Attorney Docket No. 077580-0089

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:	)	
Edmand Munger, et al.	)	
	)	
U.S. Patent No.: 6,502,135	)	
Filed: February 15, 2000	)	**Examiner:**
Issued: December 31, 2002	)	**Andrew L. Nalven**
	)	
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY	)	**Group Art Unit: 3992**
	)	
Reexamination Proceeding	)	
Control No.: 95/001,269	)	
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 15, 2010 ("the Office Action") in the above-identified Reexamination of U.S. Patent Number 6,502,135 ("the '135 Patent") having a period of response set to expire on April 15, 2010, in view of the extension of time granted on February 25, 2010.

Remarks being on page 2 of this response; and

Listing of the claims appears in Appendix A.

REMARKS

Claims 1-10, 12, and 18 are under reexamination, with claims 1, 10, and 18 being independent. Claims 1, 3, 4, 6-10, and 12 stand rejected. Claims 2 and 5 were found not to be anticipated by the documents cited in the Replacement Request for *Inter Partes* Reexamination of Patent ("Request"). Therefore, Patent Owner respectfully requests confirmation of claims 2 and 5 at this time.

Claim 18 has been added. Support for claim 18 may be found, for example, in the originally issued claims of the '135 Patent at column 47, lines 20-35 and column 47, lines 47-52. Specifically, claim 18 corresponds to the combination of claims 2 and 5. No new matter has been introduced.

Because claim 9 depends from claim 5, which was found not to be anticipated or otherwise rejected by the cited documents in the Request, it is not understood how claim 9 stands rejected. Nevertheless, the Patent Owner addresses the rejection as provided below.

I. Patent Owner's Response to the Rejection

A. Applicable Standard for Rejection Under 35 U.S.C. § 102(a)

Claims 1, 3, 4, 6-10, and 12 of the '135 Patent stand rejected under 35 U.S.C. § 102(a) as being anticipated by Aventail Connect v3.1/v2.6 Administrator's Guide ("Aventail"). That statutory provision provides that "[a] person shall be entitled to a patent unless - (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent . . . ."

With respect to a rejection under 35 U.S.C. § 102, the MPEP states that "[a] claim is anticipated only if 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 for the following reasons.

B. Aventail has not been shown to be prior art under § 102(a)

The Office Action and the Request both fail to demonstrate the actual publication date of Aventail necessary to establish a *prima facie* showing that Aventail is prior art. Both the Office

Action and the Request assert that Aventail was published between 1996 and 1999 without any stated support. Request at 5; Office Action at 2. The Patent Owner can only presume that this assertion arises from the copyright date range printed on the face of the reference. *See* Aventail at *i*. This copyright date range is not, however, the publication date of Aventail.

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 (C.C.P.A. 1981). Aventail, on its face, provides "© 1996-1999 Aventail Corporation." The copyright date does not meet this standard. 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 the document accurately represented the date the document was created, this creation date is not evidence of any sort of publication or dissemination. Without more, this 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.

Further exacerbating matters is the filing date of the '135 Patent: February 15, 2000. Suppose the relied upon sections of the Aventail reference were created on December 31, 1999, and the copyright date range accordingly amended to read "1996-1999." Under these circumstances, it is possible that the document, although created, was not made publicly available until after the filing date of the '135 Patent, six weeks after creation. Under these circumstances, Aventail clearly would not be eligible to be relied upon as prior art to the '135 Patent.

The party asserting the prior art bears the burden of establishing a date of publication. See *Carella v. Starlight Archery*, 804 F.2d 135 (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). Yet, neither the Office Action nor the Request even attempt to show that Aventail was disseminated or made publicly available.

Thus, the Patent Owner respectfully submits that the Office Action has failed to establish that Aventail is prior art to the rejected claims. Accordingly, the Patent Owner respectfully

requests that the § 102(a) rejection over Aventail be withdrawn, and the rejected claims 1 and 10, as well as claims 3, 4, 6-9 and 12 depending thereupon, be confirmed.

C. The Rejection of Claims 1, 3, 4, 6-10, and 12 Under 35 U.S.C. § 102(a)

Claims 1, 3, 4, 6-10, and 12 of the '135 Patent stand rejected under 35 U.S.C. § 102(a) as being anticipated by Aventail. The rejection was based on the reasons given by the Request on pages 11-17 and Exhibit A and based on additional reasons presented in the Office Action on pages 4-9. Assuming Aventail qualifies as prior art, the Patent Owner respectfully traverses this rejection for the following reasons.

1. Aventail has not been shown to teach a virtual private network ("VPN")

a) Claim 1

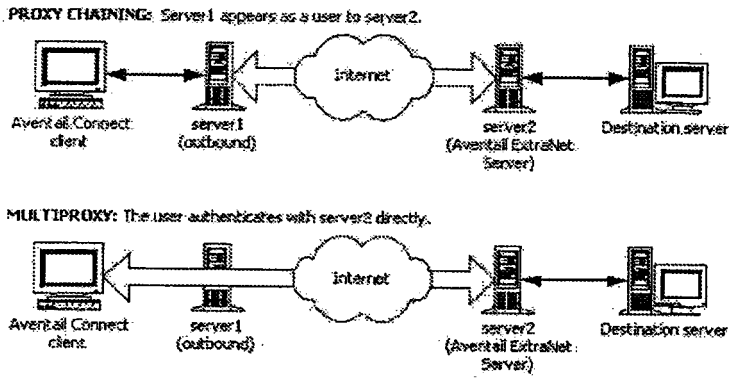
Claim 1 recites a method of transparently creating a VPN between a client computer and a target computer. As described below, Aventail fails to teach, either explicitly or inherently, at least this feature of the claimed invention. The Patent Owner's statements below are supported by an expert Declaration of Jason Nieh, Ph.D. pursuant to 37 C.F.R. § 1.1.32 ("Nieh Decl.") submitted herewith.

Aventail discloses a system and architecture for transmitting data between two computers using the SOCKS protocol. Nieh Decl. at ¶ 11. The system routes certain, predefined network traffic from a WinSock (Windows sockets) application to an extranet (SOCKS) server, possibly through successive servers. Aventail at 7; Nieh Decl. at ¶ 11. Upon receipt of the network traffic, the SOCKS server then transmits the network traffic to the Internet or external network. Aventail at 7; Nieh Decl. at ¶ 11. Aventail's disclosure is limited to connections created at the socket layer of the network architecture. Nieh Decl. at ¶ 11.

In operation, a component of the Aventail Connect software described in the reference resides between WinSock and the underlying TCP/IP stack. *See* Aventail at 9; Nieh Decl. at ¶ 12. The Aventail Connect software intercepts all connection requests from the user, and determines whether each request matches local, preset criteria for redirection to a SOCKS server. *See* Aventail at 10; Nieh Decl. at ¶ 12. If redirection is appropriate, then Aventail Connect creates a false DNS entry to return to the requesting application. *See* Aventail at 12; Nieh Decl. at ¶ 13. Aventail discloses that Aventail Connect then forwards the destination hostname to the

extranet SOCK server over a SOCKS connection. *See* Aventail at 12; Nieh Decl. at ¶ 13. The SOCKS server performs the hostname resolution. Aventail at 12; Nieh Decl. at ¶ 14. Once the hostname is resolved, the user can transmit data over a SOCKS connection to the SOCKS server. Nieh Decl. at ¶ 14. The SOCKS server, then, separately relays that transmitted data to the target. Nieh Decl. at ¶ 14.

The Request also cites to a "Proxy Chaining" and a "MultiProxy" mode disclosed in Aventail. Request at 12; Aventail at 68-73. In the "Proxy Chaining" mode, Aventail indicates that a user can communicate with a target via a number of proxies such that each proxy server acts as a client to the next downstream proxy server. Aventail at 68; Nieh Decl. at ¶ 16. As shown below, in this mode, the user does not communicate directly with the proxy servers other than the one immediately downstream from it. Aventail at 68, 72; Nieh Decl. at ¶ 16.



Aventail at 72. In the "MultiProxy" mode, Aventail indicates that the user, via Aventail Connect, authenticates with each successive proxy server directly. Aventail at 68; Nieh Decl. at ¶ 17. Regardless of the number of servers or proxies between the client and target, at least one is required and the operation of Aventail Connect does not materially differ between the methods. Nieh Decl. at ¶ 18.

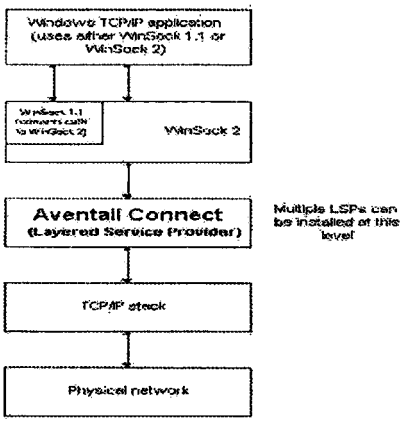
Aventail has not been shown to disclose the VPN claimed in Claim 1 of the '135 Patent for at least three reasons. Nieh Decl. at ¶ 19. First, Aventail has not been shown to demonstrate that computers connected via the Aventail system are able to communicate with each other as though they were on the same network. *Id.* at ¶ 20. Aventail discloses establishing point-to-

point SOCKS connections between a client computer and a SOCKS server. *Id.* The SOCKS server then relays data received to the intended target. *Id.* Aventail does not disclose a VPN, where data can be addressed to one or more different computers across the network, regardless of the location of the computer. *Id.*

For example, suppose two computers, A and B, reside on a public network. *Id.* at ¶ 21. Further, suppose two computers, X and Y, reside on a private network. *Id.* If A establishes a VPN connection with X and Y's network to address data to X, and B separately establishes a VPN connection with X and Y's network to address data to Y, then A would nevertheless be able to address data to B, X, and Y without additional set up. *Id.* This is true because A, B, X, and Y would all be a part of the same VPN. *Id.*

In contrast, suppose, according to Aventail, which only discloses communications at the socket layer, A establishes a SOCKS connection with a SOCKS server for relaying data to X, and B separately establishes a SOCKS connection with the SOCKS server for relaying data to Y. *Id.* at ¶ 22. In this situation, not only would A be unable to address data to Y without establishing a separate SOCKS connection (*i.e.* a VPN according to the Office Action), but A would be unable to address data to B over a secure connection. *Id.* This is one example of how the cited portions of Aventail fail to disclose a VPN. *Id.*

Second, according to Aventail, Aventail Connect's fundamental operation is incompatible with users transmitting data that is sensitive to network information. *Id.* at ¶ 23. As stated above, Aventail discloses that Aventail Connect operates between the WinSock and TCP/IP layers, as depicted on page 9:



Aventail at 9; *id.* Because Aventail discloses that Aventail Connect operates between these layers, it can intercept DNS requests. Nieh Dec. at ¶ 24. Aventail discloses that Aventail Connect intercepts certain DNS requests, and returns a false DNS response to the user if the requested hostname matches a hostname on a user-defined list. *Id.* Accordingly, Aventail discloses that the user will receive false network information from Aventail Connect for these hostnames. *Id.* If the client computer hopes to transfer to the target data that is sensitive to network information, Aventail Connect's falsification of the network information would prevent the correct transfer of data. *Id.* at ¶ 25. Thus, Aventail has not been shown to disclose a VPN. *Id.*

Third, Aventail has not been shown to disclose a VPN because computers connected according to Aventail do not communicate directly with each other. *Id.* at ¶ 26. Aventail discloses a system where a client on a public network transmits data to a SOCKS server via a singular, point-to-point SOCKS connection at the socket layer of the network architecture. *Id.* The SOCKS server then relays that data to a target computer on a private network on which the SOCKS server also resides. *Id.* All communications between the client and target stop and start at the intermediate SOCKS server. *Id.* The client cannot open a connection with the target itself. Therefore, one skilled in the art would not have considered the client and target to be virtually on the same private network. *Id.* Instead, the client computer and target computer are deliberately separated by the intermediate SOCKS server. *Id.*

For the reasons stated above, Aventail has not been shown to teach or disclose the "virtual private network" recited in claim 1. *Id.* at ¶ 27. Accordingly, the Patent Owner respectfully requests that claim 1, as well as rejected claims 3, 4, and 6-9 dependent thereupon, be confirmed.

b) Claim 10

Independent claim 10 recites "a VPN between the client computer and the secure target computer." (emphasis added). *Id.* at ¶ 28 For at least the reasons stated in Section I.C.1.a., above, Aventail similarly has not been shown to teach the invention recited in claim 10. *Id.* Accordingly, the Patent Owner respectfully requests that claim 10, as well as rejected claim 12 dependent thereupon, be confirmed.

2. Aventail has not been shown to teach a DNS proxy server as in claim 10

Claim 10 also recites a "DNS proxy server" that 1) "returns the IP address for the requested domain name if it is determined that access to a non-secure web site has been requested" and that 2) also "generates a request to create the VPN. . . if it is determined that access to a secure web site has been requested." (emphasis added). *Id.* at ¶ 30. The Office Action and Request allege that Aventail Connect is the claimed DNS proxy server. *Id.* at ¶ 31. Aventail discloses that Aventail Connect intercepts all DNS requests. *Id.* at ¶ 32. "If the hostname matches a local domain string or does not match a redirection rule, Aventail Connect passes the name resolution query through to the TCP/IP stack on the local workstation. The TCP/IP stack performs the lookup as if Aventail Connect were not running." Aventail at 11; Nieh Decl. at ¶ 32. Thus, Aventail discloses that Aventail Connect does not return the IP address if the DNS request requests the address for a non-secure web site. *Id.* As such, Aventail Connect is not taught by Aventail to correspond to the DNS proxy server recited in claim 10. *Id.*

For at least this additional reason, the Patent Owner respectfully requests that claim 10, along with rejected claim 12 that depends thereupon, be confirmed. *Id.* at ¶ 33.

II. New Claims

New claim 18 corresponds to the combination of claims 2 and 5, which were found not to be anticipated or otherwise rejected by the cited documents in the Request. Therefore, the Patent Owner respectfully requests consideration and allowance of claim 18 at this time.

III. Conclusion

For at least the reasons set forth above, the Examiner's rejection of claims 1, 3, 4, 6-10, and 12 should be withdrawn. Reconsideration and prompt confirmation of claims 1, 3, 4, 6-10, and 12 are respectfully requested. Consideration and allowance of claim 18 is also respectfully requested.

Please charge our Deposit Account No. 501133 any fees or credit any overcharges relating to this Response.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/

Toby H. Kusmer, P.C., Reg. No. 26,418
Matthew E. Leno, Reg. No. 41,149
Hasan M. Rashid, Reg. No. 62,390
McDermott Will & Emery LLP
Attorneys for Patent Owner

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com

Please recognize our Customer No. 23630 as our correspondence address.

Date: April 15, 2010

APPENDIX A

Listing of Claims:

This listing of claims will replace all prior versions, and listings, of claims in this application:

1. (Original) A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

(1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

(2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and

(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer.

2. (Original) The method of claim 1, wherein steps (2) and (3) are performed at a DNS server separate from the client computer.

3. (Original) The method of claim 1, further comprising the step of: (4) in response to determining that the DNS request in step (2) is not requesting access to a secure target web site, resolving the IP address for the domain name and returning the IP address to the client computer.

4. (Original) The method of claim 1, wherein step (3) comprises the step of, prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client computer is authorized to establish a VPN with the target computer and, if not so authorized, returning an error from the DNS request.

5. (Original) The method of claim 1, wherein step (3) comprises the step of, prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client computer is authorized to resolve addresses of non secure target computers and, if not so authorized, returning an error from the DNS request.

6. (Original) The method of claim 1, wherein step (3) comprises the step of establishing the VPN by creating an IP address hopping scheme between the client computer and the target computer.

7. (Original) The method of claim 1, wherein step (3) comprises the step of using a gatekeeper computer that allocates VPN resources for communicating between the client computer and the target computer.

8. (Original) The method of claim 1, wherein step (2) is performed in a DNS proxy server that passes through the request to a DNS server if it is determined in step (3) that access is not being requested to a secure target web site.

9. (Original) The method of claim 5, wherein step (3) comprises the step of transmitting a message to the client computer to determine whether the client computer is authorized to establish the VPN target computer.

10. (Original) A system that transparently creates a virtual private network (VPN) between a client computer and a secure target computer, comprising:

a DNS proxy server that receives a request from the client computer to look up an IP address for a domain name, wherein the DNS proxy server returns the IP address for the requested domain name if it is determined that access to a non-secure web site has been requested, and wherein the DNS proxy server generates a request to create the VPN between the client computer and the secure target computer if it is determined that access to a secure web site has been requested; and

a gatekeeper computer that allocates resources for the VPN between the client computer and the secure web computer in response to the request by the DNS proxy server.

11. (Original) The system of claim 10, wherein the gatekeeper computer creates the VPN by establishing an IP address hopping regime that is used to pseudorandomly change IP addresses in packets transmitted between the client computer and the secure target computer.

12. (Original) The system of claim 10, wherein the gatekeeper computer determines whether the client computer has sufficient security privileges to create the VPN and, if the client computer lacks sufficient security privileges, rejecting the request to create the VPN.

13. (Original) A method of establishing communication between one of a plurality of client computers and a central computer that maintains a plurality of authentication tables each corresponding to one of the client computers, the method comprising the steps of:

(1) in the central computer, receiving from one of the plurality of client computers a request to establish a connection;

(2) authenticating, with reference to one of the plurality of authentication tables, that the request received in step (1) is from an authorized client;

(3) responsive to a determination that the request is from an authorized client, allocating resources to establish a virtual private link between the client and a second computer; and

(4) communicating between the authorized client and the second computer using the virtual private link.

14. (Original) The method of claim 13, wherein step (4) comprises the step of communicating according to a scheme by which at least one field in a series of data packets is periodically changed according to a known sequence.

15. (Original) The method of claim 14, wherein step (4) comprises the step of comparing an Internet Protocol (IP) address in a header of each data packet to a table of valid IP addresses maintained in a table in the second computer.

16. (Original) The method of claim 15, wherein step (4) comprises the step of comparing the IP address in the header of each data packet to a moving window of valid IP addresses, and rejecting data packets having IP addresses that do not fall within the moving window.

17. (Original) The method of claim 13, wherein step (2) comprises the step of using a

checkpoint data structure that maintains synchronization of a periodically changing parameter known by the central computer and the client computer to authenticate the client.

18. (New) A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

(1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

(2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and

(3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer, wherein:

steps (2) and (3) are performed at a DNS server separate from the client computer, and

step (3) comprises the step of, prior to automatically initiating the VPN between the client computer and the target computer, determining whether the client computer is authorized to resolve addresses of non secure target computers and, if not so authorized, returning an error from the DNS request.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Reexamination of:	)	
Edmund Munger, et al.	)	
	)	
U.S. Patent No.: 6,502,135	)	
Filed: February 15, 2000	)	**Examiner:**
Issued: December 31, 2002	)	**Andrew L. Nalven**
	)	
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY	)	**Group Art Unit: 3992**
	)	
Reexamination Proceeding	)	
Control No.: 95/001,269	)	
Filed: December 8, 2009	)	

CERTIFICATE OF SERVICE

WE HEREBY CERTIFY that the Response to Office Action in Reexamination, filed with United States Patent and Trademark Office on April 15, 2010, was served this 15th day of April, 2010 on Requester by causing a true copy of same to be deposited as first-class mail for delivery to:

William N. Hughet
Rothwell, Figg, Ernst & Manbeck, P.C.
1425 K Street N.W.
Suite 800
Washington, D.C. 20005

Respectfully submitted,
McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/
Toby H. Kusmer, P.C., Reg. No. 26,418
Matthew E. Leno, Reg. No. 41,149
Hasan M. Rashid, Reg. No. 62,390
McDermott Will & Emery LLP
Attorneys for Patent Owner
Please recognize our Customer No. 23630 as our correspondence address.

28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617)535-3800
tkusmer@mwe.com,
mleno@mwe.com
hrashid@mwe.com
Date: April 15, 2010

BST99 1647928-1.077580.0089

Electronic Acknowledgement Receipt	
EFS ID:	7421128
Application Number:	95001269
International Application Number:	
Confirmation Number:	2038
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY
First Named Inventor/Applicant Name:	6502135
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-89
Receipt Date:	15-APR-2010
Filing Date:	08-DEC-2009
Time Stamp:	14:21:04
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Response.pdf	432309 c77ec2d4a246bcbd0441c6bc715a224629cd1a46	yes	14

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Response after non-final action-owner timely	1	1
	Applicant Arguments/Remarks Made in an Amendment	2	9
	Claims	10	14

Warnings:					
Information:					
2	Reexam Certificate of Service	Resp_Cert.pdf	24050 5c91599ee7620345db969fbea8c388d713ad38177	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	456359		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.