IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEBRASKA

PRISM TECHNOLOGIES, LLC, Plaintiff, v. McAFEE, INC.; SYMANTEC CORPORATION; and TREND MICRO INCORPORATED, Defendants.	)	8:10CV220 MEMORANDUM OPINION

In this case, plaintiff Prism Technologies, LLC ("Prism") alleges infringement of its patent, U.S. Patent No. 7,290,288 ("'288 patent"), by defendants. Defendants previously filed a motion for summary judgment of noninfringement (Filing No. 288), which the Court denied, without prejudice, because a second *Markman* hearing on disputed terms in the '288 patent had not yet been held and because adequate discovery had not yet occurred (Memorandum and Order, Filing No. 393). Since that time, the second *Markman* hearing was held on January 12, 2012, and discovery has closed.

This matter is now before the Court on new motions for summary judgment of noninfringement by defendants McAfee, Inc. ("McAfee") (Filing No. 871), Symantec Corporation ("Symantec") (Filing No. 868), and Trend Micro Incorporated ("Trend Micro") (Filing No. 849). In their motions, defendants seek to "dispose of this action" or at the very least "narrow the issues for

trial." The motions have been fully briefed (*see* Filing No. 955, at 5-6). After review of the motions, briefs, submitted evidence, and relevant law, the Court finds as follows.

I. Background and Procedural History.

The '288 patent, entitled "Method and System for Controlling Access, by an Authentication Server, to Protected Computer Resources Provided via an Internet Protocol Network," issued on October 30, 2007, from an application filed August 29, 2002 (Ex. 2, Filing No. 173) with the United States Patent and Trademark Office ("USPTO"). Prism contends that the '288 patent is a continuation-in-part of another Prism patent, U.S. Patent No. 6,516,416 ("'416 patent"), entitled "Subscription Access System for Use with an Untrusted Network," which issued on February 4, 2003, from an application filed June 11, 1997 (Ex. 3, Filing No. 173).

Prism filed its complaint in the present action on June 8, 2010 (Filing No. 1). The Court held a planning conference on November 30, 2010. At that time, the parties disputed the meaning of several of the claim terms in the '288 patent, but it was thought possible that the Court's construction of "hardware key"[1] might be dispositive of the case, making it unnecessary to construe the other disputed terms.

[1] The parties agree that "hardware key" and "access key" have the same meaning within the context of the '288 patent.

On April 11, 2011, the Court conducted the initial *Markman* hearing for the purpose of construing "hardware key." Subsequently, this Court construed "hardware key" to mean:

> An external hardware device or object from which the predetermined digital identification can be read.

(Filing No. 188, at 2).

After another hearing with the parties on July 21, 2011, it was determined that the construction of "hardware key" did not dispose of the issues in the case and that other terms in the '288 patent were still disputed. After the parties submitted additional claim construction briefs, the Court conducted a second *Markman* hearing on January 12, 2012, for the purpose of construing the additional disputed terms.

On January 20, 2012, after the second *Markman* hearing, the parties submitted a joint stipulation on claim construction, including an agreement as to the significance of claim preambles and as to the definitions of five claim terms (Filing No. 440). On February 14, 2012, the Court adopted the joint stipulation regarding the significance of the preambles and the construction of the five terms, and the Court construed the eight remaining disputed terms. In particular, the Court construed the term "digital identification" to mean "digital data whose value is known in advance or calculated at the moment" (Filing No. 469, at 11).

Each of the asserted claims of the '288 patent requires either a "hardware key" or an "access key." In this case, Prism claims that the hardware key for each defendant is a CD or DVD[2] (collectively, "CD"). Prism claims that for each defendant, two kinds of data could constitute the "digital identification" read from the hardware key.

First, each defendant's CD for a particular product contains digital information that is identical for that particular product, such as the SKU (stock-keeping unit) on McAfee's accused products. Prism alleges that the SKU distributed on McAfee's CDs "meet[s] the limitation of a digital identification that is read from the hardware key either literally or if not literally, under the doctrine of equivalents" (Filing No. 937, at 10, ¶ 16). Prism makes similar allegations for Symantec's CDs: Prism "alleges that the Vendor ID, Product ID and SKU ID . . . distributed on Symantec's accused CDs . . . literally meet the limitation of a 'digital identification' that is read from the hardware key" (Filing No. 933, at 9, ¶ 16). Likewise, for Trend Micro, Prism contends that the PID [product ID] distributed on the Trend Micro CD meets the limitation of "digital identification" (Filing No. 929, at 8, ¶ 13). The Court will refer to the digital information literally read from each

[2] In the case of McAfee, also a USB device (*see* Filing No. 937, at ¶ 15).

defendants' product CDs as described in this paragraph collectively as "SKU" data.

Second, Prism alleges that data that is created using an executable file from the CD as applied to a unique string of data from the client computer device itself also meets the limitation of a "digital identification." For example, Prism alleges that the "Machine ID used by McAfee's software meets the limitation of a 'digital identification'" (Filing No. 937, at 11, ¶ 30). While Prism also alleges that "the Machine ID is not strictly 'read' from the hardware key," nevertheless, Prism "alleges that the Machine ID would not exist but for the executable files responsible for generating the Machine ID that are, in fact, read directly from the hardware key" (*Id.*, at 11, ¶ 31). Prism makes similar allegations regarding Symantec's "machine fingerprint/ID" (Filing No. 933, at 10, ¶ 17) and Trend Micro's "GUID" (Filing No. 929, at 8, 9, ¶¶ 13, 16). The Court will refer to the unique information derived from the client computer device using an executable file read from each defendant's product CDs as described in this paragraph collectively as "Machine ID" data.

Finally, a third piece of data is relevant to defendants' motions, but this third piece is not alleged by Prism to constitute "digital identification." As Prism's expert, David Klausner, describes it for McAfee,

> During the activation process, the user of the client computer device is also required to type in a "CD Key" (also referred to as a "Product Key," "Activation Key," or "Serial Number"), which is a series of letters and/or numbers printed on a label that comes in the packaging of the McAfee software product. This CD Key data is also included in the activation request sent from the client computer device to McAfee's servers.

(Ex. 2, Filing No. 939, at 24). Likewise, Symantec's products require a "Product Key" (Ex. 3, Filing No. 934, at 22), and Trend Micro's products require a "Serial Number" (Ex. 1, Filing No. 930, at 39). The Court will refer to the information that is manually typed in by the user and is printed on a label on the packaging for each defendants' product CDs as described in this paragraph collectively as the "Serial Number." For each defendant, each Serial Number is unique.

During prosecution of the '288 patent, Prism attempted to add new claims (Claims 186 and 187) that did not include a hardware key or access key limitation (Filing No. 937 at 10, ¶ 26). By Examiner's Amendment and with approval from Prism via a telephone interview, the USPTO added the "access key" limitation back into the new claims (*Id.* at 11, ¶ 27). The examiner's March 23, 2007, statement of reasons for allowance of the '288 patent stated that "the cited prior art fails to teach or suggest a clearinghouse storing identity data of the server

computer, identity data of each client computer device, and authorization data associated with protected resources whereby the clearinghouse authorizes the client to access protected resources using the above noted stored data and the clearinghouse allowing access by the client to the protected resources stored on the server computer" (*Id.* at 17, ¶ 11).

II. Standard of Review - Summary Judgment.

Summary judgment is appropriate when, viewing the facts and inferences in the light most favorable to the nonmoving party, "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a); *see Celotex Corp. v. Catrett*, 477 U.S. 317, 321-23 (1986). "The inquiry performed is the threshold inquiry of determining whether there is the need for a trial -- whether, in other words, there are any genuine factual issues that properly can be resolved only by a finder of fact because they may reasonably be resolved in favor of either party." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 250 (1986). In a patent case, "[a]fter the claims at issue have reasonably been construed, a district court may grant summary judgment 'when it is shown that the infringement issue can be reasonably decided only in favor of the movant, when all reasonable factual inferences are drawn in favor of the non-movant.'" *Kraft Foods, Inc. v. Int'l Trading Co.*, 203 F.3d 1362, 1366 (Fed. Cir. 2000) (quoting *Voice Techs.*

Group, Inc. v. VMC Sys., Inc., 164 F.3d 605, 612 (Fed. Cir. 1999)).

III. Motions for Summary Judgment.

A. Direct, Literal Infringement. "[W]hoever without authority makes, uses, offers to sell, or sells any patented invention, within the United States or imports into the United States any patented invention during the term of the patent therefor, infringes the patent." 35 U.S.C. § 271. "An infringement analysis entails two steps. The first step is determining the meaning and scope of the patent claims asserted to be infringed. The second step is comparing the properly construed claims to the device accused of infringing." *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 976 (Fed. Cir. 1995), *aff'd*, 517 U.S. 370 (1996) (citations omitted). "It is a 'bedrock principle' of patent law that '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) (en banc) (quoting *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). "A claim is literally infringed when the accused device literally embodies each limitation of the claim." *Kraft Foods*, 203 F.3d at 1370. Having construed the disputed claim terms of the '288 patent (*see* Filing Nos. 188 and 469), the Court will now compare the construed claims to defendants' accused products.

In this case, Prism contends that each defendant infringes independent claim 87 (along with some of its dependent claims), claim 186, and claim 187. The Court will consider each in turn.

Claim 87 reads:

> 87. A method for protecting resources of a server computer, the server computer providing the protected resources to a client computer device via an untrusted network, without necessarily protecting other computer resources provided by the server computer and by other server computers to other client computer devices, the method comprising:
>
> storing (i) identity data of the client computer device having a hardware key and (ii) authorization data associated with the protected resources into a clearinghouse;
>
> generating a digital identification of the hardware key associated with the client computer device, the identity data of the client computer device comprising the digital identification;
>
> selectively requiring the client computer device to forward its identity data to the server computer;
>
> forwarding, by the client computer device, the identity data of the client computer device to the server computer;
>
> forwarding, by the server computer, the identity data of the client computer device to the clearinghouse;
>
> authenticating, by the clearinghouse, the identity of the client computer device responsive to the request for the protected resources of the server computer by the client computer device;

> authorizing, by the clearinghouse, the client computer device to receive the protected resources requested by the client computer device, based on the stored authorization data associated with the requested protected resources; and
>
> controlling, by the clearinghouse, access to the requested protected resources of the server computer responsive to successfully authenticating the client computer device making the request and responsive to successfully authorizing the client computer device.

('288 patent, 41:61-42:29). So claim 87 requires a hardware key from which the predetermined digital identification can be read. Prism maintains that the first two categories of digital data described above, the SKU and the Machine ID, constitute the claimed digital identification for each defendant.[3]

1. SKU Data. Claim 87 reads in part, "generating a digital identification of the hardware key associated with the client computer device, the identity data of the client computer comprising the digital identification" ('288 patent, 42:5-8). This Court has construed the term "identity data" to mean "data sufficient for the system to determine whether a person, organization, and/or computer is authentic and/or is entitled to access protected resources" (Filing No. 469, at 12-13).

In the context of claim construction of the term "identity data," Prism previously argued to this Court,

[3] *See* Filing No. 921, at 7, ¶¶ 6, 7, and 8.

> Claim 1 of the '288 patent, for example, recites "said at least one hardware key generating a digital identification, the identity data of said at least one client computer device comprising said digital identification." (['288 patent] at 35:8-10). Claims 31, 62, and 87 contain similar language of the client computer device's "identity data . . . comprising [said/the] digital identification." (*Id.* at 37:42-43, 39:60-62, 42:6-8). "In the patent claim context the term 'comprising' is well understood to mean 'including but not limited to.'" *CIAS, Inc. v. Alliance Gaming Corp.*, 504 F.3d 1356, 1360 (Fed. Cir. 2007). Thus, the claim language "the identity data . . . comprising said digital identification" means that the identity data must include the digital identification, and could include other items as well, but does not necessarily need to.

(Filing No. 309, at 27-28). Thereby Prism expressly acknowledged to this Court that the "identity data" term in Claim 87 requires the digital identification only (while it could be comprised of additional elements as well). This implies that the digital identification is capable of filling the role of the identity data, that is, of being "data sufficient for the system to determine whether a person, organization, and/or computer is authentic and/or is entitled to access protected resources."

In addition, in an earlier '288 patent case before this Court, Prism told the Court, "The authentication server determines whether or not a client computer device requesting

access to the protected computer resources is 'authentic' based upon a comparison of the digital identification associated with the client computer device to the digital identification stored in a database associated with the authentication server" (*Prism Techs. LLC v. Research in Motion*, 8:08CV537, Filing No. 76, at 8). There, Prism acknowledged that it is the digital identification, as a necessary component of the identity data, that is used in the comparison with the authentication server. So according to Prism's own reading of its patent, the digital identification identifies the client computer device for comparison with the database associated with the authentication server.

As this Court has written in its first claim construction order,

> The '288 patent's claims contemplate a comparison between the hardware key's digital identification and the authorization data stored on the clearinghouse database. See Claims 1, 31, 62, 87, 116, 117, 150, 185, 186, 187. If the hardware key's digital identification is not predetermined, then the authentication server would not be able to compare the hardware key's digital identification and the authorization data stored on the clearinghouse database. Without such a comparison, *authentication of the user's identity* would not be possible.

(Filing No. 188, at 10) (emphasis added). It follows that the digital identification itself, and not some other piece of data that is not read off the hardware key, must be compared to the authorization data to authenticate the user's identity. The specification of the '288 patent supports this understanding: "[T]he account holder authentication server accesses the account holder's information from its database and authenticates the login parameters. In using two or three factor authentication, this authentication involves the *comparison* of the digital ID" ('288 patent at 17:12-16 (emphasis added)). Also, "[T]wo factor authentication could be provided by some other physical device, such as 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.* at 19:50-53) (emphasis added).

Mr. Klausner states for each defendant, in a substantially similar fashion, (in this quotation, for McAfee),

> The SKU, Machine ID, and [Serial Number] data constitute data sufficient for the Anti-Piracy III system to determine whether the client computer device is entitled to activate the McAfee product installed on the client computer device. This data therefore constitutes the "identity data" of the client computer device, and includes digital identification generated from the product CD, DVD, or USB device.
>
> In reading the SKU and/or generating the Machine ID from the

> McAfee product [CD], McAfee's system is therefore "generating a digital identification of the hardware key associated with the client computer device, the identity data of the client computer device comprising the digital identification."

(Ex. 2, Filing No. 939, at 26-27; *see* for Symantec, Ex. 3, Filing No. 934, at 25 and for Trend Micro, Ex. 1, Filing No. 930, at 47-48). This is unlike the situation posited by Prism above, where the digital identification is the only ingredient of the identity data and therefore is integral to the determination of authenticity. Undoubtedly, if the manually-typed Serial Number and the Machine ID are added in as a part of the identity data, then the identity data contains data sufficient to identify the computer as authentic. In essence, then, the only function provided by what Prism purports to be the digital identification read from the defendants' CDs, the SKU, is to provide information about the product itself. But then the SKU has nothing to do with the *authentication of the user's identity*; rather, it has to do with the authentication of the *product's* identity, which is distinctly different.

The claims of the '416 patent include several of the same terms whose construction was disputed in the '288 patent. In previous litigation initiated in 2005 by Prism against other defendants (the "Delaware Case"), the United States District Court for the District of Delaware (the "Delaware Court")

construed the term "hardware key" in the context of the '416 patent to mean "external hardware device or object from which the predetermined digital identification can be read" (*Prism Tech. LLC v. Verisign, Inc.*, No. 05-214-JJF, Filing No. 449 (D. Del. Apr. 2, 2007), Ex. 6, Filing No. 173, at 3). This Court's construction for hardware key is identical to the construction given in the Delaware Case. In its brief opposing the present motions for summary judgment, Prism quotes itself from a statement to the Delaware Court in the Delaware Case:

> Moreover, nothing stated by the '416 patent inventors about their invention precludes the sharing of a hardware key amongst an authorized user group. *The hardware key need not identify anything other than itself*, and it can preferably (but not necessarily) be associated with a particular user or person. Once connected to a client computer device, and once the predetermined digital identification is read from the hardware key, *it identifies the client computer* that the subscriber happens to be using.

(Filing No. 1110, at 10) (emphasis added). But this statement only serves to show that the SKU data on defendants' CDs cannot possibly serve as the digital identification read from a hardware key, because the CD cannot "identify . . . itself." Rather, it can only place itself as a member of a group of hundreds or thousands of identical CDs with identical SKUs. Similarly, the SKU data on the CD cannot "identif[y] the client computer that

the subscriber happens to be using," because the SKU contains no information about the client computer.

In summary, the Court finds that the SKU data on each defendant's CDs cannot literally embody each limitation of claim 87, because the SKU cannot function as the required predetermined digital identification read from the hardware key. Accordingly, the Court finds that with regard to the SKU, the "infringement issue can be reasonably decided only in favor of the movant, when all reasonable factual inferences are drawn in favor of the non-movant."[4]

2. Machine ID. As required by the Court's construction of "hardware key," the "digital identification" must be read from the hardware key itself, not from somewhere else, such as the client computer. In the words of Prism's expert, Mr. Klausner, the '288 patent describes a hardware key that "*contains* a digital identification used to authenticate the device to the

[4] Trend Micro's brief in support of its motion for summary judgment for noninfringement (Filing No. 853) does not make this argument. However, in its brief in support of its motion for no induced infringement (Filing No. 1129), Trend first argues that there is no direct infringement for substantially the same reasons stated by McAfee and Symantec in their present motions. Furthermore, the original motion for summary judgment (Filing No. 288) and corresponding brief were submitted by Trend Micro on behalf of all defendants, and Trend Micro also made substantially the same arguments therein that are presented here. Accordingly, the Court will consider these arguments as having been submitted by all three defendants.

system" (Ex. 2, Filing No. 854, at 6, emphasis added).[5] In fact, according to Mr. Klausner, "when the client computer device sends a request over the network to access the protected resources, it forwards *a digital identification derived from the hardware key* as well as, in some cases, additional identifying information to the secure transaction server" (*Id.* at 7, emphasis added). In this way, Mr. Klausner differentiates between "digital identification" from the hardware key and "additional identifying information," which would not come from the hardware key. Mr. Klausner himself admits that the Machine ID is not read from the hardware key: "While this Machine ID is not strictly 'read' directly from the hardware key, . . ." (Ex. 2, Filing No. 939, at 26).

The Court finds that the Machine ID cannot constitute the "digital identification," since it is derived, using an executable file from the product CD, from unique digital information that resides on the client computer device, not the hardware key. In addition, the resulting Machine ID is not "read" from the hardware key any more than the manually-typed Serial Number. Thus defendants could not possibly infringe claim 87 with regard to the Machine ID of the client computer device as "digital identification," because the Machine ID is not literally

[5] This statement also supports the Court's conclusion that the digital identification is used for authentication and is not just a tag-along with other useful bits of identity data.

read from the hardware key, as required by the claim construction of hardware key.

In order to "protect[] resources of a server computer," as Claim 87's preamble recites, the method of Claim 87 would have to result in some limitation of the number of client computer devices that were able to access the protected resources. As Prism stated to the USPTO, "The challenge of [Prism's] application server to the clearinghouse is: ***Can this user or account holder have access to my selected resources?***" (Ex. 14, Filing No. 371, at 27). If the answer to Prism's question is always "yes," then Prism's invention serves no purpose at all. But defendants' ostensible hardware keys, the CDs associated with their software products, do not provide this access limitation. If the CD were all that was needed for access to a defendant's protected resources, then one enterprising pirate could easily buy one copy of a defendant's product and rent out the associated CD to every other resident of his college dormitory for a nominal fee, allowing each resident to access the defendant's protected resources at will.

For that reason, defendants do not guard against piracy of their protected resources by providing their customers with identical CDs that can be used by any number of non-paying interlopers. Rather, defendants protect their resources by issuing to each paying customer a predetermined Serial Number

that authenticates the identity of the customer's client computer device such that protected resources (in the form of software updates, say) are only sent to paying customers. The critical fact is that the Serial Number is not read from the CD; it resides on a label on the packaging of the product and is manually typed in by the customer. Therefore, it cannot constitute "digital identification," which must be read from a hardware key.

In this way, while the CD user does have access to the resources on the CD itself, that is, the initial version of the defendant's software product, the CD does not allow for access to the protected resources located on a server computer, such as updates to the software product. On the contrary,

> The accused systems use CDs only as a delivery mechanism for software – ***not*** as a security component. This is the exact opposite of the system contemplated by the patent, in which the hardware key is the security component, and the "protected content" is only to be delivered to the user's computer once the digital identification read from that hardware key authenticates the identity of the authorized user or the client computer.

(Filing No. 926, at 6 n.2).

Claims 186 ('288 patent, 50:34-67) and 187 ('288 patent, 51:1-52:16) fare no better, since each requires an access key, which is identical to a hardware key. For the same reasons

given above, the Court finds that defendants' product CDs cannot serve as an access key as required by claims 186 and 187. Accordingly, the Court finds that defendants do not literally, directly infringe the asserted claims of the '288 patent.

B. Doctrine of Equivalents. "Infringement under the doctrine of equivalents is a question of fact." *Kraft Foods*, 203 F.3d at 1371. But "[p]rosecution history estoppel as a limit on the doctrine of equivalents presents a question of law." *Glaxo Wellcome, Inc. v. Impax Laboratories, Inc.*, 356 F.3d 1348, 1351 (Fed. Cir. 2004).

1. Claims 186 and 187. Via the doctrine of equivalents, "a patent protects its holder against efforts of copyists to evade liability for infringement by making only insubstantial changes to a patented invention." *Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co.*, 535 U.S. 722, 727 (2002). "In some cases the Patent and Trademark Office (PTO) may have rejected an earlier version of the patent application on the ground that a claim does not meet a statutory requirement for patentability." *Id.* "When the patentee responds to the rejection by narrowing his claims, this prosecution history estops him from later arguing that the subject matter covered by the original, broader claim was nothing more than an equivalent." *Id.* "Competitors may rely on the estoppel to ensure that their own devices will not be found to infringe by equivalence." *Id.*

In particular, "A rejection [of a claim] indicates that the patent examiner does not believe the original claim could be patented." *Id.* at 734. "Estoppel arises when an amendment is made to secure the patent and the amendment narrows the patent's scope." *Id.* at 736. "A patentee who narrows a claim as a condition for obtaining a patent disavows his claim to the broader subject matter . . . . We must regard the patentee as having conceded an inability to claim the broader subject matter or at least as having abandoned his right to appeal a rejection. In either case estoppel may apply." *Id.* at 737.

"Prosecution history estoppel continues to be available as a defense to infringement, but if the patent holder demonstrates that an amendment required during prosecution had a purpose unrelated to patentability, a court must consider that purpose in order to decide whether an estoppel is precluded." *Warner-Jenkinson Co. v. Hilton Davis Chem. Co.*, 520 U.S. 17, 40-41 (1997). "Where the patent holder is unable to establish such a purpose, a court should presume that the purpose behind the required amendment is such that prosecution history estoppel would apply." *Id.* at 41. In addition, "the patentee should bear the burden of showing that the amendment does not surrender the particular equivalent in question." *Festo*, 535 U.S. at 740. "A patentee's decision to narrow his claims through amendment may be presumed to be a general disclaimer of the territory between the

original claim and the amended claim." *Id.* "[A]n amendment adding a new claim limitation constitutes a narrowing amendment that may give rise to an estoppel." *Honeywell Int'l Inc. v. Hamilton Sundstrand Corp.*, 370 F.3d 1131, 1141 (Fed. Cir. 2004).

During the prosecution of the '288 patent, Prism tried to add what would become claims 186 and 187 without the limitation of an access key. After the USPTO examiner added back in the access key limitations in an amendment, and Prism accepted the amendment, the new claims were allowed (*see* Ex. 5, Filing No. 876, at 5-6). Prism avers that the addition of the access key limitation does not constitute a narrowing amendment because claim 1 of the '288 patent contains a hardware key, and all the other claims of the '288 patent depend on claim 1, such that any new claim would already contain a hardware key/access key limitation. But McAfee persuasively argues,

> Prior to those amendments, the claims did not require that the "digital identification" be derived from an access key associated with the client computer. In other words, prior to the amendment, the claims were ambivalent as to the location from which the digital identification could be derived and read, and after amendment, the claims expressly required that the digital identification be derived and read from the hardware key. Thus, there can be no genuine dispute that these limitations narrowed the scope of claims 186 and 187.

(Filing No. 1078, at 29). The Court agrees that the access key amendments were narrowing.

The Court presumes that such narrowing amendments were made to facilitate patentability, and the burden is on Prism to rebut the presumption. Prism attempts to do so by citing the examiner's statement as to the "reasons for allowance" cited above, which does not mention the addition of the access key limitation (*see supra* pp. 6-7). Yet, as noted by Trend Micro, "Here, there can be no question that the amendments were made for purposes of patentability because the Examiner conditioned issuance of the patent on the applicant's acceptance of the amendments. (E.g., Ex. 12, p. 2 ('Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312.'))" (Filing No. 853, at 32). In addition, Trend Micro argues, "[A]s Prism itself later acknowledged, the Examiner's statement was an overview statement based only on 'claim 1 as a representative claim,' and was inaccurate as to the vast majority of claims" (Filing No. 1067, at 25, quoting Ex. 2, Filing No. 1066, at 2 (Applicant's "Comments on Statements of Reasons For Allowance."). "It was not intended to address all purportedly novel aspects of all 187 claims, and Prism in fact explicitly stated that it was not applicable to claims 186 or 187" (*Id.*).

The Court agrees that Prism has not met its burden of overcoming the presumption that the amendments including the limitation of an "access key" for claims 186 and 187 were made for purposes of patentability. Therefore, prosecution history estoppel applies to the "access key" limitation in claims 186 and 187.

2. Claim 87. "[S]ubject matter surrendered via claim amendments during prosecution is also relinquished for other claims containing the same limitation." *Glaxo*, 356 F.3d at 1356. "This court follows this rule to ensure consistent interpretation of the same claim terms in the same patent." *Id.* "[D]ifferent claims of a single patent should not be afforded different ranges of equivalents for the same claim term, 'absent an unmistakable indication to the contrary.'" *Id.* at 1356-57 (quoting *Am. Permahedge, Inc. v. Barcana, Inc.*, 105 F.3d 1441, 1446 (Fed. Cir. 1997)). Since "hardware key" and "access key" have the same meaning in the context of the '288 patent, following *Glaxo*, prosecution history estoppel also applies to the "hardware key" limitation in claim 87. Consequently, Prism is estopped from arguing that defendants have infringed the asserted claims under the '288 patent under the doctrine of equivalents as to the "hardware key" limitation.

IV. Conclusion.

When viewing the evidence in a light most favorable to the non-moving party, Prism, the Court finds that no reasonable jury could find that the CDs associated with defendants' products could constitute a "hardware key" or "access key" in the context of the '288 patent. Moreover, as a matter of law, Prism is estopped from asserting the doctrine of equivalents as to the "hardware key" limitation. Therefore, defendants' products do not infringe the '288 patent directly, jointly, or indirectly. For this reason, the Court will grant defendants' motions for summary judgment as to non-infringement. Because the Court finds that defendants do not infringe the '288 patent, the Court does not consider defendants' other issues as delineated in their motions. A separate order will be entered in accordance with this memorandum opinion.

DATED this 10th day of December, 2012.

BY THE COURT:

/s/ Lyle E. Strom

LYLE E. STROM, Senior Judge
United States District Court