Attorney Docket No. 077580-0090

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:	)	
Edmund Munger, et al.	)	
	)	
U.S. Patent No.: 7,188,180	)	
Filed: November 7, 2003	)	**Examiner:**
Issued: March 6, 2007	)	**Andrew L. Nalven**
	)	
For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	)	**Group Art Unit: 3992**
	)	
Reexamination Proceeding	)	
Control No.: 95/001,270	)	
Filed: December 8, 2009	)	

RESPONSE TO OFFICE ACTION IN REEXAMINATION

Mail Stop *INTER PARTES* REEXAM
Central Reexamination Unit
Office of Patent Legal Administration
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Patent Owner hereby responds to the Office Action dated January 19, 2010 ("the Office Action") in the Reexamination of the above-mentioned patent ("the '180 Patent") having a period of response set to expire on April 19, 2010 in view of the extension of time granted on February 25, 2010.

Remarks begin on page 2 of this response.

REMARKS

Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 of the '180 Patent are under reexamination, with claims 1, 17, and 33 being independent. Claims 1, 10, 12-15, 17, 26, 28-31, and 33 stand rejected. Claims 4, 20, and 35 are confirmed to be patentable.

Submitted herewith is a Declaration of Jason Nieh, Ph.D., Pursuant to 37 C.F.R. § 1.132 ("Nieh Dec.") in support of the Patent Owner's response.

I. Patent Owner's Response To the Rejection

A. Introduction

The Patent Owner's invention, as defined in independent claim 1, is directed to a method for accessing a secure computer network address. The method comprises the steps of: (*i*) receiving a secure domain name; (*ii*) sending a query message to a secure domain name service, the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name; (*iii*) receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and (*iv*) sending an access request message to the secure computer network address using a virtual private network communication link.

The patent provides a technique for establishing a virtual private network ("VPN") communication link between a first computer and a second computer over a computer network. '180 Patent at col. 49, ll. 57-59. To illustrate one non-limiting example, a client computer is connected to a computer network, such as the Internet. *Id.* at col. 50, ll. 1-4. The client computer connects to a server over a non-VPN communication link using a web browser to display a web page. *Id.* at col. 50, ll. 8-25.

According to one variation, the web page can contain a hyperlink for selecting a VPN communication link to the server. *Id.* at col. 50, ll. 25-31. By selecting the hyperlink, a client can secure the communication between itself and the server. *Id.* at col. 51, ll. 5-14. The user need only click the hyperlink – no need to enter user identification information, passwords, or encryption keys. *Id.* Accordingly, in this example, establishing a secure communication link between the user and server are performed transparently to a user. *Id.* To support this transparency, the technique disclosed in the '180 Patent provides for automatically replacing the

top-level domain name of the server within the web browser with a secure top-level domain name for the server. *Id.* at col. 51, ll. 15-28. For example, if the top-level domain name for the server is ".com," it may be replaced with ".scom". *Id.*

Because a secure top-level domain name can be a non-standard domain name, a query to a standard domain name system ("DNS") would return a message indicating that the universal resource locator ("URL") is unknown. *Id.* at col. 51, ll. 28-35. Therefore, according to the patent, the query can be sent to a secure domain name service for obtaining the URL for the secure top-level domain name. *Id.* The secure domain name service can contain a cross-reference database of secure domain names and corresponding secure network addresses. *Id.* at col. 52, ll. 4-26. That is, for each secure domain name, the secure domain name service stores a computer network address corresponding to the secure domain name. *Id.* An entity can register a secure domain name in the secure domain name service so that a user who desires a secure communication link to the web site of the entity can automatically obtain the secure computer network address for the secure website. *Id.* An entity can also register several secure domain names, with each respective secure domain name representing a different priority level of access to the secure website. *Id.*

For example, a securities trading website can provide users secure access so that a denial of service attack on the website will be ineffectual with respect to users subscribing to the secure website service. *Id.* Different levels of subscription can be arranged based on, for example, an escalating fee, so that a user can select a desired level of guarantee for connecting to the secure securities trading website. *Id.* When a user queries the secure domain name service for the secure computer network address for the securities trading website, the secure domain name service determines the particular secure computer network address based on the user's identity and the user's subscription level. *Id.*

B. Applicable Standards for Rejection

1. Applicable Standard for Rejection Under 35 U.S.C. § 102

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the '180 Patent stand rejected under 35 U.S.C. § 102. A rejection under 35 U.S.C. § 102 requires that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *See* MPEP § 2131, citing *Verdegaal Bros. v. Union Oil Col. of California*, 814 F.2d

628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The above-stated rejection, however, fails to meet this standard.

2. Applicable Standard for Rejection Under 35 U.S.C. § 103(a)

Claims 1, 10, 12-15, 17, 26, 28-31, and 33 of the '180 Patent also stand rejected under 35 U.S.C. § 103(a). In reconsidering the outstanding 35 U.S.C. § 103(a) rejections, the Examiner must consider any evidence supporting the patentability of the claimed invention, such as any evidence in the specification or any other evidence submitted by the Patent Owner, such as the secondary considerations of non-obviousness submitted herewith. The ultimate determination of patentability is based on the entire record, by a preponderance of evidence, which requires the evidence to be more convincing than the evidence which is sought in opposition to it. *See* MPEP § 2142 (citing *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992)).

Each of the rejections under 35 U.S.C. § 103(a) fails to meet these standards by a preponderance of the evidence.

3. Applicable Standard for Demonstrating a Publication Date

As identified below, a number of references have not been shown to qualify as prior art to the '180 Patent. The Office Action and the Request for *Inter Partes* Reexamination of Patent ("Request") both fail to demonstrate the actual publication date of various of the relied upon references necessary to establish a *prima facie* showing that each reference is prior art. The Patent Owner is left to assume that the assertion that the references are prior art arises from the copyright date printed on the face of each reference. This copyright date is not, however, the publication date.

The distinction between a publication date and a copyright date is critical. To establish a date of publication, the reference must be shown to have "been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it." *In re Wyre*, 655 F.2d 221, 226 (C.C.P.A. 1981). Unlike a publication date, a copyright date merely establishes "the date that the document was created or printed." *Hilgraeve, Inc. v. Symantec Corp.*, 271 F. Supp. 2d 964, 975 (E.D. Mich. 2003).

Presuming the author of a document accurately represented the date the document was created, this creation date is not evidence of any sort of publication or dissemination. Without

more, a bald assertion of the creation of the document does not meet the "publication" standard required for a document to be relied upon as prior art.

The party asserting the prior art bears the burden of establishing a date of publication. *See Carella v. Starlight Archery*, 804 F.2d 135, 139 (Fed. Cir. 1986) (finding that a mailer did not qualify as prior art because there was no evidence as to when the mailer was received by any of the addresses). Here, the Office bears the burden of establishing a prima facie case of unaptentability, including that the references relied upon are proper prior art. *See In re Hall*, 781 F.2d 897 (Fed. Cir. 1986)(Affidavits on public availability of a reference were necessary for the Examiner to establish the reference to be prior art.). Yet, neither the Office Action nor the Request even attempt to show that various of the references identified below were disseminated or made publicly available.

Thus, the Patent Owner respectfully submits that, as demonstrated below, a number of references relied upon in the Office Action have not been shown to be prior art to the rejected claims. Accordingly, the Patent Owner respectfully requests that the rejections over these references be withdrawn.

C. The Rejection of Claims Over Alleged Prior Art

The outstanding rejections rely on the erroneous premise that the "secure domain name" and "secure domain name service" recited in independent claims 1, 17, and 33 of the '180 Patent are a standard domain name and domain name service, respectively. In the interest of brevity, the Patent Owner here reveals the fault in this premise by outlining the differences here at the outset and refers back to these statements when addressing each rejection of the Office Action below.

The Request and Office Action rely on the erroneous premise that a secure domain name is a domain name that happens to correspond to a secure computer. *See, e.g.,* Office Action at 6; Request at 15. Alternatively, the Request and Office Action rely on the faulty position that a secure domain name corresponds to an address that simply requires authorization. Request at 21. These assertions are in clear contradiction to the specification of the '180 Patent, which takes pains to explain that a secure domain name is different from a domain name that just happens to be associated with a secure computer or just happens to be associated with an address requiring authorization. *Id.*; '180 Patent at col. 51, ll. 18-28; Nieh Dec. at ¶ 10. To illustrate, in various

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.