onto a subscriber's hardware key. ( *See* '416 Patent, col. 6, ll. 54-55, col. 14, ll. 52-53). However, the language in Claims 1 and 24 does not require that the hardware key be microcoded with a "predetermined digital identification." Rather, Claim 1 refers to "at least one hardware key being *adapted to generate* a predetermined digital identification," with no specific limitation on when that information is generated. ('416 Patent, col. 35, ll. 47-48)(emphasis added). Moreover, Defendants' proposed construction would invalidate dependant claims 6 and 31, which each state that the first server computer can change the predetermined digital identification. ('416 Patent, col. 40, ll. 13-15).

In light of these considerations, and guided by the claim and specification language, the Court declines to import the specification limitation of microcoding into the claim language as Defendants' propose. Instead, the Court construes the term "predetermined digital identification" to mean "digital data whose value is known in advance or calculated at the moment."

**G. Subscriber Client Computer**

[18] Plaintiff contends that the inventors never intended the "Subscriber Client Computer" to be limited to just a personal computer. Rather, Plaintiff contends, the subscriber client computer encompasses "any programmable electronic device that is capable of running the client software means." (D.I. 207 pg. 21). Plaintiff further contends that the patent covers devices which have been invented since 1997 and that can perform the functions and steps defined in the asserted claims. Defendants contend that because the specification consistently describes the subscriber's computer as a "desktop" or personal computer, Plaintiff's proposed construction is inconsistent with the intrinsic evidence.

After reviewing the term "subscriber client computer" in the context of the specification and other claims, the Court agrees with Defendants, that the "subscriber client computer" described in the '416 Patent is not as broad as Plaintiff now proposes. Though nothing in the claim language requires the subscriber client computer to be a desktop computer, every description of the subscriber client computer suggests that it is a desktop personal computer or Macintosh. ('416 Patent col. 4, ll. 39-40, col. 5, ll. 35-40, col. 9, ll. 1-3, col. 14, ll. 57-58, 63-66, and Figs. 1 and 2). The repeated disclosure of using a personal computer, and corresponding figures, limit the "subscriber client computer" to "a computer that a subscriber uses to access selected computer resources of the first server computer." FN3

FN3. To the extent that Defendants may seek further clarification on the phrase "resources of the first server computer," as used in this construction, the Court would direct the parties to this Memorandum Opinion's earlier construction of "first server computer" and "selected resources of said [at least a] first server computer." The Court's construction of those terms applies here as well, and use of the phrase "resources of the first server computer" in no way suggests that the resources must be stored on the first server computer.

**H. "Identity Data" as it relates to the Subscriber Client Computer and "Part Of Said Identity Data"**

[19] The parties disagree about what the term "identity data" identifies as it relates to the Subscriber Client Computer, as well as the meaning of the word "part." Thus, the Court must construe each term.

Defendants contend that the "identity data" at issue must uniquely identify the subscriber client computer, not the subscriber, because the claim language refers to identity data "of" the subscriber client computer. After considering the claim language and the specification, the Court again concludes that Defendants' are restrictively reading the word "of." The term is not limited, as Defendants have argued, to the identity data that uniquely identifies the subscriber client computer. When discussed in the '416 Patent, the identity data of the subscriber client computer is that identity data which is transmitted by the subscriber client computer and used by the invention to verify the identity of the subscriber. ( *See generally* '416 Patent). Accordingly, the Court construes "Identity Data" as it relates to the Subscriber Client Computer to mean "data sufficient for the patented system to determine whether a person, organization, and/or computer is authentic and/or is entitled to assess said selected computer resources".

[20] The Court will next consider whether "part of said identity data" should be construed to encompass the entirety of the identity data or whether it must refer only to a subset of the identity data. Plaintiff contends that nothing in the '416 patent or prosecution history precludes the invention from using only the hardware key's predetermined digital identification to authenticate a user. Plaintiff contends that, when the claims refer to the predetermined digital identification as being "part" of the identity data, the claims anticipate that the predetermined digital identification could be combined with other information, or could be sufficient on its own, to authenticate a subscriber. The specification, however, reveals that Plaintiff's position is

inconsistent with the '416 Patent.

The '416 Patent discloses that the "identity data" needed to authenticate a subscriber depends upon the type of authentication scheme employed. The patent discloses that there can be one factor or two factor authentication. ( Id. at col. 1, ll. 60-61). When using one factor authentication, the identity data is the subscriber's username and password. Id. When using two-factor authentication, the "identity data" includes the predetermined digitalidentification from the hardware key. ( Id. at col. 1, ll. 61-63). Thus, the patent discloses that to successfully authenticate a subscriber under a one-factor scheme, that subscriber must correctly present a username and password, while successful authentication in a two-factor scheme requires the subscriber to present a username, password and the predetermined digital identification from a hardware key. Moreover, the patent never suggests the hardware key's predetermined digital identification alone could be enough to authenticate a subscriber. Rather, the specification makes clear that the optional hardware key is only used with two-factor authentication. ( Id. at col. 1, ll. 58-67). In those instances where the hardware key is used for authentication, it is always in the context of two-factor identification. ( *See* id. at col. 2, ll. 28-32, col. 3, ll. 45-47, col. 5, ll. 15-18, 50-55, col. 7, ll. 59-65, col. 13, ll. 44-46, col. 14, ll. 48-58, and col. 21, 45-49). Accordingly, the Court declines to construe "part of said identity data" as encompassing the entirety of the identity data, and instead construes it to mean "some, but not all, of the identity data of the subscriber client computer."

**I. "... to thereby confirm that said [or a] hardware key is connected to said subscriber client computer[.]"**

[21] The parties dispute when this phrase calls for the invention to confirm that the hardware key is connected to a subscriber client computer. Defendants propose that it occurs "after initial authentication, but before session termination," or, in other words, during re-authentication only. Plaintiff contends that the "to thereby confirm" limitations in claims 1 and 24 are broad enough to allow the hardware key's connection to be confirmed during both initial authentication and re-authentication.

As discussed in the preceding section of this Memorandum Opinion, the specification teaches that the "identity data" of the subscriber client computer is comprised of a subscriber's username, password and, in the case of two-factor identification, a hardware key's predetermined digital identification. ( Id. at col. 35, ll. 48-50). Per Claims 1 and 24, the first server computer is adapted to forward the "identity data" of the subscriber client computer "at the beginning of an operating session." ( Id. at col. 35, ll. 36-40). Consistent with the Court's construction of "operating session," once the identity data is confirmed, including confirmation that the hardware key is connected, an operating session begins. It therefore follows that the claim limitations requiring forwarding of the predetermined digital identification *during* an operating session do not read on initial authentication.

The '416 Patent describes that the invention initially authenticates subscribers, and then re-authenticates them throughout the operating session. Initial authentication occurs at login, and results in initiating an operating session. Re-authentication occurs after initial authentication but before the operating session terminates. Therefore, pursuant to the patent language and teachings, the phrase "to thereby confirm that said hardware key is connected to said subscriber client computer" only applies to the system's efforts to confirm that the hardware key is attached during re-authentication. Accordingly, the Court construes this phrase to mean "to verify after initial authentication, but before session termination, that the hardware key remains connected to the subscriber client computer."

**J. Permit[ing] access**

[22] Defendants have urged the Court to construe "permit[ing] access" as meaning"authorizing the use of," which they contend reflects the term's ordinary meaning in light of the specification. However, Defendants have not presented sufficient evidence to warrant departing from the claim language in favor of a synonym. Accordingly the court will construe "permit [ing] access" to mean "permitting the subscriber client computer to access said selected computer resources."

**K. Client Software Means**

The parties agree that "Client Software Means" is a means-plus-function element construed pursuant to 35 U.S.C. s. 112, para. 6. (D.I. 207, at 7). They disagree, however, about the scope of the function and the corresponding structure.

**1.** ***Scope of the Function***

[23] Under Section 112, para. 6, the Court must first determine what function is performed by the claim element. In making this determination, the Court must be careful to neither "narrow the scope of the function beyond the claim language" nor "broaden the scope of the claimed function by ignoring clear limitations in the claim language." Cardiac Pacemakers, Inc. v. St. Jude Med., Inc., 296 F.3d 1106, 1113 (Fed.Cir.2002). The parties disagree about two different parts of this element's functional scope. First, they disagree as to whether the language "adapted to" is part of the function. Second, they disagree about whether the function should be temporally limited.

As to the first dispute, Plaintiff contends that, by including the language "adapted to," the claim demands only a capability, not a requirement, to forward a subscriber client computer's identity data to a first server computer. (D.I. 266 at 12). Defendants contend that the "adapted to" language should be read out of the function, just as the word "for" would be in a conventional means-plus-function clause. (D.I. 306 at 2-3). The result of Defendants' proposed construction would be to require the client software means to forward a subscriber client computer's identity data to said first server computer. Id.

As to the second dispute, Plaintiff contends that the functional recitation is not temporally limited. While acknowledging that this element's language includes the phrase "at the beginning of an operating session in which access to selected computer resources is requested[,]" Plaintiff contends that this language is not a functional limitation of the element, and, therefore, should be subject to traditional claim construction principles rather than means-plus-function construction. (D.I. 266 at 7). Conversely, Defendants contend that the function must include the temporal limitations of the claim language to avoid improperly broadening the scope of the claimed function. (D.I. 266 at 30-32). They contend that the claimed function for "Client Software Means" is not forwarding the identity data at any time, but rather, forwarding the identity data at a particular time. Id.

[24] Often means-plus-function limitations are written as a "means for" performing a recited function. *See* Lucent Techs., Inc. v. Extreme Networks, Inc., 367 F.Supp.2d 649, 669 (D.Del.2005). Here, the applicants used the formulation "means adapted to" perform a recited function. The issue before the Court, then, is whether "adapted to" merely precedes the claimed function or whether it is a part of the claimed function. The Court agrees with Plaintiff that ignoring the "adapted to" language introduces an unintended requirement into the claim element, because the claim language only discloses a capability. *See* Berg Tech., Inc. v. Foxconn Int'l, Inc., 1999 WL 96414, **3-4, 1999 U.S.App. LEXIS 2796, at (Fed.Cir.1999) ("adapted

to" is commonly understood to mean "capable of"). Therefore, the "adapted to" language does more than precede the recited function; it is a part of the recited function.

[25] [26] A means-plus-function clause does not limit all terms in the clause to what is disclosed in the patent or equivalents. "[Section] 112, para. 6 applies only to interpretation of the means or step that performs a recited function when a claim recites insufficient structure or acts for performing the function." IMS Tech., Inc. v. Haas Automation, Inc., 206 F.3d 1422, 1432 (Fed.Cir.2000). In this case, the client software means is "adapted to forward the subscriber client computer's identity data to said first server computer at the beginning of an operating session in which access to selected computer resources is required." ( *See* '416 Patent, col. 256, line 42-45). The beginning of an operating session, however, is not the means or step for performing the data forwarding, and therefore, is not subject to Section 112, para. 6. Accordingly, the Court concludes that while "client software means" is a means-plus-function element, the means-plus-function interpretation does not apply to the phrase "at the beginning of an operation session in which access to selected computer resources is requested[.]"

Thus, the function performed is "adapted to forward a subscriber client computer's identity data to said first server computer." "At the beginning of an operating session in which access to selected computer resources is requested[,]" is not construed pursuant to 35 U.S.C. s. 112, para. 6, and is instead construed in accordance with the Court's previous construction of "operating session."

**2. *Corresponding Structure***

[27] Second, the Court must determine what structure corresponds to the claimed function. The parties disagree about the structure of the client software means, and the algorithm to be performed by that structure.FN4 The Court finds that the ' 416 Patent specification links the claimed function of the client software means to software products that were available at the time of the patent application. ('416 Patent at 5:48-50, 56-63). Therefore, the structure is that software identified in the specification that can carry out the function, namely "that portion of the identity and access components (e.g. that portion of the subscriber software running on the subscriber client computer (Fig.2)) that preferably uses the transmission control protocol/internet protocol (TCP/IP) and/or user datagram protocol/internet protocol (UDP/IP) to communicate with the first server computer and equivalents there of." ( *contra* McKesson Info. Solutions LLC v. TriZetto Group, Inc., 2006 WL 891048, *2, 2006 U.S. Dist. LEXIS 16097, at (D.Del.2006)) (structure limited to disclosed algorithm only because specification linked to software that did not exist at time of patenting).

FN4. The Court declines to define the exact algorithm disclosed in the specification, but notes that the client software means structure is limited to carrying out the algorithms described in the '416 patent. *See* WMS Gaming Inc. v. International Game Tech., 184 F.3d 1339 (Fed.Cir.1999).

**L. Server Software Means**

The parties agree that this claim element is a means-plus-function limitation governed by 35 U.S.C. s. 112, para. 6. The parties also agree that the element has two corresponding functions and structures. Consistent with its construction of "adapted to" and "at the beginning of an operating session in which access to selected computer resources of said first server computer is requested," the Court construes this claim element as follows:

**1.** ***First Function and Corresponding Structure***

[28] The first function is "adapted to forward the first server computer's identity data and identity data of each subscriber client computer to said clearinghouse means." The corresponding structure is "that portion of the identity and access management components (e.g. software running on the server 34 (Fig.2)) that preferably uses the transmission control protocol/internet protocol (TCP/IP) and/or user datagram protocol/internet protocol (UDP/IP) to communicate with the subscriber client computer and the clearinghouse 30 (Fig.2), and equivalents thereof."

**2.** ***Second Function and Corresponding Structure***

[29] The second function is "adapted to selectively request the subscriber client computer to forward said predetermined digital identification to the first server computer to thereby confirm that said hardware key is connected to said subscriber client computer." The corresponding structure is "that portion of the server software that selectively determines whether (e.g. upon a request for access to protected computer resources) to request the subscriber client computer to forward its digital identification to the first server computer to confirm the presence of a hardware key, and equivalents thereof."

**M. "Clearinghouse Means" In Claim 1**

The parties agree that this claim element, as it appears in Claim 1, is governed by 35 U.S.C. s. 112, para. 6. They also agree that four distinct functions are performed by the clearinghouse means, though they disagree over what those functions and corresponding structures are. The Court adopts the following constructions, consistent with its discussion about the language "adapted to" and the necessity of temporal limitations in the "client software means" subsection.

**1.** ***First Function and Corresponding Structure***

[30] The first function is "storing identity data of said first server computer and the identity data of each of said subscriber client computers." The corresponding structure is "a processor programmed to store the identity data of the first server computer and identity data of the subscriber client computer in a structured query language (SQL) database using an open database connectivity (ODBC) driver."

[31] Section 112, para. 6 allows patentees to express a limitation in their patent claims "as a means or a step for performing a specified function without the recital or structure ... in support thereof." 35 U.S.C. s. 112, para. 6. Plaintiff chose to employ this section when describing the "clearinghouse means" in Claim 1, resulting in a means-plus-function limitation. However, a consequence of choice is that scope of the means-plus-function limitation is limited to the "corresponding structure described in the specification and equivalents thereof." Genzyme Corp. v. Atrium Med. Corp., 212 F.Supp.2d 292, 302 (D.Del.2002) (citing J & M Corp. v. Harley-Davidson, Inc., 269 F.3d 1360, 1367 (Fed.Cir.2001)).

Plaintiff proposes that the corresponding structure to this first function is "any clearinghouse server(s) with the software capable of storing identity data and equivalents thereof." This construction, however, is much broader than the structure described in the specification. The specification describes a structured language query (SQL) database that can collect and store the identity data of the first server computer and subscriber client computers. ('416 Patent at Figs. 1, 3, and 4, col. 2, ll. 3-4, col. 4, ll. 50-52, and col. 6, ll. 61-65). It also describes that an open database connectivity (ODBC) driver is used so the clearinghouse means can communicate with other components of the invention. Id. Accordingly, the Court agrees with Defendants

that the corresponding structure for the first function is "processor(s) programmed to store the identity data of the first server computer and identity data of the subscriber client computer in a structured query language (SQL) database using an open database connectivity (ODBC) driver."

**2.** ***Second Function and Corresponding Structure***

[32] The second function is "adapted to authenticate the identity of said subscriber client computer," The corresponding structure is "that portion of the clearinghouse software (e.g. a user authentication daemon 58) which authenticates the subscriber client computer, and equivalents thereof."

**3.** ***Third Function and Corresponding Structure***

[33] The third function is "adapted to authenticate the identity of said first server computer." The corresponding structure is "that portion of the clearinghouse software" (e.g. a user authentication daemon 58) which authenticates the first server, and equivalents thereof.

**4.** ***Fourth Function and Corresponding Structure***

[34] The fourth function is "adapted to permit access to said selected computer resources." The corresponding structure is "that portion of the clearinghouse software which authenticates the first server and equivalents thereof".

**N. "Clearinghouse Means" in Claim 24**

[35] The parties disagree about the applicability of 35 U.S.C. s. 112, para. 6 to "clearinghouse means" as used in Claim 24. Defendants contend that the patentee's use of the word "means" clearly signals that the patentee intended this to be a means-plus-function clause. Under this theory, the word "means" gives rise to the presumption that Section 112, para. 6 applies to the claim element. Defendants further contend that Plaintiff cannot overcome this presumption, because the claim does not recite a function that corresponds with the clearinghouse means or a sufficiently definite structure for performing the function. Therefore, Defendants contend, Section 112, para. 6 applies to the claim element. Plaintiff contends that Claim 24 is a step-plus-function claim, not a means-plus-function claim, and under step-plus-function construction rules, Section 112, para. 6 is not presumed to apply.

The first question the Court must answer is whether Claim 24 invokes a means-plus-function limitation or a step-plus-function limitation, or neither. When interpreting section 112, para. 6, "structure" and "material" are associated with means-plus-function claims, whereas "acts" or "steps" are associated with step-plus-function claim elements. Seal-Flex, 172 F.3d at 843 (Fed.Cir.1999)(citing O.I. Corp. v. Tekmar Co. Inc., 115 F.3d 1576, 1583 (Fed.Cir.1997)).

Because Claim 24 claims "[a] method of controlling access ... comprising the steps of [the claimed elements, including clearinghouse means]," FN5 the Court is not persuadedby Defendants' argument that the mere presence of the word "means" makes this claim element a means-plus-function element. Instead, the Court agrees with Plaintiff that Claim 24 is a method claim, and considers the term "clearinghouse means" in Claim 24 to be little more than an "overzealous use" of the word means. *See* Genzyme, 212 F.Supp.2d at n. 10 (D.Del.2002). In light of this determination, Section 112, para. 6 could apply to this claim term only under the step-plus-function analysis.

FN5. Contrast this language with that of Claim 1, which claims "[a] system for controlling the operation of and access ... comprising [the claimed elements.]" ('416 Patent at Col. 35 ll. 25-30)

[36] [37] The second question the Court must answer is whether Claim 24 is written in step-plus-function format so as to invoke Section 112, para. 6. Generally, if a claim element includes the words "step for," it is presumed to be a step-plus-function limitation, and Section 112, para. 6 is presumed to apply. However, when the claim uses the word "step" alone, or "steps of," then Section 112, para. 6 is presumed not to apply to that element. St. Clair Intellectual Prop. Consultants, Inc. v. Canon Inc., 2004 WL 1941340, **25-26, 2004 U.S. Dist. LEXIS 17489 at *78 (citing Seal-Flex, 172 F.3d at 849 (Fed.Cir.1999)).

The first limitation of Claim 24 describes the step of "registering identity data ... in a clearinghouse means[.]" ('416 Patent at col. 38, ll. 42-46). The second limitation of Claim 24 describes the step of "requiring a subscriber client computer to forward its identity data to said clearinghouse means [.]" ( Id. at ll. 47-50). The fourth and fifth limitations of Claim 24 describe the steps of "attempting to authenticate the identity data [of a subscriber client computer and first server computer] ... from said clearinghouse means [.]" ( Id. at ll. 56-63). The Court concludes that none of these elements are written in step-plus-function format, because, (1) the language "step for" is not used, and (2) the limitations individually describe the precise acts required to control *access to* selected computer resources. Thus, Section 112, para. 6 does not apply to the term "clearinghouse means" as used in Claim 24.

[38] Having concluded that the use of the term "clearinghouse means" in Claim 24 invokes neither a means-plus-function limitation or step-plus function limitation, and therefore, concluding that Section 112, para. 6 does not apply, the Court adopts Plaintiff's proposed construction of "clearinghouse means" in Claim 24. Accordingly, "clearinghouse means" is construed to mean "any clearinghouse server(s) with software capable of storing and authenticating identity data."

**V. Conclusion**

For the reasons discussed, the Court has denied Plaintiff's Motion For Leave To Supplement The Markman Hearing Record (D.I.376) and construed the disputed terms and phrases of the patent-in-suit as provided herein. An Order consistent with this Memorandum Opinion will be entered setting forth the meaning of the disputed phrases in the patent-in-suit, and denying Plaintiff's Motion.

***ORDER***

At Wilmington, this *2* day of April 2007, for the reasons set forth in the Memorandum Opinion issued this date,

IT IS HEREBY ORDERED that:

1. Plaintiff's Motion For Leave To Supplement The Markman Hearing Record is ***DENIED.***

2. For the purposes of United States Patent No. 6,516,416, the following terms and phrases are construed as follows:

a. **"Untrusted Network"** is construed to mean "a public network with no controlling organization, with the path to access the network being undefined and the user being anonymous."

b. **"Subscriber"** is construed to mean "a person, organization, or computer registered to be allowed access to selected computer resources."

c. **"First Server Computer"** is construed to mean "a computer that makes available information or other resources."

d. **"Selected Computer Resources of at least a [or said] first server computer"** is construed to mean "computer services, applications, or content that can be accessed by (either directly or indirectly) said first server computer."

e. **"Operating Session"** is construed to mean "a period of communication between the subscriber client computer and the first server computer that follows successful initial authentication and ends upon termination of authorized access, such as upon a log-out or time-out due to prolonged inactivity."

f. **"Hardware Key"** is construed to mean "external hardware device or object from which the predetermined digital identification can be read."

g. **"Connected"** is construed to mean "in communication with, inserted in, or attached to."

h. **"Predetermined Digital Identification"** is construed to mean "digital data whose value is known in advance or calculated at the moment".

i. **"Subscriber Client Computer"** is construed to mean "a computer that a subscriber uses to access selected computer resources of the first server computer."

j. **"Identity Data" as it relates to the Subscriber Client Computer** is construed to mean "data sufficient for the patented system to determine whether a person, organization, and/or computer is authentic and/or is entitle to assess said selected computer resources."

k. **"Part Of Said Identity Data"** is construed to mean "some, but not all, of the identity data of the subscriber client computer."

l. **"To thereby confirm that said [or a] hardware key is connected to said subscriber client computer"** is construed to mean "to verify after initial authentication, but before session termination, that the hardware key remains connected to the subscriber client computer."

m. **"Permit[ing] Access"** is construed to mean "permitting the subscriber client computer to access said selected computer resources."

n. **Client Software Means** is a means plus function element construed pursuant to 35 U.S.C. s. 112, para. 6. The claimed function is "adapted to forward the subscriber client computer's identity data to said first server computer." The corresponding structure consists of that portion of the identity and access components (e.g. that portion of the subscriber software running on the subscriber client computer (Fig.2)) that preferably uses the transmission control protocol/internet protocol(TCP/IP) and/or user datagram protocol/internet protocol (UDP/IP) to communicate. The term "at the beginning of an operating session in which access to selected computer resources is requested" is not construed pursuant to 35 U.S.C., s. 112, para. 6, and is construed

consistent with the meaning of "operating session."

o. **"Server Software Means"** is a means plus function element construed pursuant to 35 U.S.C. s. 112, para. 6. It has two distinct functions and corresponding structures.

1. The first claimed function is "adapted to forward the first server computer's identity data and identity data of each subscriber client computer to said clearinghouse means." The first corresponding structure is "processor(s) programmed to store the identity data of the first server computer and identity data of the subscriber client computer in a structured query language (SQL) database using an open database connectivity (ODBC) driver."

2. The second claimed function is "adapted to selectively request the subscriber client computer to forward said predetermined digital identification to the first server computer to thereby confirm that said hardware key is connected to said subscriber client computer." The corresponding structure is "that portion of the server software that selectively determines whether (e.g. upon a request for access to protected computer resources) to request the subscriber client computer to forward its digital identification to the first server computer to confirm the presence of a hardware key, and equivalents thereof."

p. **"Clearinghouse Means" as used in Claim 1** is a means plus function element construed pursuant to 35 U.S.C. s. 112, para. 6. It has four distinct functions and corresponding structures.

1. The first claimed function is "storing identity data of said first server computer and the identity data of each of said subscriber client computers." The corresponding structure is "a processor programmed to store the identity data the first server computer in a structured query language (SQL) database using an open database connectivity (ODBC) driver."

2. The second claimed function is "adapted to authenticate the identity of said first server computer." The corresponding structure is "that portion of the clearinghouse software (e.g. a user authentication daemon 58) which authenticates the subscriber client computer, and equivalents thereof."

3. The third claimed function is "adapted to authenticate the identity of said first server computer." The corresponding structure is "that portion of the clearinghouse software" (e.g. a user authentication daemon 58) which authenticates the first server, and equivalents thereof.

4. The fourth function is "adapted to permit access to said selected computer resources." The corresponding structure is "that portion of the clearinghouse software which authenticates the first server and equivalents thereof".

q. **"Clearinghouse Means" as used in Claim 24** is not a means plus function element construed pursuant to 35 U.S.C. s. 112, para. 6. It is construed to mean "any clearinghouse server(s) with software capable of storing and authenticating identity data."

r. **"Authenticate"** is construed to mean "determine that something is, in fact, what it purports to be."

s. **"Adapted to forward"** is construed to mean "capable of transmitting."

t. **"Requiring ... to forward"** is construed to mean "requiring that certain information be transmitted."

u. **"It's" in the context of "its identity data"** is construed to refer to the identity data of a first server computer as the term appears in Column 35, line 36 of the '416 Patent, and is also construed to refer to the identity data of a subscriber client computer as the term appears in Column 35, line 42.