IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Inter Partes* Reexamination of:	)	
	)	
Victor Larson et al.	)	Control No.: 95/001,788
	)	
U.S. Patent No. 7,418,504	)	Group Art Unit: 3992
	)	
Issued: August 26, 2008	)	Examiner: Roland Foster
	)	
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	)	Confirmation No.: 5823

Mail Stop *Inter Partes* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PATENT OWNER'S RESPONSE TO OFFICE ACTION OF DECEMBER 29, 2011

TABLE OF CONTENTS

I. INTRODUCTION

VirnetX Inc. ("Patent Owner"), the owner of U.S. Patent No. 7,418,504 ("the '504 patent"), hereby responds to the Office Action ("Office Action" or "OA") and Order granting reexamination ("Order") mailed on December 29, 2011, in the above-identified reexamination proceeding, which was initiated by Third-Party Requester, Apple Inc. ("Requester"), on October 18, 2011 ("the Request" or "Req."). Patent Owner is grateful for the one-month extension of time to respond, extending the time for reply to March 29, 2012. The Examiner adopted all thirty-five issues the Requester identified.

The patent at issue in this reexamination, the '504 patent, is part of a family of patents ("Munger patent family") that stems from U.S. provisional application nos. 60/106,261 ("the '261 application"), filed on October 30, 1998, and 60/137,704 ("the '704 application"), filed on June 7, 1999. The '504 patent is a continuation of U.S. application no. 09/558,210 ("the '210 application"), filed April 26, 2000, (now abandoned), which is a continuation-in-part of U.S. application no. 09/504,783 (now U.S. Patent No. 6,502,135, "the '135 patent"). The '135 patent is a continuation-in-part of U.S. application no. 09/429,643 (now U.S. Patent No. 7,010,604, "the '604 patent"), which claims priority to the '261 and '704 applications.

The Munger patent family discloses numerous inventions relating to secure communications. Patents in this family have been subject to several reexamination proceedings and district court actions. For instance, three other patents from the family were asserted in an action against Microsoft Corporation in the Eastern District of Texas.[1] The jury found the asserted claims willfully infringed and not invalid and awarded VirnetX over one hundred million dollars in damages. (Ex. A-1 at 2.) Microsoft also sought reexamination of two of the patents, but all claims were confirmed during those proceedings. (*See* control nos. 95/001,269 and 95/001,270.) And just recently, the Office denied a request for reexamination of one of the patents in the Munger patent family. (Order in control no. 95/001,792.)

Given that the validity of the patents in the Munger patent family has now been tested multiple times, and for the other reasons set forth below, including that the asserted references do not disclose or suggest the combination of features recited in the claims, Patent Owner requests

---

[1] One of these patents, U.S. Patent No. 6,839,759 was asserted initially but was dropped from this case before trial.

reconsideration and withdrawal of all the rejections in the Office Action and confirmation of the patentability of all of the claims of the '504 patent.

Patent Owner's statements below are supported, where indicated, by an expert Declaration of Angelos D. Keromytis, Ph.D. ("Keromytis Decl.") and a Declaration of Dr. Robert Dunham Short III ("Short Decl.").

A. Applicable Legal Standards

1. The Law of Anticipation

"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." *Verdegaal Bros. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the . . . claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989). Although identity of terminology is not required, the elements must be arranged as required by the claim. *In re Bond*, 910 F.2d 831, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990). Thus, "unless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim, it . . . cannot anticipate under 35 U.S.C. § 102." *Net MoneyIn, Inc. v. Verisign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008).

2. The Law of Obviousness

A claim can only be rejected as being obvious if the differences between it and the prior art "are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art." *See* 35 U.S.C. § 103(a) (1994); *Graham v. John Deere Co.*, 383 U.S. 1, 13-14 (1966). The ultimate determination of whether an invention is obvious is a legal conclusion based on underlying factual inquiries including: (1) the scope and content of the prior art; (2) the level of ordinary skill in the art; (3) the differences between the claimed invention and the prior art; and (4) objective evidence of secondary considerations of nonobviousness. *See Graham*, 383 U.S. at 17-18; *Miles Labs., Inc. v. Shandon Inc.*, 997 F.2d 870, 877, 27 U.S.P.Q.2d 1123, 1128 (Fed. Cir. 1993).

A statement that modifications of the prior art to meet the claimed invention would have been "well within the ordinary skill of the art at the time the claimed invention was made" because the references relied upon teach that all aspects of the claimed invention were individually known in the art, is not sufficient to establish a *prima facie* case of obviousness without some objective reason to combine the teachings of the references. M.P.E.P. § 2143.01 (citing *Ex parte Levengood*, 28 U.S.P.Q.2d 1300 (B.P.A.I. 1993)). "[R]ejections on obviousness cannot be sustained by mere

conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418, 82 U.S.P.Q.2d 1385, 1396 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988, 78 U.S.P.Q.2d 1329, 1336 (Fed. Cir. 2006)).

Further, even in view of *KSR*, it is not permissible to simply "pick and choose" elements of the prior art to arrive at the claimed subject matter. There must be some basis or rationale suggesting the modification and a reasonable expectation of success. M.P.E.P. § 2143.02

3. The Law of Inherency

The express, implicit, and inherent disclosures of a prior art reference may be relied upon in the rejection of claims under 35 U.S.C. § 102 or § 103. M.P.E.P. § 2112. The fact that a certain result or characteristic *may* occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *Id.* To establish inherency, the extrinsic evidence must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. *Id.*

B. Background of the '504 Patent

The '504 patent discloses several embodiments of a domain name service ("DNS") system for establishing a secure communication link, such as a virtual private network ("VPN") communication link, between devices connected to a network. In one such embodiment, a novel, specialized DNS server receives a traditional DNS request, and the DNS server automatically facilitates the establishment of a secure communication link between a target node and a user. (Keromytis Decl. ¶ 16; '504 patent 39:46-51.) This specialized DNS server is different from a conventional DNS server known at the time of the invention for at least the reason that the specialized DNS server supports the establishment of a secure communication link beyond merely a requested IP address or public key. (Keromytis Decl. ¶ 16.)

For example, in the exemplars of FIGS. 26 and 27 of the '504 patent, reproduced below, a DNS server 2602 including a DNS proxy 2610 supports establishing a VPN link between a computer 2601 and a secure target site 2604. ('504 patent 39:67-41:59; Keromytis Decl. ¶ 17.)

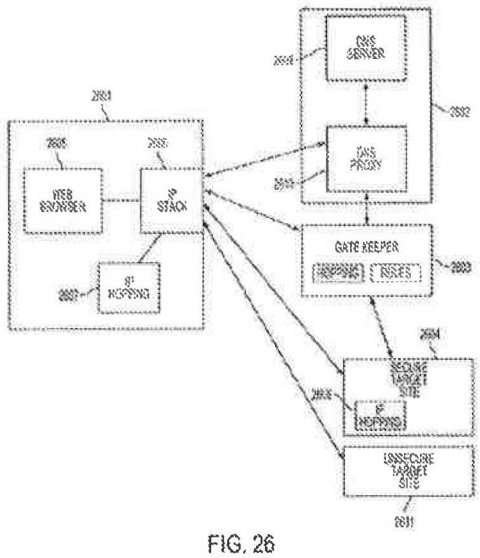


FIG. 26

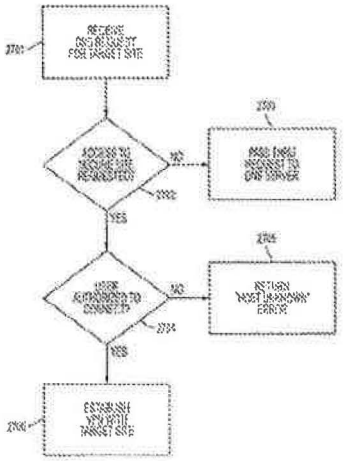


FIG. 27

In one embodiment, the DNS server 2602 receives a DNS request for a target site from computer 2601. ('504 patent 40:49-52; Keromytis Decl. ¶ 18.) The DNS proxy 2610 determines whether the target site is a secure site. ('504 patent 40:6-8, 40:49-56; Keromytis Decl. ¶ 18.) If access to a secure site has been requested, the DNS proxy 2610 determines whether the computer 2601 is authorized to access the site. ('504 patent 40:57-59; Keromytis Decl. ¶ 18.) If so, the DNS proxy 2610 transmits a message to gatekeeper 2603 to facilitate the creation of a VPN link between computer 2601 and secure target site 2604. ('504 patent 40:18-24.) The DNS proxy 2610 then responds to the computer's 2601 DNS request with an address received from the gatekeeper 2604. (*Id.* at 40:19-22; Keromytis Decl. ¶ 18.) A secure VPN link is then established between the computer 2601 and the secure target site 2604. ('504 patent 41:5-8; Keromytis Decl. ¶ 18.) As shown in this example, the specialized DNS server supports creating a secure communication link and does more than a conventional DNS server at the time of the invention. (Keromytis Decl. ¶ 18.)

The '504 patent highlights this distinction between the specialized DNS server disclosed in its specification and a conventional DNS scheme, which merely returns a requested IP address or public key:

> Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name "Yahoo.com," the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser . . . .
>
> . . .

> One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project (RFC 2535).
>
> The conventional scheme suffers from certain drawbacks. For example, any user can perform a DNS request. Moreover, DNS requests resolve to the same value for all users.
>
> According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user.

('504 patent 39:7-51; Keromytis Decl. ¶ 19.) Compared with a conventional DNS known at the time of the filing date of the '504 patent, the specialized DNS disclosed in the '504 patent supports establishing a secure communication link. (Keromytis Decl. ¶ 19.) The claims of the '504 patent are also directed to a domain name service for establishing a secure communication link. (*See, e.g.*, '504 patent 55:49-56, 57:48-58, 60:3-14; Keromytis Decl. ¶ 19.)

II. CLAIMS 1-60 ARE PATENTABLE

A. The Rejections Based on *Solana* and/or *Reed* Are Improper Because Neither Reference Has Been Shown to Be Prior Art (Grounds 1-8, 11, 15, 19, 24, 28, and 33)

As a threshold matter, Patent Owner notes that the Request and the Office Action rely on the following two references without showing that these references have been published:

1. E. Solana et al., "Flexible Internet Secure Transactions Based on Collaborative Domains," Lecture Notes in Computer Science, vol. 1361, at 37-51 ("*Solana*") (Req. Ex. X1); and
2. M. Reed et al., "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA ("*Reed*") (Req. Ex. X10).

Neither reference is a patent. The entirety of the support for these references being prior art printed publications is a bald assertion in the Request, adopted by the Office Action, that the references were publicly distributed prior to the effective date of the '504 patent. This attorney argument does not establish these references as prior art for at least the following reasons.

1. A Reference Is a "Printed Publication" Only When the Requisite Showing Is Made

Solana and *Reed* are prior art only if they are "printed publications." The statutory phrase "printed publication" means that the alleged reference must have been sufficiently accessible to the public interested in the art. *In re Cronyn*, 890 F.2d 1158, 1160 (Fed. Cir. 1989) (quoting *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1568 (Fed. Cir. 1988)). M.P.E.P. § 2128 provides in part:

> A reference is a "printed publication" only "upon a satisfactory showing that such document has 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 Wyer,* 655 F.2d 221, 210 USPQ 790 (C.C.P.A. 1981) (quoting *I.C.E. Corp. v. Armco Steel Corp.*, 250 F. Supp. 738, 743, 148 USPQ 537, 540 (SDNY 1966)).

Thus, a showing of dissemination and public accessibility are the keys to the legal determination of whether a document was "published." The record is devoid of any showing that *Solana* and *Reed* were disseminated or otherwise publicly available *at the time asserted* by the Requester. Rather, the Request baldly asserts that "*Solana* is a printed publication that was distributed to the public without restriction no later than 1997." (Req. at 11.) Similarly, the Request asserts that "*Reed* is a printed publication that was distributed publicly without restriction no later than December 13, 1996 . . . ." (*Id.* at 12.)

Solana contains no publication date on the document. The face of the document identifies only that the authors are affiliated with the University of Geneva. There is no indication on the document that it was published on the date asserted by the Requester.

Reed identifies the 12th Annual Security Applications Conference, San Diego, CA, and a date of December 9-13, 1996, but there is no evidence that the document was actually "published" within those dates, nor that the document was "otherwise available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, could locate it" at the time.

2. Requester Failed to Satisfy Its Duty to Disclose Any Evidence of Publication and Is Presumed to Have None

Under 37 C.F.R. § 11.18, the Requester was required to produce any evidence proving

Solana or *Reed* were publicly distributed without restriction at the time asserted by the Requester.[2] Yet, it produced none. The logical conclusion is that no such evidence exists. Should the Requester subsequently attempt to introduce any evidence that *Solana* or *Reed* is prior art at the time asserted by the Requester, then the remedies provided by 37 C.F.R. § 11.18(c) should be exercised—absent a showing that the evidence was not available to the Requester at the time the Request was filed—to strike the paper attempting to submit that evidence, 37 C.F.R. § 11.18(c)(1), or to terminate this proceeding entirely, 37 C.F.R. § 11.18(c)(5)).

3. Requester's Bare Contention of Publication Is Inadequate

As stated above, the Requester's sole basis for relying on *Solana* and *Reed* as prior art is a bald assertion that they were printed publications distributed before the critical date. These bald assertions are nothing more than attorney argument, which is not evidence. *See In re Wyer*, 655 F.2d 221, 227 (C.C.P.A. 1981) ("[T]he one who wishes to characterize the information, in whatever form it may be, as a 'printed publication' . . . *should produce sufficient proof* of its dissemination or that it has otherwise been available and accessible to persons concerned with the art to which the document relates and thus most likely to avail themselves of its contents . . . ." (emphasis added)).

The M.P.E.P. expressly recognizes that attorney argument is not evidence: M.P.E.P. § 716.01(c) ("The arguments of counsel cannot take the place of evidence in the record." (citing *In re Schulze*, 346 F.2d 600, 602, 145 U.S.P.Q. 716, 718 (C.C.P.A. 1965))). Although M.P.E.P. § 716.01(c) focuses on certain types of evidence typically used to rebut rejections, it is not exclusive to those types of evidence. Moreover, the broader notion of M.P.E.P. § 716.01(c) that attorney argument cannot replace real evidence is a well founded, common-sense position permeating the Office rules.

Because the record is devoid of evidence that *Solana* and *Reed* were printed publications on the dates asserted, each rejection based, in whole or in part, on either reference is fatally defective. Patent Owner respectfully requests that all such rejections (specifically Grounds 1-8, 11, 15, 19, 24, 28, and 33) be withdrawn. Without admitting that *Solana* and *Reed* are publications as of the dates

---

[2] 37 C.F.R. § 11.18(b)(2)(iii) requires that all "*factual contentions have evidentiary support or, **if specifically so identified**, are likely to have evidentiary support after a reasonable opportunity for further investigation or discovery* . . . ." (emphasis added). The Requester's factual contentions regarding the public distribution of *Solana* and *Reed* do not state that those contentions are likely to have evidentiary support.

asserted by the Requester, Patent Owner will assume, *arguendo*, that the references are publications as of the asserted dates for the purposes of this response.

B. The Rejections Based on the RFC Documents (Grounds 2, 5-8, 10, 13-20, and 22-35) Are Improper Because the RFC Documents Have Not Been Shown to Be Prior Art

Similarly, the Request and the Office Action rely on several RFC documents (collectively referred to in this section as "the RFC documents") without showing that these references have been published:

1. RFC 2230, "Key Exchange Delegation Record for the DNS" ("RFC 2230") (Req. Ex. X4);
2. RFC 2538, "Storing Certificates in the Domain Name System (DNS)" ("RFC 2538") (Req. Ex. X5);
3. RFC 2401, "Security Architecture for the Internet Protocol" ("RFC 2401") (Req. Ex. X6);
4. RFC 2065, "Domain Name System Security Extensions" ("RFC 2065") (Req. Ex. X7);
5. RFC 920, "Domain Requirements" ("RFC 920") (Req. Ex. X8);
6. RFC 2504, "Users' Security Handbook" ("RFC 2504") (Req. Ex. X9);
7. RFC 1035, "Domain Names—Implementation and Specification" ("RFC 1035") (Req. Ex. Y2);
8. RFC 1123, "Requirements for Internet Hosts—Applications and Support" ("RFC 1123") (Req. Ex. Y3);
9. RFC 1825, "Security Architecture for the Internet Protocol" ("RFC 1825") (Req. Ex. Y4);
10. RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" ("RFC 2459") (Req. Ex. Y5); and
11. RFC 1034, "Domain Names—Concepts and Facilities" ("RFC 1034") (Req. Ex. Y6).

The RFC documents cited in the Request cannot be relied on as publications as of the asserted dates because the record is devoid of evidence that any of these references are patents or printed publications as of those dates.

The Requester appears to have relied on the date (month and year, or year) indicated in each of the RFC documents. The Requester asserted, for example, that "RFC 2230 is a printed publication

that was distributed to the public without restriction no later than November 1997, and is publicly available at http://tools.ietf.org/html/rfc2230." (Req. at 11.) However, the indication of a particular date in a document, without any description thereof, does not necessarily mean that the indicated date is the publication date of the document or the date when the documents were first publicly available. Nor is it evident that, even if the documents were each distributed on the dates indicated, such distribution was "without restriction" since it is unknown who had access to the documents. These documents refer to a "Network Working Group." Such a reference is vague at best as to whether these documents were disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, could locate it at the time alleged by the Requester. Thus, such dates provided in each of the RFC documents are insufficient to establish them as publications constituting prior art under 35 U.S.C. §§ 102 and 103 as of the asserted dates. While the Requester has mentioned that each RFC document is currently available on the Internet, the fact that they are *currently* available on the Internet does not establish the documents as publications at the times alleged by the Requester. M.P.E.P. § 2128 states in part:

> Prior art disclosures on the Internet or on an on-line database are considered to be publicly available as of the date the item was *publicly posted*. Absent evidence of the date that the disclosure was publicly posted, if the publication itself does not include a publication date (or retrieval date), it cannot be relied upon as prior art under 35 U.S.C. 102(a) or (b).

M.P.E.P. § 2128 (emphasis added).

M.P.E.P. § 2128 clearly requires a "publication date" or "retrieval date" for a prior art disclosure on the Internet or on an on-line database. The Requester, however, has failed to provide any evidence that the date indicated in each of the RFC documents, which is a disclosure on the Internet, is a "publication date" or "retrieval date."

For the same reasons discussed above with regard to *Solana* and *Reed*, the Requester's assertion that the RFC documents are prior art is, therefore, nothing more than attorney argument, which is not evidence. *See In re Wyer*, 655 F.2d at 227.

Because the record is devoid of evidence that the RFC documents were printed publications, each rejection based in whole or in part on any of these references is fatally defective. Patent Owner respectfully requests that all such rejections (specifically, Grounds 2, 5-8, 10, 13-20, and 22-35) be withdrawn. Without admitting that the RFC documents are publications as of the dates asserted by the Requester, Patent Owner will assume, *arguendo*, that the references are publications as of the asserted dates for the purposes of this response.

C. Independent Claims 1, 36, and 60 Are Patentable over the Cited Art Applied in the Rejections of These Claims (Grounds 1, 5, 9, 13, 17, 21, 25, and 30)

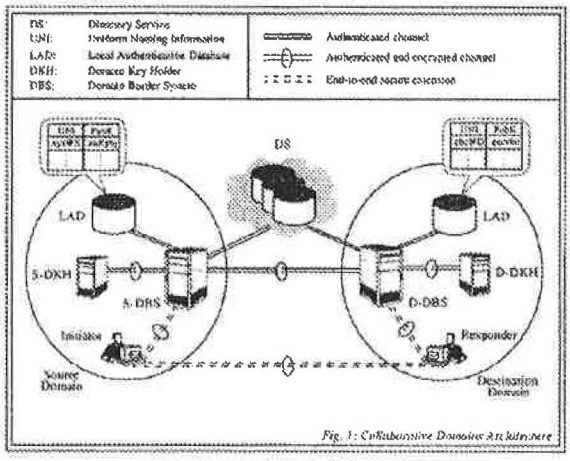
The Office Action rejects independent claims 1, 36, and 60 under §§ 102 and 103 on multiple grounds, as discussed below (Grounds 1, 5, 9, 13, 17, 21, 25, and 30). However, for at least the reasons discussed below, each of these rejections should be withdrawn.

1. Independent Claims 1, 36, and 60 Are Patentable over *Solana* (Ground 1)

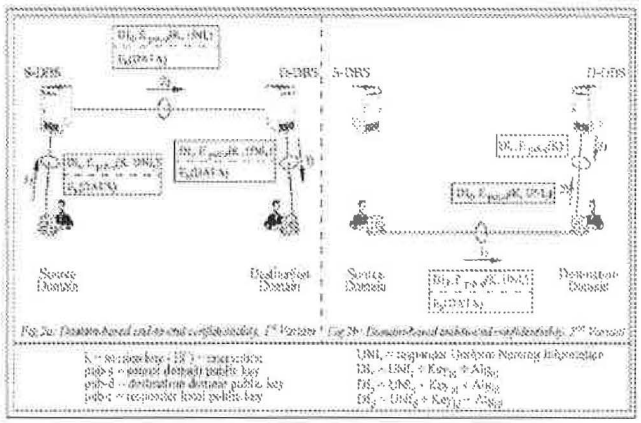
The Office Action rejects claims 1, 36, and 60 under § 102(b) as being anticipated by *Solana* (Ground 1). (OA at 4-6.) For the reasons discussed below, the rejection fails to establish that *Solana* discloses each and every feature of the claims, and thus should be withdrawn.

a) Overview of *Solana*

Solana discloses a domain-based security architecture for Internet transactions. (*Solana* Abstract, 41-43, Fig. 1.) Regarding Fig. 1, reproduced below, *Solana* discloses that the architecture includes a directory service ("DS") that binds domains to their public keys and a local authentication database ("LAD") that includes the public keys for each principal within a domain. (*Id.* at 43.) *Solana* discloses that each security domain includes a domain key holder ("DKH") that stores the key ring of domain public/private key pairs and a domain border system ("DBS") that performs various tasks related to inter-domain collaboration. (*Id.* at 43-44.) *Solana* also discloses uniform naming information ("UNI") that is used to designate both domains and principals within domains. (*Id.* at 43.) The UNI may be "a common name, an E-mail address, or a network address." (*Id.*)



Solana discloses two alternatives for communicating between an initiator in a source domain and a responder in a destination domain. (*Id.* at Figs. 2a, 2b.)



In the configuration relating to Fig. 2a, the initiator sends a communication to a source DBS ("S-DBS"). (*Id.* at 45.) The communication includes a header that contains a session key and uniform naming information ("UNI") for the responder and is encrypted with a public key of the source domain. (*Id.*) The S-DBS receives the communication, decrypts the header using its private key, re-encrypts the same header using the public key of the destination domain, and sends the transaction to the destination DBS ("D-DBS"). (*Id.* at 45-46.) The D-DBS likewise extracts the header, finds the local public key of the responder in the LAD, re-encrypts the same header with the responder local public key, and forwards the transaction to the responder. (*Id.* at 46.)

In the configuration relating to Fig. 2b, the initiator sends a similar communication directly to the responder that includes the same header as in the configuration of Fig. 2a, except the header is encrypted with the destination domain public key. (*Id.* at 45-46.) The responder forwards the header to the D-DBS, and the D-DBS sends the header back, this time encrypted with the responder local public key. (*Id.*)

b) *Solana* Does Not Disclose the Elements of Independent Claim 1

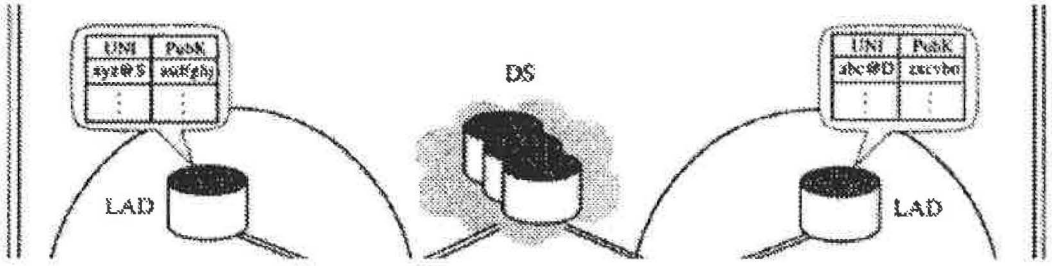
(1) *Solana* Does Not Disclose "a Domain Name Service System Configured to . . . Store Domain Names and Corresponding Network Addresses"

Independent claim 1 recites, *inter alia*, "a domain name service system configured to . . . store a plurality of domain names and corresponding network addresses . . . ." The Request and the Office Action assert that *Solana*'s DS is a "secure DNS system[] that store[s] a plurality of domain names and corresponding network addresses," and suggest that *Solana*'s UNIs, which may be published in the DS, allegedly include both domain names and corresponding network addresses. (Req. at 42.) However, *Solana* does not disclose the above-identified limitations of claim 1 for at least the following reasons.

First, *Solana* does not disclose that the DS stores a plurality of domain names and corresponding network addresses. Instead, *Solana* merely discloses that the DS stores "naming information and . . . certificates that securely bind domains to their public keys." (*Solana* 43; Keromytis Decl. ¶ 24.) Thus, if anything, *Solana*'s DS stores naming information for domains and *corresponding public keys* for the domains. (Keromytis Decl. ¶ 24.) But *Solana* does not disclose that the DS stores a plurality of domain names and *corresponding network addresses*.

Second, the "naming information" stored in *Solana*'s DS also does not include both domain names *and corresponding network addresses*. *Solana* explains that the "naming information" is stored in the DS in the form of UNIs, which may include "a common name, an E-mail address, *or* a network address." (*Solana* 43 (emphasis added); Keromytis Decl. ¶ 25.) Thus, the UNI disclosed by *Solana* does not include *both* a domain name and a corresponding network address.

Further, in Fig. 1, reproduced in part below, *Solana* discloses in greater detail how UNIs and corresponding keys may also be stored together in the LAD, another database separate from the DS. But the LAD also does not store domain names and corresponding network addresses:



(*Solana* 43.) The UNI/PubK tables in Fig. 1 show how the LAD associates a UNI of a particular principal with its public key. (*Solana* 43-44; Keromytis Decl. ¶ 26.) As shown, the UNI "xyz@S" for a principal in the source domain corresponds to public key "asdfghj," and the UNI "abc@D" for a principal in the destination domain corresponds to public key "zxcvbn." (*Solana* Fig. 1; Keromytis Decl. ¶ 26.) But again, the UNI itself does not include both a domain name and a corresponding network address. (*Solana* 43; Keromytis Decl. ¶ 26.) Moreover, the UNI stored in the LAD is associated with a public key, and not with a network address. (*Solana* Fig. 1; Keromytis Decl. ¶ 26.)

Third, contrary to the assertions in the Request and the Office Action, one of ordinary skill in the art would not have understood *Solana*'s DS to be a domain name service system. (Keromytis Decl. ¶ 27.) As discussed, *Solana*'s DS stores naming information ("UNIs") for domains and certificates that bind those domains to public keys. (*Id.*) But *Solana* does not disclose that the DS resolves domain names—resolving domain names into IP addresses is outside the scope of *Solana*. (*Id.*)

Because, as explained above, *Solana* fails to disclose "a domain name service system configured to . . . store a plurality of domain names and corresponding network addresses," as recited in independent claim 1, *Solana* does not anticipate independent claim 1.

(2) *Solana* Does Not Disclose "a Domain Name Service System Configured to . . . Receive a Query for a Network Address"

Independent claim 1 recites "a domain name service system configured to . . . receive a query for a network address . . . ." The Request and the Office Action cite portions discussing three different figures in *Solana* as allegedly disclosing this feature. (Req. at 42-44 (citing *Solana* Figs. 1, 2a, 2b).) As discussed below, none of the figures and corresponding disclosure relied on by the Request and Office Action describe a query for a network address.

First, contrary to the Request and the Office Action's assertions, Fig. 1 does not disclose a domain name service system configured to receive a query for a network address. With respect to Fig. 1 of *Solana*, the Request and the Office Action assert that *Solana* "explains that its secure DNS systems are designed to handle the 'generic Internet transaction' which . . . is generated by requests initiated by the two principals—the 'initiator' and the 'responder.'" (*Id.* at 43.) The Request continues: "[I]n Figure 1, the initiator and the responder entities are shown as making requests that are acted upon by the DNS system to establish an authenticated and encrypted channel of communications." (*Id.*)

But nothing in *Solana* even suggests that these alleged "requests" include a query for a network address. (Keromytis Decl. ¶ 30.) To the contrary, the "requests" sent from the initiator and responder, discussed in greater detail below with respect to Figs. 2a and 2b, are queries for *keys* stored in the DS or the LAD. (*See generally Solana* 45-46 ("The initiator . . . issues a DS query *to obtain the destination domain public key*" (emphasis added)); Keromytis Decl. ¶ 30.) Indeed, Fig. 1 of *Solana* discloses an architecture that distributes public keys used to establish authenticated and/or encrypted channels—not an architecture that receives queries for network addresses. (Keromytis Decl. ¶ 30.)

Second, Fig. 2a of *Solana* also does not disclose a domain name service system configured to receive a query for a network address. With respect to Fig. 2a, the Request and the Office Action assert that "the DNS system acts on requests to determine network addresses of the initiator and responder principals." (Req. at 44.) The Request and the Office Action also point to the three communications shown in Fig. 2a and explained on pages 45-46 of *Solana* as allegedly disclosing these "requests to determine network addresses of the initiator and responder principals." (*Id.* at 43-

44.)

These positions are misplaced because the communications of Fig. 2a and the corresponding disclosure in *Solana* describe no such requests. Instead, *Solana* discloses that the first communication in Fig. 2a is sent from the source domain to the S-DBS and includes "a header containing the session key and the UNI of the responder," and a payload containing encrypted data (depicted in Fig. 2a as "E_k(DATA)"). (*Solana* 45; Keromytis Decl. ¶ 32.) Nothing in *Solana* describes or suggests that the communication includes a request for a network address. (Keromytis Decl. ¶ 32.) Moreover, the remaining two communications shown in Fig. 2a merely involve forwarding the communication from the S-DBS to the D-DBS and then from the D-DBS to the responder. (*Solana* 45-46; Keromytis Decl. ¶ 32.) Each of these communications includes the same header containing the same session key and UNI of the responder—the only difference being that the header is encrypted with the public key of the recipient during each communication (i.e., the public key of the destination domain during communication 2 and the public key of the responder during communication 3). (*Solana* 45-46; Keromytis Decl. ¶ 32.) Thus, none of the three communications shown in Fig. 2a describe a request for a network address.

Further, Fig. 2a does not disclose "a domain name service system configured to . . . receive a query for a network address," because the alleged domain name service system (*Solana*'s DS) does not receive the alleged query for a network address. In particular, *Solana* discloses that the configuration of Fig. 2a "is particularly convenient for principals lacking access to a global DS." (*Solana* 46; Keromytis Decl. ¶ 33.) In other words, the DS—the alleged domain name service system—is not involved in the method disclosed in Fig. 2a. (Keromytis Decl. ¶ 33.) Thus, Fig. 2a does not disclose "a domain name service system configured . . . to receive a query for a network address," as recited in claim 1.

Third, Fig. 2b of *Solana* also does not disclose a domain name service system configured to receive a query for a network address. With respect to Fig. 2b, the Request and the Office Action cite the three communications described in connection with Fig. 2b, and assert that "*Solana* thus describes secure DNS systems that act on requests for network addresses and associated information." (Req. at 44.)

But just like Fig. 2a, Fig. 2b does not disclose any queries for network addresses, let alone the recited domain name service system configured to receive a query for a network address. For example, *Solana* explains that the first communication in Fig. 2b includes the initiator generating the same header as in the first communication in Fig. 2a. (*Solana* 46; Keromytis Decl. ¶ 34.) Then, the initiator issues a "DS query *to obtain the destination domain public key for header encryption.*"

(*Solana* 46, emphasis added; Keromytis Decl. ¶ 34.) Thus, the only query issued by the initiator is a query for a public key, and not a query for a network address. (*Solana* 46; Keromytis Decl. ¶ 34.)

Because, as explained above, *Solana* fails to disclose "a domain name service system configured to . . . receive a query for a network address," as recited in independent claim 1, *Solana* does not anticipate claim 1.

(3) *Solana* Does Not Teach "a Domain Name Service System Configured to . . . Comprise an Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

Independent claim 1 recites "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link." The Request and the Office Action assert that *Solana* discloses this feature because: (1) *Solana* teaches that its system includes "a Domain Key Holder (DKH) and a Domain Border System (DBS) that manage and use keys/certificates to handle authentication and encryption functions"; and (2) "the patent owner has asserted that the use of certificates in connection with establishment of secure communication links comprises an 'indication' that a DNS system can support secure communications." (Req. at 45.) These positions are incorrect because *Solana* does not disclose the domain name service system recited in claim 1.

As discussed above, *Solana* does not disclose the recited domain name service system because *Solana* does not disclose a system configured to (1) store a plurality of domain names and corresponding network addresses or (2) receive a query for a network address. Because *Solana* does not describe a domain name service system, it cannot disclose an indication that a domain name service system supports establishing a secure communication link, as recited in claim 1.

The Request and the Office Action suggest that the keys and certificates in *Solana* are indications that the DS, DKH, and DBS of *Solana* support establishing the alleged secure communication link. But no combination of *Solana*'s DS, DKH, or DBS can be the recited domain name service system because none of these components are configured to (1) store a plurality of domain names and corresponding network addresses or (2) receive a query for a network address, as for example recited in claim 1 of the '504 patent. Moreover, one of ordinary skill in the art at the time of the application for the '504 patent would not have understood the DS, DKH, or DBS to be a domain name service system. (Keromytis Decl. ¶ 36.) As discussed above, the DS described by *Solana* does not store a plurality of domain names and corresponding network addresses or receive a query for a network address. Indeed, the Request and the Office Action do not show how the DKH and DBS disclosed by *Solana* include these features. That is because they do not. And, thus, they

could not, in the eyes of one of ordinary skill in the art, be considered a domain name service system, as recited in claim 1. (*Id.*)

In addition, it is irrelevant whether—as the Request and Office Action assert—"the patent owner has asserted that the use of certificates in connection with establishment of secure communication links comprises an 'indication' that a DNS system can support secure communications." (Req. at 45.) The certificates and keys disclosed by *Solana* and relied upon by the Office Action are distributed by systems that are not domain name service systems, as recited in claim 1. (*See supra* Sections II.C.1.b.1 and II.C.1.b.2.)

Thus, for at least the reasons set forth above, *Solana* does not disclose "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in independent claim 1.

Based on the foregoing, because *Solana* fails to disclose the aforementioned features of claim 1, claim 1 is not anticipated by *Solana*. Accordingly, Patent Owner requests that the rejection of claim 1 under 35 U.S.C. § 102 be withdrawn, and the patentability of claim 1 should be confirmed.

c) *Solana* Does Not Disclose the Elements of Independent Claims 36 and 60

Independent claims 36 and 60 include recitations similar to those described above with respect to claim 1. For example, claim 36 recites "instructions executable in a domain name service system, the instructions comprising code for: . . . storing a plurality of domain names and corresponding network addresses; receiving a query for a network address; and supporting an indication that the domain name service system supports establishing a secure communication link." And claim 60 recites, for example, "storing a plurality of domain names and corresponding network addresses," "receiving a query for a network address," and "the domain name service system comprising an indication that the domain name service system supports establishing a secure communication link." As explained above, *Solana* does not disclose these features. Thus, for reasons similar to those discussed above in connection with independent claim 1, *Solana* does not anticipate claims 36 and 60. Accordingly, for similar reasons, Patent Owner requests that the rejection of claims 36 and 60 under 35 U.S.C. § 102 be withdrawn, and the patentability of the claims should be confirmed.

2. Independent Claims 1, 36, and 60 Are Patentable over *Solana* in View of RFC 2504 (Ground 5)

The Office Action rejects claims 1, 36, and 60 as being obvious over *Solana* in view of RFC 2504 (Ground 5). (OA at 4-6.) However, these rejections should be withdrawn because RFC 2504

does not make up for the above-noted deficiencies of *Solana*, and RFC 2504 does not disclose an indication that the domain name service system supports establishing a secure communication link.

To begin with, RFC 2504 does not make up for the deficiencies of *Solana* discussed above. In particular, RFC 2504 does not disclose at least (1) a domain name service system configured to store domain names and corresponding network addresses or (2) a domain name service system configured to receive a query for a network address, as recited in independent claim 1. Nor do the Request and the Office Action rely on RFC 2504 as allegedly disclosing these features. (*See, e.g.*, Req. at 89-92 (citing only to *Solana* for these features).) Because RFC 2504 does not disclose, and is not relied on as disclosing, these claimed features, combining RFC 2504 with *Solana* does not remedy *Solana*'s deficiencies. For at least these reasons, the rejection of claims 1, 36, and 60 as being obvious over *Solana* in view of RFC 2504 should be withdrawn and the claims should be found patentable.

Moreover, the Request and the Office Action are incorrect in alleging that RFC 2504 discloses an indication that the domain name service system supports establishing a secure communication link, as recited in independent claim 1. (*Id.* at 89-92.) RFC 2504 is a document that "provides guidance to the end-users of computer systems and networks about what they can do to keep their data and communication private." (RFC 2504 at 2.) As such, RFC 2504's focus is with end-user functionality and steps that end-users can take to protect their network communications. (*See* RFC 2504; Keromytis Decl. ¶ 39.) RFC 2504 does not discuss DNS functionality. (Keromytis Decl. ¶ 39.) Moreover, RFC 2504 does not disclose the recited domain name service system of claim 1 at least because RFC 2504 does not disclose storing domain names and corresponding network addresses or receiving a query for a network address. (*Id.*) Because RFC 2504 does not disclose a domain name service system, it does not disclose an indication that *the domain name service system* supports establishing a secure communication link, as recited by claim 1. (*Id.*)

The Request and the Office Action also assert that "the use of visible indications, such as a 'lock' or 'key' icon through a web browser," disclose such an indication. (Req. at 91.) But whatever the lock or key icons of RFC 2504 indicate, they do not indicate that *the domain name service system* supports establishing a secure communication link, because no such domain name service system is disclosed in RFC 2504. (Keromytis Decl. ¶ 40.)

As such, *Solana* in view of RFC 2504 fails to disclose or suggest a domain name service system configured to store domain names and corresponding network addresses, receive a query for a network address, and comprise an indication that the domain name service system supports establishing a secure communication link, as recited in independent claim 1. As such, *Solana* in view

of RFC 2504 does not render obvious claim 1.

Independent claims 36 and 60 include recitations similar to those described above with respect to claim 1. As explained above, *Solana* in view of RFC 2504 does not disclose or suggest a domain name service system configured to store domain names and corresponding network addresses, receive a query for a network address, and comprise an indication that the domain name service system supports establishing a secure communication link. Thus, for reasons similar to those discussed above in connection with independent claim 1, *Solana* in view of RFC 2504 does not render obvious claims 36 and 60.

Because, for at least the reasons set forth above, *Solana* in view of RFC 2504 does not render obvious claims 1, 36, and 60, the rejection of these claims under 35 U.S.C. § 103 over *Solana* in view of RFC 2504 should be withdrawn, and the claims should be confirmed as patentable.

3. Independent Claims 1, 36, and 60 Are Patentable over *Provino* (Ground No. 9)

The Office Action rejects claims 1, 36, and 60 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,557,037 to Provino ("*Provino*") (Ground No. 9). (OA at 7.) For the reasons discussed below, *Provino* does not disclose each and every feature of the claims, and thus the rejection should be withdrawn.

a) Overview of *Provino*

Provino discloses a system for connecting an external device to a device on a virtual private network via a secure tunnel between the external device and a firewall associated with the virtual private network. (*Provino* Abstract.) Referring to FIG. 1 of *Provino*, reproduced below, when an operator at a device 12(m) wishes to connect to a device 13 on the Internet, the operator inputs a human-readable address of the device 13, causing the device 12(m) to send a message to a name server 17 requesting the corresponding Internet address of the device 13. (*Id.* at 8:14-40, 11:5-11.) The name server 17 does not have the addresses of the devices 31 on the virtual private network 15, except for the address of the firewall 30 of the virtual private network 15. In response to a request for the Internet address of a device 31 on the virtual private network 15, the name server returns the Internet address of the firewall 30. (*Id.* at 10:45-55, 11:11-16.)

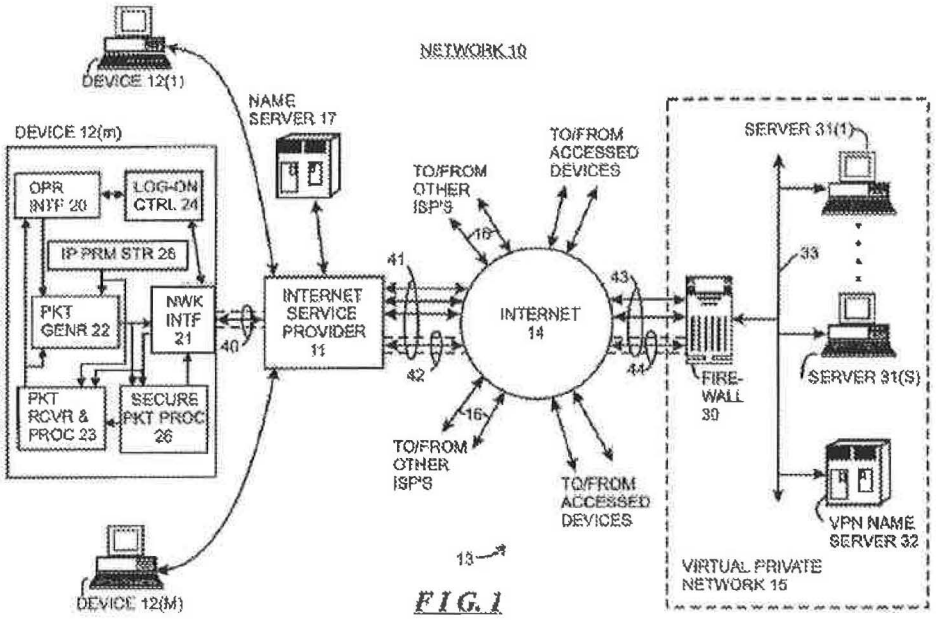


FIG. 1

The device 12(m) initiates establishment of a secure tunnel with the firewall 30. (*Id.* at 9:32-56, 10:56-58, 11:13-16.) Further, the firewall 30 provides the device 12(m) with the identification of a second name server 32 inside the virtual private network 15. (*Id.* at 10:62-63.) The device 12(m) sends, over the secure tunnel, a message to the second name server 32 requesting the Internet address of the device 31 on the virtual private network 31 corresponding to the human-readable address of the device 31. (*Id.* at 10:62-67, 11:17-26.) Thereafter, the device 12(m) is able to communicate with the device 31 on the virtual private network 15 via the secure tunnel.

b) *Provino* Does Not Disclose Each and Every Element of Independent Claims 1, 36, and 60

Independent claim 1 recites, among other things, "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link." *Provino* does not disclose at least these elements of claim 1.

The Request and the Office Action allege that "the identification of firewall 30 by name server 17 comprises an indication that the name server 17 supports establishing a secure communication link." (Req. at 122.) This is incorrect. As described in the summary above, *Provino*'s name server 17—which the Request and the Office Action allege discloses the claimed domain name service system—just resolves the Internet address of the firewall 30 in response to a request to resolve the human-readable address of the firewall 30. (Keromytis Decl. ¶ 44.) This is not an indication that the name server 17 (the alleged domain name service system) supports establishing a secure communication link, because the name server 17 resolves the requested Internet address of

any device 13 on the Internet (firewall 30 or otherwise), provided that is able to do so. (*Id.*) *Provino*'s name server 17 (the alleged domain name service system) operates just like a conventional domain name service system and does not have any additional functionality that could be considered to comprise an indication that the name server 17 supports establishing a secure communication link. Indeed, since the only disclosed capability of the name server 17 is to indiscriminately return a requested Internet address of a device, *Provino* does not even suggest that the name server 17 has the capability to support establishing a secure communication link. (*Id.*) Accordingly, *Provino*'s name server 17 returning a requested Internet address cannot comprise an indication that the name server 17 supports establishing a secure communication link, since *Provino* does not even disclose that it has that capability to begin with. (*Id.*) *Provino* cannot be viewed as disclosing indicating a feature when it is silent on that feature in the first place.

Supporting this conclusion, *Provino*'s alleged domain name service system (the name server 17) is consistent with a conventional domain name service system that the '504 patent distinguishes from a "domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (*See, e.g.*,'504 patent 39:7-42; Keromytis Decl. ¶ 45.) For example, the '504 patent indicates that a conventional domain name service system merely returns an IP address that was requested of it. (Keromytis Decl. ¶ 45.) In one embodiment, the '504 patent explains that "[c]onventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a *requested* computer or host. For example, when a computer user types in the web name 'Yahoo.com,' the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser . . . ." ('504 patent 39:7-13 (emphasis added); Keromytis Decl. ¶ 45; *see also* '504 patent 39:14-42.) In another example, the '504 patent identifies a conventional domain name service system that stores public keys of different machines so that hosts can request and receive those public keys from the domain name service system. ('504 patent 39:34-42; Keromytis Decl. ¶ 45.) Similar to the conventional domain name systems described by the '504 patent, the name server 17 of *Provino* merely returns a requested Internet address of a device corresponding to the human-readable address of that device, such as the requested IP address corresponding to a domain name like "Yahoo.com." (*Compare Provino* 8:48-51 *with* '504 patent 39:7-13. *See also* Keromytis Decl. ¶ 45.)

The '504 patent recognizes that such conventional domain name systems suffer from certain drawbacks and thus discloses embodiments that address them, including "a domain name service system configured to . . . comprise an indication that the domain name service system supports

establishing a secure communication link," as recited in claim 1. (*See, e.g.*, '504 patent 39:43-41:61; Keromytis Decl. ¶ 46.) And since *Provino*'s alleged domain name service system (the name server 17) is a mere conventional domain name server of the type distinguished by the '504 patent, one of ordinary skill in the art would not have understood *Provino* to disclose or suggest "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1.

The rejection of claim 1 in view of *Provino* is further misplaced because it improperly relies on a misinterpretation of the language of claim 1. For instance, in attempting to map aspects of *Provino* onto claim 1, the Request and the Office Action allege that "*Provino* shows the authorization and engagement of device 12(m) through the firewall comprises an indication of a secure communication link discernible to a user." (Req. at 122.) Apparently as part of this assertion, they further allege that "*Provino* also teaches the engagement of device 12(m) to include provision of the decryption algorithm and associated decryption key from the firewall 30 to use in decrypting message packets from the VPN." (*Id.*)

Claim 1, however, does not recite "an indication of a secure communication link discernible to a user." Claim 1 instead recites "an indication that the domain name service system supports establishing a secure communication link." Even if *Provino*'s alleged "authorization and engagement" discloses "an indication of a secure communication link discernible to a user," as alleged, it does not disclose "an indication that *the domain name service system* supports establishing a secure communication link" (emphasis added), as recited in claim 1. (Keromytis Decl. ¶ 48.) As discussed, *Provino* does not teach that the alleged domain name service system (the name server 17) even has the capability to support establishing a secure communication link, and, thus, the reference cannot disclose any indication that the domain name service system supports establishing a secure communication link, as recited in claim 1.

In addition, based on the excerpts of *Provino* cited in Request and the Office Action, it appears that the alleged "authorization and engagement" refers to the process in which the device 12(m) and the firewall 30 engage to establish the secure tunnel (i.e., the alleged secure communication link). (*See Provino* 9:46-10:12; Keromytis Decl. ¶ 49.) This process, however, does not involve the alleged domain name service system in *Provino* (the name server 17), and thus cannot disclose or suggest "a *domain name service system* configured to . . . comprise an indication that the *domain name service system* supports establishing a secure communication link" (emphases added), as recited in claim 1. (Keromytis Decl. ¶ 49.) Just because the device 12(m) and the firewall 30 establish a secure tunnel does not mean that the alleged *domain name service system* is configured to

comprise an indication that the *domain name service system* supports establishing a secure communication link, as recited in independent claim 1. (*Id.*)

For the foregoing reasons, *Provino* fails to disclose all of the elements of claim 1, and *Provino* does not anticipate the claim. Thus, the rejection of claim 1 under 35 U.S.C. § 102 should be withdrawn, and the patentability of claim 1 should be confirmed.

Additionally, independent claims 36 and 60 include recitations similar to those discussed above in connection with claim 1. For example, claim 36 recites "[a] machine-readable medium comprising instructions executable in a domain name service system, the instructions comprising code for . . . supporting an indication that the domain name service system supports establishing a secure communication link." And claim 60 recites "[a] method of providing a domain name service for establishing a secure communication link . . . the domain name service system comprising an indication that the domain name service system supports establishing a secure communication link." Thus, for at least reasons similar to those described above in connection with claim 1, *Provino* does not anticipate claims 36 and 60. As such, the rejection of claims 36 and 60 under 35 U.S.C. § 102 should be withdrawn, and the patentability of the claims should be confirmed.

4. Independent Claims 1, 36, and 60 Are Patentable over *Provino* in View of RFC 2230 (Ground 13)

The Office Action rejects claims 1, 36, and 60 as being obvious over *Provino* in view of RFC 2230 (Ground 13). (OA at 8.) This rejection should also be withdrawn and the claims should be confirmed.

As discussed in the preceding section, *Provino* does not disclose at least "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited by independent claim 1. Moreover, RFC 2230 does not remedy the deficiencies of *Provino* because, as discussed in detail in Section II.C.7, *infra*, RFC 2230 also fails to disclose or suggest a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link. As such, any combination of *Provino* and RFC 2230 still fails to disclose or suggest at least a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link, as recited in independent claim 1. In addition, since independent claims 36 and 60 recite features similar to independent claim 1, any combination of *Provino* and RFC 2230 fails to disclose or suggest all of the elements of these claims as well.

Based on the foregoing, Patent Owner respectfully submits that because the proposed

combination of *Provino* and RFC 2230 fails to disclose the claimed elements of each of claims 1, 36, and 60, those claims would not have been obvious over *Provino* in view of RFC 2230 under 35 U.S.C. § 103. Accordingly, the rejection should be withdrawn, and the patentability of claims 1, 36, and 60 should be confirmed.

5. Independent Claims 1, 36, and 60 Are Patentable over *Provino* in View of RFC 2504 (Ground 17)

The Office Action rejects claims 1, 36, and 60 as being obvious over *Provino* in view of RFC 2504 (Ground 17). (OA at 8.) As discussed below, these rejections should be withdrawn at least because RFC 2504 does not make up for the above-noted deficiencies of *Provino*.

The Request and the Office Action rely on RFC 2504 solely to allegedly show an indication that the domain name service system supports establishing a secure communication link. (Req. at 198-99.) However, as discussed above with respect to the rejection of *Solana* in view of RFC 2504, RFC 2504 does not disclose an indication that the domain name service system supports establishing a secure communication link, as recited in independent claim 1. Instead, RFC 2504 is a document that "provides guidance to the end-users of computer systems and networks about what they can do to keep their data and communication private." (RFC 2504 at 2.) As such, RFC 2504 is primarily concerned with end-user functionality and steps that end-users can take to protect their network communications. (*See* RFC 2504; Keromytis Decl. ¶ 53.) RFC 2504 does not discuss DNS functionality. (Keromytis Decl. ¶ 53.) Moreover, RFC 2504 does not disclose storing domain names and corresponding network addresses or receiving a query for a network address. (*Id.*) Because RFC 2504 does not disclose a domain name service system, RFC 2504 cannot disclose an indication that the domain name service system supports establishing a secure communication link, as required by claim 1. (*Id.*)

Further, the Request and the Office Action assert that "the use of visible indications, such as a 'lock' or 'key' icon through a web browser" disclose such an indication. (Req. at 198-99.) But whatever the lock or key icons of RFC 2504 indicate, they do not indicate that *the domain name service system* supports establishing a secure communication link, because no such domain name service system is disclosed in RFC 2504. (Keromytis Decl. ¶ 54.)

As such, *Provino* in view of RFC 2504 does not disclose or suggest at least a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link, as recited in independent claim 1, and the similar features recited in independent claims 36 and 60. Based on the foregoing, *Provino* in view of RFC 2504 does not render obvious claims 1, 36, and 60 under 35 U.S.C. § 103. Accordingly, the rejection of claims

1, 36, and 60 under this basis should be withdrawn, and the claims should be confirmed as patentable.

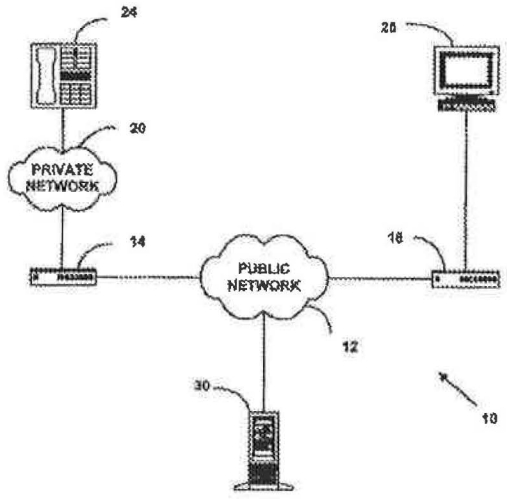
6. Independent Claims 1, 36, and 60 Are Patentable over *Beser* (Ground 21)

The Office Action rejects claims 1, 36, and 60 under § 102(e) as being anticipated by U.S. Patent No. 6,496,867 to Beser et al. ("*Beser*") (Ground 21). (OA at 9.) For the reasons discussed below, the rejection fails to establish that *Beser* discloses each and every feature of the claims, and thus should be withdrawn.

a) Overview of *Beser*

Beser discloses a system for initiating a tunneling connection that hides the identity of the originating and terminating ends of the tunneling association from other users. (*Beser* Abstract.) With reference to Fig. 1, reproduced below, *Beser* discloses that a first network device 14 informs a trusted-third-party network device 30 of a request to initiate a tunneling connection received from an originating telephony device 24. (*Beser* 7:62-8:4, 10:2-6, 11:9-10.)

FIG. 1



The request to initiate a tunneling connection includes a unique identifier for a terminating telephony device 26. (*Id.* at 10:4-6.) After being informed of the request, trusted-third-party network device 30 associates an identifier of terminating telephony device 26 with a public IP address of a second network device 16. (*Id.* at 11:26-32.) Then, private IP addresses for each of the originating telephony device 24 and the terminating telephony device 26 are negotiated and distributed to the second network device 16 and the first network device 14, respectively. (*See, e.g.*, *id.* at 11:59-

12:54.) This way, the tunneling connection "hides the identity of the originating and terminating ends of the tunneling association from the other users of the public network." (*Id.* at 2:36-39.)

b) *Beser* Does Not Disclose "a Domain Name Service System Configured . . . to Comprise an Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

For at least the two reasons discussed below, *Beser* fails to disclose "a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link," as recited in independent claim 1.

First, *Beser* does not disclose a secure communication link and, thus, cannot disclose an indication that the domain name service system supports establishing a secure communication link. The Request and the Office Action assert that *Beser* discloses a secure communication link by negotiating "first and second private IP addresses . . . in a manner to ensure anonymity and hide the identities of the originating and terminating devices . . . ." (Req. at 231.) This is incorrect.

Specifically, *Beser* does not disclose establishing a secure communication link between the originating and terminating devices because *Beser* does not disclose that the communication between these two devices is encrypted. Instead, *Beser* discloses establishing a tunneling association that merely hides the identity of the originating and terminating ends of the tunneling association from the other users of a public network. (*Beser* 2:36-39; Keromytis Decl. ¶¶ 55, 58; *see also* Req. at 231.) But the communication between these two devices is not encrypted and, thus, no secure communication link is established. (Keromytis Decl. ¶¶ 57-58.) In fact, *Beser* acknowledges that encryption exists, but teaches away from using it in the configurations disclosed by *Beser* because, according to *Beser*, encryption may provide insufficient protection, may be infeasible to implement, and/or may create service problems due to computer-power limitations. (*Beser* 1:54-67; Keromytis Decl. ¶ 58). Thus, one of ordinary skill in the art, when reading *Beser*, would understand that *Beser*'s tunneling technique does not establish a secure communication link, but instead provides an alternative to establishing one. (Keromytis Decl. ¶ 58.)

One of ordinary skill in the art would have understood a secure communication link to require encryption. (*Id.*) For example, the '504 patent explains that "[d]ata security is usually tackled using *some form of data encryption*." ('504 patent 1:55-56, emphasis added.) Moreover, in the ongoing litigation involving the '504 patent, the Requester agreed with Patent Owner that a secure communication link requires encryption. (*See* Ex. A-2 at 2-4, 10-11 (where the Requester proposed that "secure communication link" be construed to require both encryption and anonymity by proposing a construction of "virtual private network communication link").) Thus, both Patent

Owner and the Requester agree that a secure communication link requires encryption.

Second, *Beser* fails to disclose that the domain name service system comprises an *indication* that the domain name service system supports establishing a secure communication link. The Request and the Office Action assert that Beser's "negotiation" discloses the claimed indication. (Req. at 231-32.) This is incorrect. Beser's "negotiation" is merely a distribution of network addresses. (Keromytis Decl. ¶ 60.) For example, the trusted-third-party network device 30 forwards the public and private IP addresses of the first network device to the second network device, and vice versa. (*See Beser* 13:10-14:33, Fig. 9; Keromytis Decl. ¶ 60.) But merely distributing IP addresses to the first and second network devices is not an "indication that the domain name service system supports establishing a secure communication link." (Keromytis Decl. ¶ 60.) At most, *Beser* merely shows that the trusted-third-party network device 30 is configured to distribute IP addresses to entities seeking them.

For the foregoing reasons, *Beser* fails to disclose all of the elements of claim 1 and does not anticipate the claim. Thus, the rejection of claim 1 under 35 U.S.C. § 102 should be withdrawn, and the patentability of claim 1 should be confirmed.

Additionally, independent claims 36 and 60 recite similar elements as those highlighted above with respect to claim 1. For example, claim 36 recites "instructions executable in a domain name service system, the instructions comprising code for: . . . receiving a query for a network address; and supporting an indication that the domain name service system supports establishing a secure communication link." And claim 60 recites "receiving a query for a network address," and "the domain name service system comprising an indication that the domain name service system supports establishing a secure communication link." Thus, *Beser* does not anticipate claims 36 and 60 for reasons similar to those reasons discussed above for independent claim 1. Accordingly, Patent Owner requests that the rejection of claims 36 and 60 under 35 U.S.C. § 102 be withdrawn, and the patentability of these claims should be confirmed.

7. Independent Claims 1, 36, and 60 Are Patentable over RFC 2230 (Ground 25)

The Office Action rejects claims 1, 36, and 60 under 35 U.S.C. § 102(b) as being anticipated by RFC 2230 (Ground 25). (OA at 10.) As discussed above, RFC 2230 has not been shown to be prior art under 35 U.S.C. § 102 and thus is not an anticipating reference to any '504 patent claim. In addition, for the reasons discussed below, even if RFC 2230 were properly shown to be prior art to the '504 patent, the reference does not disclose each and every feature of the claims, and thus the rejection should be withdrawn.

a) Overview of RFC 2230

RFC 2230 discloses a mechanism to delegate authorization for one node to act as a key exchanger for a second node. (RFC 2230 at 1.) In particular, RFC 2230 "specifies a new kind of DNS Resource Record (RR), known as the Key Exchanger (KX) record." (*Id.* at 2.) "The KX record is useful in providing an authenticatible method of delegating authorisation for one node to provide key exchange services on behalf of one or more, possibly different, nodes." (*Id.* at 1.)

Figure 1 of RFC 2230, reproduced below, shows a Subnet-to-Subnet Example of key exchange delegation. (*Id.* at 3.) When an originating node S sends packets to a destination node D, an IPsec router R1 for originating node S decides whether to provide IPsec service for the traffic. (*Id.* at 2-3.) If R1 has decided that traffic from S to D should be protected, it performs a DNS lookup for the records associated with the domain of D. (*Id.* at 3.) If R1 only knows the IP address for D, then it first performs a reverse DNS lookup to determine the domain of D before it performs the DNS lookup for the records associated with the domain of D. (*Id.*)

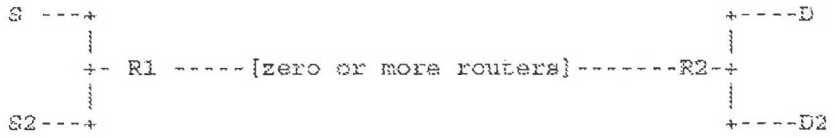


Figure 1: Network Diagram for Subnet-to-Subnet Example

KX record(s) returned from the DNS lookup indicate(s) a set of one or more delegated key exchangers for the domain of D—in this case, R2. (*Id.*) Based on the KX record including the domain name of R2 as the delegated key exchanger for D, R1 selects R2 as a key exchanger and "initiates a key management session with that key exchanger (in this example, R2)." (*Id.*) A KX record has the following syntax:

```
<domain-name>  IN  KX  <preference> <domain-name>
```

which means that "Internet nodes about to initiate a key exchange with <domain-name 1> should instead contact <domain-name 2> to initiate the key exchange for a security service between the initiator and <domain-name 2>." (*Id.* at 8.)

R2 then performs a KX record lookup on S to confirm that R1 is the delegated key exchanger for S. (*Id.* at 3-4.) Then, "[i]f the proposed IPsec Security Association is acceptable to both R1 and R2, each of which might have separate policies, then they create that IPsec Security Association via Key Management." (*Id.* at 4.)

b) RFC 2230 Does Not Disclose Each and Every Element of Independent Claim 1

Independent claim 1 recites "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link." RFC 2230 does not disclose at least these elements of claim 1.

The Request and the Office Action propose two alternatives for why RFC 2230 allegedly discloses a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link. (Req. at 280-81.) First, they allege that "[t]he secure DNS systems described in RFC 2230 include indications, via the KX resource record, that the systems support establishing secure communication links." (*Id.* at 280.) Second, the Request and the Office Action allege that "during the establishment of the IPSec Security Association, a further indication is provided that the secure DNS systems support establishing a secure communication link." (*Id.*) The Request and Office Action are incorrect on both counts for the following reasons.

(1) A KX Resource Record Is Not "an Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

The KX record in RFC 2230 is not an indication that the alleged *domain name service system* supports establishing a secure communication link, as recited in claim 1. (Keromytis Decl. ¶ 65.) Instead, as described above, the KX record includes the domain name of a *delegated key exchanger node* (e.g., R2). (*Id.*) Specifically, the KX record includes domain name(s) of a "*set of nodes* [that] are authorised key exchanger nodes for the destination D." (RFC 2230 at 3, emphasis added; Keromytis Decl. ¶ 65.) RFC 2230 specifies that the delegated key exchanger nodes are the "IPsec-capable routers" R1 and R2 or the IPsec-capable router R1 and the destination node D itself, depending upon the configuration (Subnet-to-Subnet, Subnet-to-Host, or Host-to-Subnet). (RFC 2230 at 2-5; Keromytis Decl. ¶ 65.) But based on the description in RFC 2230, one of ordinary skill in the art would have understood that the IPsec-capable routers R1 and R2 and the destination node D are *separate* from the alleged domain name service system to which the DNS lookup was sent and from which the KX record was obtained. (Keromytis Decl. ¶ 65.) Thus, the KX record includes the domain name of a delegated device, *separate* from the alleged domain name service system, which is capable of key management. Accordingly, one of ordinary skill in the art would not have understood the KX record to comprise an indication that the *domain name service system* supports establishing a secure communication link. (*Id.*) While including the domain name of a certain delegated IPsec node capable of key exchange, the KX record includes no indication about the capabilities of the alleged domain name service system itself, and certainly does not include an indication that the

domain name service system supports establishing a secure communication link, as recited in claim 1. (*Id.*)

Indeed, the alleged domain name service system disclosed by RFC 2230 does not support establishing a secure communication link because it merely returns a KX record when one is requested. (*Id.*) RFC 2230 does not disclose that the alleged domain name service system does anything else, and does not disclose that it supports establishing a secure communication link. RFC 2230 cannot be viewed as disclosing that a domain name service system comprises an indication that it supports establishing a secure communication link when the reference does not even teach that the alleged domain name service has the capability to support establishing a secure communication link to begin with. (*Id.*)

(2) The Alleged Establishment and Use of an IPsec Security Association Is Not "an Indication that the Domain Name Service System Supports Establishing a Secure Communication Link"

According to the Request and the Office Action, "during the establishment of the IPSec Security Association, a further indication is provided that the secure DNS systems support establishing a secure communication link." (Req. at 280.) To support this assertion, the Request and the Office Action block-quote the first four paragraphs of RFC 2230, page 5 (section 2.1.2 Subnet-to-Host Example), and then state, "Thus, D verifies the authorization and permits creation of an IPSec Security Association on behalf of S. This indication supports establishment of the secure communication link between 'S' and 'D.'" (*Id.* at 280-81.)

The quoted passage of RFC 2230 explains how, in the Subnet-to-Host Example, "D can verify that R1 is authorised to create an IPsec Security Association" before R1 engages in key exchange with the destination D. (RFC 2230 at 5; Keromytis Decl. ¶ 67.) The destination D does this by requesting a "forward DNS lookup on S to locate the KX records for S." (RFC 2230 at 5; Keromytis Decl. ¶ 67.) The destination D will engage in key management with R1 so long as the returned KX record "indicate[s] that R1 is an authorised key exchanger for S." (RFC 2230 at 5; Keromytis Decl. ¶ 67.)

As discussed above, however, a KX record does not comprise an indication that the alleged *domain name service system* supports establishing a secure communication link, as recited in claim 1. Based on RFC 2230, one of ordinary skill in the art would have understood a KX record to include the domain name of a device, *separate* from the alleged domain name service system, that supports key management for the source S rather than to indicate whether the alleged domain name service supports establishing a secure communication link. For instance, in the example cited by the Request

and the Office Action, the returned KX record must include the domain name of *R1* before the destination D will proceed with key management. (RFC 2230 at 5, emphasis added; Keromytis Decl. ¶ 68.) Accordingly, one of ordinary skill in the art would have understood the KX record to include the domain name of a *separate IPsec router R1* capable of key exchange on behalf of the source S, not to indicate the alleged *domain name service system* supports establishing a secure communication link. (Keromytis Decl. ¶ 68.) Thus, the destination D's verification that R1 is the authorized key exchanger for the source S in RFC 2230 does not disclose the claimed domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link, as recited in claim 1. (*Id.*)

In addition, one of ordinary skill in the art would not have understood the creation and use of the IPsec Security Association between D and R1 to disclose an indication that the alleged domain name service system supports establishing a secure communication link. (*Id.* ¶ 69.) As explained, one of ordinary skill in the art would have understood the destination D and the IPsec router R1 as *separate* from the alleged domain name service system, and thus would not have viewed the establishment and use of an IPsec Security Association between these devices to comprise an indication that the alleged *domain name service* system supports establishing a secure communication link. (*Id.*)

(3) RFC 2230 Discloses a Conventional Domain Name Service System Distinguished by the '504 Patent

Confirming the conclusions above, the alleged domain name service system in RFC 2230 is consistent with a conventional domain name service system that the '504 patent distinguishes from a "domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (*See, e.g.*,'504 patent 39:7-42; Keromytis Decl. ¶ 70.) As discussed, the '504 patent indicates that a conventional domain name service system merely returns an IP address or public key that was requested of it. (Keromytis Decl. ¶ 70.) For instance, the '504 patent explains that "[c]onventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a *requested* computer or host. For example, when a computer user types in the web name 'Yahoo.com,' the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser . . . ." ('504 patent 39:7-13, emphasis added; Keromytis Decl. ¶ 70; *see also* '504 patent 39:14-42.) In another example, the '504 patent identifies conventional domain name service systems that store public keys of different machines so that hosts can request and receive those public keys from the domain name service system. ('504 patent 39:34-42; Keromytis

Decl. ¶ 70.) Similar to the conventional domain name systems described by the '504 patent, the domain name service system described in RFC 2230 merely returns a KX resource record requested for a particular domain name. (*See, e.g.*, RFC 2230 at 3; Keromytis Decl. ¶ 70.)

The '504 patent recognizes that such conventional domain name systems suffer from certain drawbacks and thus discloses embodiments that address them, including "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (*See, e.g.*, '504 patent 39:43-41:61; Keromytis Decl. ¶ 71.) And since RFC 2230's alleged domain name service system is a mere conventional domain name server of the type distinguished by the '504 patent, one of ordinary skill in the art would not have understood RFC 2230 to disclose or suggest a domain name service system configured to comprise an indication that the domain name service system supports establishing a secure communication link, as recited in claim 1.

For the foregoing reasons, RFC 2230 fails to disclose all of the elements of claim 1, and RFC 2230 does not anticipate the claim. Thus, the rejection of claim 1 under 35 U.S.C. § 102 based on RFC 2230 should be withdrawn, and the patentability of claim 1 should be confirmed.

Additionally, independent claims 36 and 60 include recitations similar to those discussed above in connection with claim 1. For example, claim 36 recites "[a] machine-readable medium comprising instructions executable in a domain name service system, the instructions comprising code for . . . supporting an indication that the domain name service system supports establishing a secure communication link." And claim 60 recites "[a] method of providing a domain name service for establishing a secure communication link . . . the domain name service system comprising an indication that the domain name service system supports establishing a secure communication link." Thus, for at least reasons similar to those described above in connection with claim 1, RFC 2230 does not anticipate claims 36 and 60. As such, the rejection of claims 36 and 60 under 35 U.S.C. § 102 should be withdrawn, and the patentability of the claims should be confirmed.

8. Independent Claims 1, 36, and 60 Are Patentable over RFC 2538 (Ground 30)

The Office Action rejects claims 1, 36, and 60 under 35 U.S.C. § 102(e) as being anticipated by RFC 2538 (Ground 30). (OA at 12.) As discussed above, RFC 2538 has not been shown to be prior art under 35 U.S.C. § 102 and thus is not an anticipating reference to any '504 patent claim. In addition, for the reasons discussed below, even if RFC 2538 were properly shown to be prior art to the '504 patent, the reference does not disclose each and every feature of the claims, and thus the rejection should be withdrawn.

a) Overview of RFC 2538

RFC 2538 discloses a domain name system resource record ("RR"), the CERT RR, for storing certificates in the DNS. (RFC 2538 at 1.) RFC 2538 describes a certificate as "a binding . . . of a public key . . . and identity, authorization, or other information." (*Id.* at 2.) RFC 2538 recommends storing CERT RRs in the DNS under a domain name of the entity that controls the private key corresponding to the public key being certified. (*Id.* at 5.) According to the Request, "[t]his permits the system to provide, in response to a query with respect to the particular domain name, the appropriate public key certificate associated with that domain." (Req. at 324.)

b) RFC 2538 Does Not Disclose Each and Every Element of Independent Claims 1, 36, and 60

Independent claim 1 recites, among other things, "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link." The Request and the Office Action assert that the CERT RR of RFC 2538 discloses the recited "indication that the domain name service system supports establishing a secure communication link." (Req. at 324-25.) This is incorrect.

To begin with, the Request suggests that the DNS server that stores the CERT RR is the claimed domain name service system. (*Id.* at 322-24.) But the certificate in a CERT RR merely binds a public key to some "identity, authorization, or other information." (RFC 2538 at 2; Keromytis Decl. ¶ 74.) It does not include any indication about the capabilities of the DNS server in which the certificate is stored. (Keromytis Decl. ¶ 74.) RFC 2459, relied on by the Request, discloses the basic syntax for one type of certificate mentioned in RFC 2538—the X.509 certificate. However, nothing in the basic syntax includes any information that indicates that the DNS server supports establishing a secure communication link. (RFC 2459 at 15-24; Keromytis Decl. ¶ 74.) Indeed, the DNS server disclosed by RFC 2538 does not support establishing a secure communication link—it merely returns a certificate when one is requested. (Keromytis Decl. ¶ 74.) RFC 2538 does not disclose that the DNS server does anything else, and certainly does not disclose that it supports establishing a secure communication link. (*Id.*) As such, RFC 2538 cannot be viewed as disclosing that a domain name service system comprises an indication that the domain name service system supports establishing a secure communication link when the reference fails to disclose that the domain name service has the capability to support establishing a secure communication link to begin with.

In fact, RFC 2538's alleged domain name service system, the DNS, is consistent with a conventional domain name service system that the '504 patent distinguishes from a "domain name

service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (*See, e.g.*,'504 patent 39:7-42; Keromytis Decl. ¶ 75.) For example, the '504 patent indicates that a conventional domain name service system merely returns an IP address or public key that was requested of it. (Keromytis Decl. ¶ 75.) In one embodiment, the '504 patent explains that "[c]onventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host." ('504 patent 39:7-13; Keromytis Decl. ¶ 75; *see also*'504 patent 39:14-42.) In another example, the '504 patent identifies a conventional domain name server that stores public keys of different machines so that hosts can request and receive those public keys from the domain name service system. ('504 patent 39:34-42; Keromytis Decl. ¶ 75.) Similar to the conventional domain name servers described by the '504 patent, the DNS of RFC 2538 merely returns a CERT RR with a public key in response to a request for one. (*See, e.g.*, Req. at 324, stating "[t]his permits the system to provide, in response to a query with respect to the particular domain name, the appropriate public key certificate associated with that domain;" Keromytis Decl. ¶ 75.)

The '504 patent recognizes that such conventional domain name servers suffer from certain drawbacks and thus discloses embodiments that address them, including "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (*See, e.g.*, '504 patent 39:43-41:61; Keromytis Decl. ¶ 76.) And since RFC 2538's DNS (i.e., the alleged domain name service system) is a mere conventional domain name server of the type distinguished by the '504 patent, one of ordinary skill in the art would not have understood RFC 2538 to disclose or suggest "a domain name service system configured to . . . comprise an indication that the domain name service system supports establishing a secure communication link," as recited in claim 1. (Keromytis Decl. ¶ 76.)

Finally, the Request and Office Action incorrectly allege that "the patent owner has asserted that the use of certificates in connection with establishment of secure communication links comprises an 'indication' that a DNS system can support secure communications." (Req. at 325.) But the quotation relied upon by the Request and the Office Action includes no such admission:

> Further, in preparing devices for the FaceTime call, Apple's Server(s) ensure that the participant devices have local iPhone security certificates for use in verifying identity and otherwise securing the communication link. The audio/video stream in a FaceTime call is encrypted to create a secure communication link.

(*Id.* at 38, quoting Req. Ex. B2 at 7). Contrary to the Requester's representation, the above statement

shows no indication that Patent Owner believes that the mere presence of a public key certificate stored in a domain name server, such as that disclosed by RFC 2538, is an indication that a domain name service system supports establishing a secure communication link. Instead, as discussed above, the '504 patent specification itself recognizes that storing public key certificates in a domain name server is conventional.

For the foregoing reasons, RFC 2538 fails to disclose all of the elements of claim 1 and does not anticipate the claim. Thus, the rejection of claim 1 under 35 U.S.C. § 102 should be withdrawn, and the patentability of claim 1 should be confirmed.

Additionally, independent claims 36 and 60 include recitations similar to those discussed above in connection with claim 1. For example, claim 36 recites "[a] machine-readable medium comprising instructions executable in a domain name service system, the instructions comprising code for . . . supporting an indication that the domain name service system supports establishing a secure communication link." And claim 60 recites "[a] method of providing a domain name service for establishing a secure communication link . . . the domain name service system comprising an indication that the domain name service system supports establishing a secure communication link." Thus, for at least reasons similar to those described above in connection with claim 1, RFC 2538 does not anticipate claims 36 and 60. As such, the rejection of claims 36 and 60 under 35 U.S.C. § 102 should be withdrawn, and the patentability of the claims should be confirmed.

D. Dependent Claims 2-35 and 37- 59 Are Patentable over the Cited References (Grounds 1-35)

The Office Action also rejects dependent claims 2-35 and 37-59 on several grounds. Dependent claims 2-35 depend from independent claim 1, and dependent claims 37-59 depend from independent claim 36. As explained above, *Solana*, *Provino*, *Beser*, RFC 2230, RFC 2538, and/or RFC 2504, alone or in combination, do not disclose or suggest the features of claims 1 and 36, and thus do not support the rejections of those claims. The rejections of the above-listed dependent claims should also be withdrawn and the claims confirmed because the additional references cited against these claims do not remedy the deficiencies of the primary references discussed above with respect to independent claims 1 and 36. Nor does the Office Action allege that these additional references do so. Accordingly, for at least the reasons set forth above, the rejections of these claims should be withdrawn and the claims confirmed. Additionally, the dependent claims discussed below are also allowable for the additional reasons discussed below.

E. Dependent Claims 5, 23, and 47 Are Patentable over the Cited References

Dependent claim 5 recites that the "domain name service system is configured to authenticate the query [for a network address] . . . ." Similarly, dependent claim 23 recites that "the domain name service system is configured to authenticate the query for the network address," and dependent claim 47 recites that "the instructions [executable in a domain name service system] comprise code for authenticating the query for the network address." The Office Action rejects dependent claims 5, 23, and 47 on several grounds. Dependent claims 5, 23, and 47 each depend from independent claim 1 or 36, and are therefore also allowable at least by virtue of their dependence from one of these allowable claims. Thus, the rejections of claims 5, 23, and 47 should be withdrawn for the reasons discussed above with regard to the independent claims. In addition, the rejections should be withdrawn for at least the reasons discussed below.

1. Rejections Based on *Solana* (Grounds 1, 2, 5, and 6)

The Office Action rejects one or more of dependent claims 5, 23, and 47 as anticipated by *Solana* (Ground 1), and as being obvious over *Solana* in view of one or more combinations of RFC 920 and RFC 2504 (Grounds 2, 5, and 6). (OA at 5-6.) However, *Solana*, RFC 920, and/or RFC 2504, either alone or in combination, do not disclose or suggest the additional features of claims 5, 23, and 47, for the reasons discussed below.

In each of the rejections of claims 5, 23, and 47, the Office Action and the Request rely only on *Solana* as allegedly disclosing the subject matter of these claims, asserting that *Solana*'s source and destination domains are securely connected through an authenticated and encrypted channel. (*See* Req. at 46, 52, 66, 80, 92, 95, 103-04, 111.) However, as discussed above with regard to independent claim 1, *Solana* does not even disclose a query for a network address. Accordingly, *Solana* cannot disclose authenticating the query for a network address if it does not disclose the query in the first place.

RFC 920 and RFC 2504 do not make up for the above-noted deficiencies of *Solana*. Indeed, the Request and the Office Action do not even allege that they do. Because *Solana*, RFC 920, and RFC 2504 do not disclose authenticating a query for a network address, the references do not anticipate or render obvious claims 5, 23, and 47. As such, the rejections should be withdrawn and the claims confirmed.

2. Rejections Based on *Provino* (Grounds 9, 10, 13, 14, 17, and 18)

The Office Action rejects one or more of dependent claims 5, 23, and 47 as anticipated by *Provino* (Ground 9), and as being obvious over *Provino* in view of one or more of RFC 920, RFC 2230, and RFC 2504 (Grounds 10, 13, 14, 17, and 18). (OA at 7-9.) Dependent claims 5, 23, and 47

ultimately depend from one of independent claims 1 and 36, and are therefore also allowable at least by virtue of their dependence from these allowable claims, as discussed above. Moreover, *Provino*, RFC 920, RFC 2230, and/or RFC 2504, either alone or in combination, do not disclose or suggest the additional features of claims 5, 23, and 47, for the reasons discussed below.

In the rejections of claims 5, 23, and 47, the Office Action and the Request rely only on *Provino* as allegedly disclosing the subject matter of these claims. (*See, e.g.*, Req. at 168 (stating that "*Provino* also shows every feature of claim 5").) For example, regarding claim 5, the Request and the Office Action assert that *Provino* discloses the domain name service system configured to authenticate the query for the network address using a cryptographic technique because "Provino teaches systems that receive a query for a network address from the operator (and subsequently) from device 12(m). . . . This occurs during dialog between the initiating and responding entities." (*See, e.g.*, *id.* at 123.) To support their assertion, the Request and the Office Action block-quote a passage of *Provino* discussing the dialog between the device 12(m) and the firewall 30 that sets up the secure tunnel. (*Id.*, citing *Provino* 9:56-10:12.) The Request and the Office Action are incorrect.

The only encryption or decryption described in the cited passage of *Provino* refers to encrypting *message packets* sent between the device 12(m) and the firewall 30 over the secure tunnel. (*Provino* 9:56-10:12; Keromytis Decl. ¶ 78.) This encryption of message packets does not occur until the secure tunnel has been set up—*after* the device 12(m) has already sent the alleged query for the network address of the firewall 30 to the alleged domain name service system (name server 17). (Keromytis Decl. ¶ 78.) *Provino* does not disclose authenticating the alleged query for a network address, that is, the message sent to the name server 17 requesting the Internet address of a device corresponding to a provided human-readable address of that device. (*Id.*)

RFC 920, RFC 2230 and RFC 2504 do not make up for the above-noted deficiencies of *Provino*. Indeed, the Request and the Office Action do not even allege that they do. Because *Provino*, RFC 920, RFC 2230, and RFC 2504 do not disclose authenticating a query for a network address, the references do not anticipate or render obvious claims 5, 23, and 47. As such, the rejections should be withdrawn and the claims confirmed.

F. Dependent Claims 8 and 9 Are Patentable over the Cited References

Dependent claim 8 recites that the "domain name service system is connectable to a virtual private network through the communication network." Claim 9 depends from claim 8 and thus includes the features of claim 8. The Office Action rejects claims 8 and 9 on several grounds. Dependent claims 8 and 9 each depend from independent claim 1, and are therefore also allowable at least by virtue of their dependence from this allowable claim. Thus, the rejections of claims 8 and 9

should be withdrawn for the reasons discussed above with regard to the independent claims. In addition, the rejections should be withdrawn and the claims should be confirmed for at least the reasons discussed below.

1. Rejections Based on *Solana* (Grounds 1 and 5)

The Office Action rejects dependent claims 8 and 9 as anticipated by *Solana* (Ground 1), and as being obvious over *Solana* in view of RFC 2504 (Ground 5). (OA at 5-6.) *Solana* and RFC 2504, either alone or in combination, do not disclose or suggest the additional features of claims 8 and 9, for the reasons discussed below.

In each of the grounds of rejection, the Office Action and the Request rely only on *Solana* as allegedly disclosing the features of claim 8. (Req. at 47, 92-93.) Specifically, the Request and the Office Action assert that the following quotation from *Solana* discloses that the domain name service system is connectable to a virtual private network, as recited in claim 8: "organizations concerned by security issues conceive strong internal security policies and interact with the Internet through very restrictive firewalls or by means of well-protected Virtual Private Networks (VPN)." (Req. at 47, quoting *Solana* 38).) But this quotation only discloses that organizations may use virtual private networks. (Keromytis Decl. ¶ 79.) It does not disclose or suggest that the alleged domain name service system (*Solana*'s DS) is connectable to a virtual private network. (*Id.*) In fact, the quotation discussed above is the only time *Solana* mentions virtual private networks. That portion, or any other portion of *Solana*, does not disclose that the DS is connectable to a virtual private network. (*Id.*)

RFC 2504 does not make up for the above-noted deficiencies of *Solana*, and, as discussed, the Request and the Office Action do not assert that it does. As such, *Solana* and RFC 2504, either alone or in combination, do not anticipate or render obvious dependent claim 8, which is therefore allowable. Dependent claim 9 is also allowable at least by virtue of its dependence from claim 8, as well as for reciting additional features. Accordingly, Patent Owner requests that the rejections of claims 8 and 9 in view of *Solana* and/or RFC 2504 be withdrawn.

2. Rejections Based on *Provino* (Grounds 9, 13, and 17)

The Office Action rejects dependent claims 8 and 9 as anticipated by *Provino* (Ground 9), and as being obvious over *Provino* in view of one or more combinations of RFC 2230 and RFC 2504 (Grounds 13 and 17). (OA at 7-8.) *Provino*, RFC 2230, and/or RFC 2504, either alone or in combination, do not disclose or suggest the additional features of claims 8 and 9, for the reasons discussed below.

In each of the grounds of rejection of claims 8 and 9, the Office Action and the Request rely on *Provino* as allegedly disclosing the subject matter of these claims, asserting that "Fig.1 of *Provino* discloses secure DNS systems connectable to a virtual private network (15) through the communication network (Internet 14.)" (Req. at 124; *see id.* at 168, 199.) This is incorrect.

As discussed above, the Request and the Office Action allege that *Provino*'s name server 17 discloses the claimed domain name service system. But *Provino* does not teach that the name server 17 ever connects to *Provino*'s virtual private network 15 (the alleged virtual private network). (Keromytis Decl. ¶ 81.) In fact, it is the external device 12(m) rather than the name server 17 that connects to *Provino*'s virtual private network 14 over the secure tunnel with the firewall 30. (*Id.*) *Provino* just discloses that the name server 17 performs the conventional domain name service function of returning the Internet address of a device 13 on the Internet (e.g., firewall 30) in response to receiving a request from the external device 12(m) containing the human-readable address of that device. (*Id.*) The system diagram in Fig. 1 of *Provino* also does not show that the alleged domain name service system (name server 17) is connectable to the virtual private network 15. (*Id.*) Because the alleged domain name service system (*Provino*'s name server 17) is not taught to ever connect to the virtual private network 15, *Provino* fails to disclose that "the domain name service system is connectable to virtual private network through the communication network," as recited by dependent claim 8. (*Id.*)

Moreover, RFC 920 and RFC 2504 do not make up for the above-noted deficiencies of *Provino*. Indeed, the Request and the Office Action do not even allege that they do. Because *Provino*, RFC 920, and RFC 2504 also do not disclose that the alleged domain name service system is connectable to a virtual private network through the communication network, these references do not anticipate or render obvious dependent claim 8, which is therefore allowable. Dependent claim 9 is also allowable at least by virtue of its dependence from claim 8, as well as for reciting additional features. As such, the rejections should be withdrawn.

3. Rejections Based on *Beser* (Ground 23)

The Office Action rejects dependent claims 8 and 9 as being obvious over *Beser* in view of RFC 2401 (Ground 23). (OA at 10.) *Beser* and RFC 2401, either alone or in combination, do not disclose or suggest the additional features of claims 8 and 9, for the reasons discussed below.

In particular, *Beser* and RFC 2401 do not disclose that the "domain name service system is connectable to a virtual private network," as recited in dependent claim 8 and its dependent claim 9. The Request and the Office Action assert that *Beser* in view of RFC 2401 would have rendered this feature obvious because "RFC 2401 describes . . . a model where edge routers on two different

networks are used to establish the encrypted IP tunnel through which the network devices (*i.e.*, the 'first' and 'second' network devices of *Beser*) will communicate." (Req. at 270; Keromytis Decl. ¶ 82.) However, even if *Beser* and RFC 2401 were combined in the way asserted by the Request and Office Action, this combination would not disclose or suggest the subject matter of claim 8. (*Id.*) Instead, the proposed combination would allegedly result in a virtual private network between the *first and second network devices* of *Beser*. (*Id.*) As discussed above with respect to independent claim 1, the Request and the Office Action assert that the *trusted-third-party network device 30*, and not the *first and second network devices*, is the domain name service system. Thus, the asserted combination does not result in a domain name service system being connectable to a virtual private network, as recited in dependent claim 8 and its dependent claim 9. (*Id.*) Accordingly, the rejections of claims 8 and 9 under 35 U.S.C. § 103 should be withdrawn and the claims found patentable.

4. Rejections Based on RFC 2230 (Ground 27)

The Office Action rejects dependent claims 8 and 9 as being obvious over RFC 2230 in view of RFC 2401 (Ground 27). (OA at 11.) Moreover, RFC 2230 and RFC 2401, either alone or in combination, do not disclose the additional features of claims 8 and 9, for the reasons discussed below.

In particular, RFC 2230 and RFC 2401 do not disclose that the "domain name service system is connectable to a virtual private network," as recited in dependent claim 8 and its dependent claim 9. The Request and the Office Action assert that RFC 2230 in view of RFC 2401 would have rendered this feature obvious because "RFC 2401 describes . . . a model where edge routers on two different networks are used to establish the encrypted IP tunnel through which the network devices (*i.e.*, the 'S' and 'D' network devices of RFC 2230) will communicate." (Req. at 314.) However, even if RFC 2230 and RFC 2401 were combined in the way asserted by the Request and Office Action, this combination would not disclose or suggest the subject matter of claim 8 and its dependent claim 9. (Keromytis Decl. ¶ 83.) Instead, the Request and Office Action's combination would allegedly result in a virtual private network between *the originating device S and the destination device D* of RFC 2230. (*Id.*) As discussed above with respect to independent claim 1, one of ordinary skill in the art would have understood these devices to be *separate* from the alleged domain name service system (to which the KX record lookup is sent). (*Id.*) Thus, even if the combination were made, it would not result in the alleged domain name service system being connectable to a virtual private network, as recited in dependent claim 8 and its dependent claim 9. Accordingly, the rejection of these claims should be withdrawn.

5. Rejections Based on RFC 2538 (Ground 32)

The Office Action rejects dependent claims 8 and 9 as being obvious over RFC 2538 in view of RFC 2401 (Ground 32). (OA at 12.) RFC 2538 and RFC 2401, either alone or in combination, do not disclose the additional features of claims 8 and 9, for the reasons discussed below. Thus, the alleged combinations of RFC 2538 and RFC 2401 fail to disclose, suggest, or render obvious the elements of these claims.

The Request and the Office Action assert that the alleged combination of RFC 2538 with RFC 2401 would render obvious a domain name service system connectable to a virtual private network. (Req. at 354-55.) This is incorrect. As discussed, RFC 2538 merely discloses the use of CERT RRs for storing certificates in the domain name system. RFC 2401 discloses the IPsec protocol. (RFC 2401 at 2.) Neither reference discloses a domain name service system connectable to a virtual private network. (Keromytis Decl. ¶ 84.) Indeed, the Request and the Office Action assert that RFC 2401 discloses establishing a virtual private network between *network devices*. (*See* Req. at 355, stating "RFC 2401 describes . . . a model where edge routers on two different networks are used to establish the encrypted IP tunnel through which the network devices will communicate." *See also* Keromytis Decl. ¶ 84.) Nothing in RFC 2401 discloses or suggests that the described network devices are domain name service systems, let alone are the domain name service system recited in claim 8. (*Id.*) Thus, even if the combination proposed by the Office Action were made, it would not result in a domain name service system being connectable to a virtual private network, as recited in dependent claim 8 and its dependent claim 9. (*Id.*) Accordingly, the rejections of claims 8 and 9 should be withdrawn.

G. Dependent Claims 16, 17, 27, 33, 40, 41, 51, and 57 Are Patentable over the Cited References

Dependent claims 16, 17, 27, 33, 40, 41, 51, and 57 recite the following:

> the domain name service system *is configured to support establishing a secure communication link* between the first location and the second location (claim 16, emphasis added);
>
> the domain name service system . . . comprises *an indication that the domain name service system supports establishing a secure communication link* (claim 17, emphasis added);
>
> the domain name service system *is configured to enable establishment of a secure communication link* between a first location and a second location transparently to a user at the first location (claim 27, emphasis added);

> the domain name service system *is configured to enable establishment of a secure communication link* between a first location and a second location (claim 33, emphasis added);
>
> the instructions [executable in a domain name service system] comprise code for . . . *establishing a secure communication link* between the first location and the second location (claim 40, emphasis added);
>
> the instructions [executable in a domain name service system] comprise code for *indicating that the domain name service system supports the establishment of a secure communication link* (claim 41, emphasis added);
>
> the domain name service system *is configured to enable establishment of a secure communication link* between a first location and a second location transparently to a user at the first location (claim 51, emphasis added); and
>
> the domain name service system *is configured to enable establishment of a secure communication link* between a first location and a second location (claim 57, emphasis added).

The Office Action rejects claims 16, 17, 27, 33, 40, 41, 51, and 57 on several grounds. Dependent claims 16, 17, 27, 33, 40, 41, 51, and 57 each depend from one of independent claims 1 and 36, and are therefore also allowable at least by virtue of their dependence from these allowable claims. Thus, the rejections of claims 16, 17, 27, 33, 40, 41, 51, and 57 should be withdrawn for the reasons discussed above with regard to the independent claims. In addition, the rejections should be withdrawn and the claims should be confirmed for at least the reasons discussed below.

1. Rejections Based on *Solana* (Grounds 1 and 5)

The Office Action rejects dependent claims 16, 17, 27, 33, 40, 41, 51, and 57 as anticipated by *Solana* (Ground 1), and as being obvious over *Solana* in view of RFC 2504 (Ground 5). (OA at 5-6.) *Solana* and RFC 2504, either alone or in combination, do not disclose the additional features of claims 16, 17, 27, 33, 40, 41, 51, and 57, for the reasons discussed below. Thus, the alleged combinations of *Solana* and RFC 2504 fail to disclose or suggest the elements of these claims.

Solana does not disclose the features of these claims. As discussed above with regard to independent claims 1, 36, and 60, *Solana* does not disclose the recited domain name service system that is configured to comprise an indication that the domain name service system supports establishing a secure communication link. Because *Solana* does not describe such a recited domain name service system, it cannot disclose that the domain name service system is configured to support establishing a secure communication link, as recited in claim 16 and similarly recited in claim 40. For the same reasons, *Solana* cannot disclose that the domain name service system comprises an indication that the domain name service system supports establishing a secure communication link,

as recited in claim 17 and similarly recited in claim 41, or a domain name service system that is configured to enable establishment of a secure communication link, as recited in claims 27, 33, 51, and 57.

RFC 2504 does not remedy the above-noted deficiencies of *Solana*. As discussed above with regard to independent claims 1, 36 and 60, RFC 2504 also does not disclose the recited domain name service system. Because RFC 2504 does not describe the recited domain name service system, it cannot disclose that the domain name service system is configured to support establishing a secure communication link, as recited in claim 16 and similarly recited in claim 40. For the same reasons, it cannot disclose that the domain name service system comprises an indication that the domain name service system supports establishing a secure communication link, as recited in claim 17 and similarly recited in claim 41, or that the domain name service system is configured to enable establishment of a secure communication link, as recited in claims 27, 33, 51, and 57.

Thus, *Solana* and RFC 2504, alone or in combination, do not disclose or suggest the features of claims 16, 17, 27, 33, 40, 41, 51, and 57, and the rejections of those claims should be withdrawn.

2. Rejections Based on *Provino* (Grounds 9, 13, and 17)

The Office Action rejects dependent claims 16, 17, 27, 33, 40, 41, 51, and 57 as anticipated by *Provino* (Ground 9), and as being obvious over *Provino* in view of one or more combinations of RFC 2230 and RFC 2504 (Grounds 13 and 17). (OA at 7-8.) *Provino*, RFC 2230, and/or RFC 2504, either alone or in combination, do not disclose the additional features of claims 16, 17, 27, 33, 40, 41, 51, and 57, for the reasons discussed below. Thus, the alleged combinations of *Provino*, RFC 2230, and RFC 2504 fail to disclose or suggest the elements of these claims.

As discussed above with regard to independent claims 1, 36, and 60, *Provino* does not disclose the recited domain name service system that is configured to comprise an indication that the domain name service system supports establishing a secure communication link. Because *Provino* does not describe such a domain name service system, it cannot disclose that the domain name service system is configured to support establishing a secure communication link, as recited in claim 16 and similarly recited in claim 40. For the same reasons, it cannot disclose that the domain name service system comprises an indication that the domain name service system supports establishing a secure communication link, as recited in claim 17 and similarly recited in claim 41, or that the domain name service system is configured to enable establishment of a secure communication link, as recited in claims 27, 33, 51, and 57.

RFC 2230 and RFC 2504 do not remedy the above-noted deficiencies of *Provino*. As discussed above with regard to independent claims 1, 36 and 60, RFC 2230 and RFC 2504 also do

not disclose the recited domain name service system. Because RFC 2230 and RFC 2504 do not describe the recited domain name service system, they cannot disclose that the domain name service system is configured to support establishing a secure communication link, as recited in claim 16 and similarly recited in claim 40. For the same reasons, they cannot disclose that the domain name service system comprises an indication that the domain name service system supports establishing a secure communication link, as recited in claim 17 and similarly recited in claim 41, or that the domain name service system is configured to enable establishment of a secure communication link, as recited in claims 27, 33, 51, and 57.

Thus, *Provino*, RFC 2230, and RFC 2504, alone or in combination, do not disclose or suggest the features of claims 16, 17, 27, 33, 40, 41, 51, and 57, and the rejections of those claims should be withdrawn.

3. Rejections Based on *Beser* (Ground 21)

The Office Action rejects dependent claims 16, 17, 27, 33, 40, 41, 51, and 57 as being anticipated by *Beser* (Ground 21). (OA at 9.) *Beser* does not disclose the additional features of claims 16, 17, 27, 33, 40, 41, 51, and 57, for the reasons discussed below. Thus, *Beser* does not disclose the elements of these claims.

As discussed above with regard to independent claims 1, 36, and 60, *Beser* does not disclose the recited domain name service system that is configured to comprise an indication that the domain name service system supports establishing a secure communication link. Because *Beser* does not describe such a domain name service system, it cannot disclose that the domain name service system is configured to support establishing a secure communication link, as recited in claim 16 and similarly recited in claim 40. For the same reasons, it cannot disclose that the domain name service system comprises an indication that the domain name service system supports establishing a secure communication link, as recited in claim 17 and similarly recited in claim 41, or that the domain name service system is configured to enable establishment of a secure communication link, as recited in claims 27, 33, 51, and 57.

Thus, *Beser* does not disclose the features of claims 16, 17, 27, 33, 40, 41, 51, and 57, and the rejection of those claims should be withdrawn.

4. Rejections Based on RFC 2230 (Ground 25)

The Office Action rejects dependent claims 16, 17, 27, 33, 40, 41, 51, and 57 as being anticipated by RFC 2230 (Ground 25). (OA at 10.) RFC 2230 does not disclose the additional features of claims 16, 17, 27, 33, 40, 41, 51, and 57, for the reasons discussed below.

As discussed above with regard to independent claims 1, 36, and 60, RFC 2230 does not disclose the recited domain name service system that is configured to comprise an indication that the domain name service system supports establishing a secure communication link. Because RFC 2230 does not describe such a domain name service system, it cannot disclose that the domain name service system is configured to support establishing a secure communication link, as recited in claim 16 and similarly recited in claim 40. For the same reasons, it cannot disclose that the domain name service system comprises an indication that the domain name service system supports establishing a secure communication link, as recited in claim 17 and similarly recited in claim 41, or that the domain name service system is configured to enable establishment of a secure communication link, as recited in claims 27, 33, 51, and 57.

Thus, RFC 2230 fails to disclose or suggest the features of claims 16, 17, 27, 33, 40, 41, 51, and 57, and the rejections of those claims as anticipated by RFC 2230 should be withdrawn.

5. Rejections Based on RFC 2538 (Ground 30)

The Office Action rejects dependent claims 16, 17, 27, 33, 40, 41, 51, and 57 as being anticipated by RFC 2538 (Ground 30). (OA at 12.) RFC 2538 does not disclose the additional features of claims 16, 17, 27, 33, 40, 41, 51, and 57, for the reasons discussed below.

As discussed above with regard to independent claims 1, 36, and 60, RFC 2538 does not disclose the recited domain name service system that is configured to comprise an indication that the domain name service system supports establishing a secure communication link. Because RFC 2538 does not describe the recited domain name service system, it cannot disclose that the domain name service system is configured to support establishing a secure communication link, as recited in claim 16 and similarly recited in claim 40. For the same reasons, it cannot disclose that the domain name service system comprises an indication that the domain name service system supports establishing a secure communication link, as recited in claim 17 and similarly recited in claim 41, or that the domain name service system is configured to enable establishment of a secure communication link, as recited in claims 27, 33, 51, and 57.

Thus, RFC 2538 does not disclose the features of claims 16, 17, 27, 33, 40, 41, 51, and 57, and the rejection of those claims should be withdrawn.

H. Dependent Claims 18 and 42 Are Patentable over the Cited References

Dependent claim 18 recites "at least one of the plurality of domain names is reserved for secure communication links," and dependent claim 42 recites "the instructions comprise code for reserving at least one of the plurality of domain names for secure communication links." The Office Action rejects claims 18 and 42 on several grounds. Dependent claims 18 and 42 depend from

independent claims 1 and 36, respectively, and are therefore also allowable at least by virtue of their dependence from these allowable claims. Thus, the rejections of claims 18 and 42 should be withdrawn for the reasons discussed above with regard to the independent claims. In addition, the rejections should be withdrawn and the claims should be confirmed for at least the reasons discussed below.

1. Rejections Based on *Solana* (Grounds 1 and 5)

The Office Action rejects dependent claims 18 and 42 as anticipated by *Solana* (Ground 1), and as being obvious over *Solana* in view of RFC 2504 (Ground 5). (OA at 5-6.) *Solana* and RFC 2504, either alone or in combination, do not disclose the additional features of claims 18 and 42, for the reasons discussed below. Thus, the alleged combinations of *Solana* and RFC 2504 fail to disclose or suggest the elements of these claims.

The Request and the Office Action assert that *Solana*'s "domain names employing Uniform Naming Information (UNI) of the responder" disclose that "at least one of the plurality of domain names is reserved for secure communication links," as recited in claim 18 and similarly recited in claim 42. (Req. at 50-51; *see also id.* at 64, 94, 102.) This is incorrect. *Solana* discloses that the UNI may be a common name, an e-mail address, or a network address. (*Solana* 43.) But *Solana* does not disclose that this common name, e-mail address, or network address is *reserved* for secure communication links. (Keromytis Decl. ¶ 85.) *Solana* does not disclose that the UNI can only be used for secure communication links, and merely establishing an alleged secure communication link with the responder UNI does not disclose that the responder UNI is *reserved* for secure communication links. (*Id.*) As such, *Solana* does not disclose domain names reserved for secure communication links.

RFC 2504 does not make up for the deficiencies of *Solana* because RFC 2504 also does not disclose domain names reserved for secure communication links. And the Request and the Office Action do not assert that RFC 2504 discloses this feature. Accordingly, *Solana* and RFC 2504, alone or in combination, do not disclose or suggest the features of claims 18 and 42, and the rejections of these claims should be withdrawn.

2. Rejections Based on *Beser* (Ground 21)

The Office Action rejects dependent claims 18 and 42 as being anticipated by *Beser* (Ground 21). (OA at 9.) *Beser* does not disclose the additional features of claims 18 and 42, for the reasons discussed below.

The Request and the Office Action assert that *Beser* discloses domain names reserved for secure communication links because *Beser* discloses associating a unique identifier (which may be a

domain name) in a tunneling request with the first and second network devices. (Req. at 236, 251.) But merely associating the unique identifier of terminating telephony device 26 that is included in the request with another network device does not disclose reserving that unique identifier for secure communication links. (Keromytis Decl. ¶ 86.) *Beser* discloses that the unique identifier may include a dial-up number, an e-mail address, a domain name, an employee number, a driver's license number, etc. (*Beser* 10:37-11:8.) But *Beser* does not disclose reserving any of these identifiers for secure communication links. (Keromytis Decl. ¶ 86.) The portions in *Beser* relied upon by the Request and the Office Action as allegedly disclosing this feature merely point to the negotiation process of *Beser* that the Request and the Office Action earlier asserted was the recited "indication." These portions do not disclose reserving domain names for secure communication links. (*Id.*)

Thus, *Beser* does not disclose that at least one of the plurality of domain names is reserved for secure communication links, as recited in dependent claim 18 and similarly recited in dependent claim 42. Accordingly, the rejections of these claims should be withdrawn.

3. Rejections Based on RFC 2230 (Ground 25)

The Office Action rejects dependent claims 18 and 42 as being anticipated by RFC 2230 (Ground 25). (OA at 10.) RFC 2230 does not disclose the additional features of claims 18 and 42, for the reasons discussed below.

In the rejection of claims 18 and 42, the Request and the Office Action allege RFC 2230 discloses that "at least one of the plurality of domain names is reserved for secure communication links," citing to RFC 2230's statement that "[o]nce R1 has decided that the packet from S to D should be protected, it performs a secure DNS lookup for the records associated with domain D." (Req. at 284, 296.) RFC 2230 does not support this position.

While RFC 2230 discloses that IPsec Security Associations *can* be established between domains, the reference does not disclose that any domain names are *reserved* for secure communication links. (Keromytis Decl. ¶ 88.) As highlighted by the passage cited by the Request and the Office Action, in the Subnet-to-Subnet Example, before R1 even performs a DNS lookup, "R1 [first] makes the *policy decision* to provide the IPsec service for traffic from R1 destined for R2. *Once R1 has decided* that the packet from S to D should be protected, it performs a secure DNS lookup for the records associated with domain D." (RFC 2230 at 3, emphases added; Keromytis Decl. ¶ 88.) R1 or D makes a similar policy decision in the other embodiments as well:

> R1 makes the *policy decision* that IP Security is needed for the packet travelling from S to D. Then, R1 performs the secure DNS lookup for D (RFC 2230 at 4, emphasis added); and

> D makes the *policy decision* that IP Security is needed for the packets from D to S. Then D performs the secure DNS lookup for S (*id.* at 6, emphasis added).

(Keromytis Decl. ¶ 88.) Since an external policy decision determines whether to provide security for packets sent between given domains, it is possible to establish a connection to a domain with *or* without IP Security. (*Id.*) Thus, RFC 2230 does not disclose "at least one of the plurality of domain names is *reserved* for secure communication links" (emphasis added), as recited in claims 18 and 42. In fact, RFC 2230 is silent on reserving domain names for secure communication links. (*Id.*)

Thus, RFC 2230 fails to disclose or suggest the features of claims 18 and 42, and the rejections of those claims as anticipated by RFC 2230 should be withdrawn.

4. Rejections Based on RFC 2538 (Ground 30)

The Office Action rejects dependent claims 18 and 42 as being anticipated by RFC 2538 (Ground 30). (OA at 12.) RFC 2538 does not disclose the additional features of claims 18 and 42, for the reasons discussed below.

The Request and Office Action assert RFC 2538 discloses domain names reserved for secure communication links because it discloses that "domain names are associated with certificates used for secure communication links." (Req. at 328, 340.) But merely storing a certificate under a domain name related to its subject, as disclosed in RFC 2538, does not mean that the domain name is reserved for secure communication links. (RFC 2538 at 5; Keromytis Decl. ¶ 89). In fact, nothing in RFC 2538 discloses or suggests that the domain name associated with the certificate may be used only for secure communication. (Keromytis Decl. ¶ 89.) As such, RFC 2538 does not disclose that domain names stored are reserved for secure communication links, as recited in dependent claim 18 and similarly recited in dependent claim 42. Accordingly, the rejection of these claims should be withdrawn.

I. Dependent Claims 24 and 48 Are Patentable over the Cited References

Dependent claim 24 recites "at least one of the plurality of domain names comprises an indication that the domain name service system supports establishing a secure communication link," and dependent claim 48 recites "at least one of the plurality of domain names includes an indication that the domain name service system supports the establishment of a secure communication link." The Office Action rejects claims 24 and 48 on several grounds. Dependent claims 24 and 48 depend from independent claims 1 and 36, respectively, and are therefore also allowable at least by virtue of their dependence from these allowable claims. Thus, the rejections of claims 24 and 48 should be withdrawn for the reasons discussed above with regard to the independent claims. In addition, the

rejections should be withdrawn and the claims should be confirmed for at least the reasons discussed below.

1. Rejections Based on *Solana* (Grounds 1, 2, 5, and 6)

The Office Action rejects dependent claims 24 and 48 as anticipated by *Solana* (Ground 1), and as being obvious over *Solana* in view of one or more of RFC 920 and/or RFC 2504 (Grounds 2, 5, and 6). (OA at 5-6.) *Solana*, RFC 920, and/or RFC 2504, either alone or in combination, do not disclose or suggest the additional features of claims 24 and 48, for the reasons discussed below. Thus, the alleged combinations of *Solana*, RFC 920, and/or RFC 2504 fail to disclose or suggest the elements of these claims.

The Request and the Office Action assert that because *Solana* discloses domain names that are associated with certificates needed for secure transactions, those domain names are "'secure names' associated with secure communications and thereby comprise indications that its secure DNS systems support establishing a secure communication link." (*See, e.g.*, Req. at 52-53.) This is incorrect. The mere association of a domain name with a certificate does not disclose anything about what the domain name itself comprises. (Keromytis Decl. ¶ 91.) In particular, just because a domain name is associated with a certificate does not mean that the domain name itself comprises an indication that a domain name system supports establishing a secure communication link. (*Id.*)

In fact, *Solana* does not disclose that the UNIs (the alleged domain names) include any indication of the capabilities of the DS (the alleged domain name service system), much less an indication that the DS supports establishing a secure communication link. (*Id.* ¶ 92.) For example, *Solana* discloses two examples of UNIs in Fig. 1: xyz@S and abc@D. (*Solana* 43, Fig. 1.) But *Solana* does not disclose that these UNIs, or any other UNIs, comprise an indication that the DS supports establishing a secure communication link. (Keromytis Decl. ¶ 92.)

RFC 920 and RFC 2504 do not make up for the above-noted deficiencies of *Solana*. The Request relies on RFC 920 as "including general criteria for establishing new domain names." (*See, e.g.*, Req. at 80-83.) But the "general criteria" in RFC 920 do not disclose a domain name that comprises an indication that the domain name service system supports establishing a secure communication link. (Keromytis Decl. ¶ 93.) Nor do the Request and the Office Action assert that it does. (Req. at 80, 111-12.) RFC 2504 also does not disclose, and is not relied upon as allegedly disclosing, these features of claims 24 and 48. (*See, e.g.*, *id.* at 95-96, 111-12.)

Accordingly *Solana*, RFC 920, and RFC 2504, alone or in combination, do not disclose or suggest the features of claims 24 and 48, and the rejections of these claims should be withdrawn.

2. Rejections Based on *Provino* (Grounds 9, 10, 13, 14, 17, and 18)

The Office Action rejects dependent claims 24 and 48 as anticipated by *Provino* (Ground 9), and as being obvious over *Provino* in view of one or more combinations of RFC 920, RFC 2230, and/or RFC 2504 (Grounds 10, 13, 14, 17, and 18). (OA at 7-9.) *Provino*, RFC 920, RFC 2230, and/or RFC 2504, either alone or in combination, do not disclose or suggest the additional features of claims 24 and 48, for the reasons discussed below. Thus, the alleged combinations of *Provino*, RFC 920, RFC 2230, and/or RFC 2504 fail to disclose or suggest the elements of these claims.

In the rejections of claims 24 and 48, the Request and the Office Action allege that *Provino* discloses a domain name that comprises or includes an indication that the domain name service system supports establishing a secure communication link because "Provino also discloses use of nameservers to resolve human-readable domain names to provide appropriate Internet address[es], and that domain names (e.g., domain name associated with VPN 15) are associated with secure transactions over the Internet." (*See, e.g.*, Req. at 128.) This is incorrect for at least two reasons.

First, as discussed above with respect to the independent claims, *Provino*'s alleged domain name service system (name server 17) is not configured to comprise an indication that the domain name service system supports establishing a secure communication link. (Keromytis Decl. ¶ 95.) Rather, *Provino*'s alleged domain name service system is a conventional domain name service system, recognized and distinguished by the '504 patent, that merely responds to a request for the Internet address of a device (firewall 30 or otherwise) corresponding to the human-readable name for that device. (*Id.*) Thus, *Provino*'s alleged domain name service system does not even have the capability to support establishing a secure communication link, let alone to comprise an indication that the domain name service system supports establishing a secure communication link, as recited by independent claim 1. (*Id.*) Because *Provino*'s alleged domain name service system does not even have the capability to support establishing a secure communication link, it cannot store at least one domain name that comprises or includes an indication that the alleged domain name service system supports establishing a secure communication link, as recited by dependent claims 24 and 48. (*Id.*)

In addition, the fact that *Provino*'s alleged domain name service system resolves the Internet address of the firewall 30 (with which the device 12(m) may at some point later establish a secure tunnel) when it is requested does not disclose anything about what the alleged domain name of the firewall 30 itself comprises. (*Id.* ¶ 96.) Just because an alleged domain name (human-readable address) is associated with a firewall does not mean that the alleged domain name itself includes or comprises an indication that a domain name system supports establishing a secure communication link, as recited in claims 24 and 48. (*Id.*) *Provino* does not provide any specifics about the content

of the alleged domain names stored in *Provino*'s name server 17, and certainly does not disclose that they can comprise or include an indication of the capabilities of the alleged domain name service system, much less an indication that it supports establishing a secure communication link, as recited by claims 24 and 48. (*Id.*) Indeed, as discussed, *Provino* does not even disclose that the alleged domain name service system is capable of supporting establishing a secure communication to begin with. (*Id.*)

RFC 920, RFC 2230, and RFC 2504 do not make up for the above-noted deficiencies of *Provino*. Although the Request alleges that RFC 920 "includ[es] general criteria for establishing new domain names" (Req. at 152), the "general criteria" in RFC 920 do not disclose a domain name that comprises an indication that the domain name service system supports establishing a secure communication link. Nor do the Request and the Office Action assert that it does. RFC 2230 and RFC 2504 also do not disclose, and are not relied upon as allegedly disclosing, these features of claims 24 and 48.

Accordingly *Provino*, RFC 920, RFC 2230, and RFC 2504, alone or in combination, do not disclose or suggest the features of claims 24 and 48, and the rejections of these claims should be withdrawn.

3. Rejections Based on *Beser* (Grounds 21 and 22)

The Office Action rejects dependent claims 24 and 48 as being anticipated by *Beser* (Ground 21), and as being obvious over *Beser* in view of RFC 920 (Ground 22). (OA at 9-10.) *Beser* and/or RFC 920 do not disclose or suggest the additional features of claims 24 and 48, for the reasons discussed below, and thus do not disclose or suggest the elements of these claims.

The Request and the Office Action assert that *Beser* discloses a domain name that comprises an indication that the domain name service system supports establishing a secure communication link because the domain names in *Beser* "are 'secure names' associated with secure communications." (Req. at 238-39.) This is incorrect. Merely using a domain name in secure communications, as asserted by the Request and the Office Action, does not disclose anything about what the domain name itself comprises. (Keromytis Decl. ¶ 98.) In particular, just because a domain name is "associated with secure communications" does not mean that the domain name comprises an indication that a domain name system supports establishing a secure communication link. (*Id.*) In fact, *Beser* does not disclose that the alleged domain names (i.e., unique identifiers) include any indication of the capabilities of the alleged domain name service system (i.e., trusted-third-party network device 30), let alone an indication that the alleged domain name service system supports

establishing a secure communication link. (*Id.*) Thus, *Beser* does not disclose the features of claims 24 and 48.

RFC 920 does not make up for the above-noted deficiencies of *Beser*. The Request relies on RFC 920 as "including general criteria for establishing new domain names." (Req. at 265-66.) But, as discussed, the "general criteria" in RFC 920 do not disclose a domain name that comprises an indication that the domain name service system supports establishing a secure communication link. (Keromytis Decl. ¶ 99.) Nor do the Request and the Office Action assert that it does. (Req. at 265-66.)

Thus, *Beser* and RFC 920, alone or in combination, do not disclose or render obvious the subject matter of claims 24 and 48, and the rejections should be withdrawn.

4. Rejections Based on RFC 2230 (Grounds 25 and 26)

The Office Action rejects dependent claims 24 and 48 as being anticipated by RFC 2230 (Ground 25), and as being obvious over RFC 2230 in view of RFC 920 (Ground 26). (OA at 10-11.) The alleged combination of RFC 2230 and RFC 920 does not disclose or suggest the additional features of claims 24 and 48, for the reasons discussed below. Thus, the alleged combination of RFC 2230 and RFC 920 does not disclose or suggest the elements of these claims.

In the rejections of claims 24 and 48, the Request and the Office Action allege that RFC 2230 discloses a domain name that comprises or includes an indication that the domain name service system supports establishing a secure communication link because "RFC 2230 discloses secure DNS systems providing for secure communication links between multiple domains ('S' and 'D') that are established via use of systems that incorporate and use the KX resource record." (Req. at 286.) This is incorrect for at least two reasons.

First, as discussed above with respect to the independent claims, RFC 2230's alleged domain name service system is not configured to comprise an indication that the domain name service system supports establishing a secure communication link. (Keromytis Decl. ¶ 101.) Rather, as discussed above, RFC 2230 discloses a conventional domain name service system that is recognized and distinguished by the '504 patent. (*Id.*) Thus, RFC 2230's alleged domain name service system does not have the capability to support establishing a secure communication link, let alone to comprise an indication that the domain name service system supports establishing a secure communication link, as recited by independent claim 1. (*Id.*) Because the alleged domain name service system does not even have the capability to support establishing a secure communication link, RFC 2230 cannot disclose or suggest that the alleged domain name service system stores at least one domain name that

comprises or includes an indication that the alleged domain name service system supports establishing a secure communication link, as recited by dependent claims 24 and 48. (*Id.*)

In addition, the mere fact that RFC 2230 discloses that IPsec Security Associations can be created between an originating device S and a destination device D does not disclose anything about what the domain names associated with these devices themselves include. (*Id.* ¶ 102.) Specifically, just because a Security Association is created between two devices does not mean that their domain names include or comprise an indication that the alleged domain name system supports establishing a secure communication link, as recited in claims 24 and 48. (*Id.*) RFC 2230 does not describe any specifics about the content of the domain names, and certainly does not disclose that they can comprise or include an indication of the capabilities of the alleged domain name service system. (*Id.*) Thus, RFC 2230 does not disclose that at least one of the plurality of domain names comprises or includes an indication that the domain name service system supports establishing a secure communication link, as recited by claims 24 and 48.

RFC 920 does not make up for the above-noted deficiencies of RFC 2230, nor do the Request and the Office Action assert that it does. (Req. at 310-11.) Accordingly, RFC 2230 and RFC 920, alone or in combination, do not disclose or suggest the features of claims 24 and 48, and the rejections of these claims should be withdrawn.

5. Rejections Based on RFC 2538 (Grounds 30 and 31)

The Office Action rejects dependent claims 24 and 48 as being anticipated by RFC 2538 (Ground 30), and as being obvious over RFC 2538 in view of RFC 920 (Ground 31). (OA at 12.) The alleged combination of RFC 2538 and RFC 920 does not disclose or suggest the additional features of claims 24 and 48, for the reasons discussed below. Thus, the alleged combination of RFC 2538 and RFC 920 does not disclose or suggest the elements of these claims.

The Request and the Office Action assert that RFC 2538 discloses a domain name that comprises an indication that the domain name service system supports establishing a secure communication link because the domain names in RFC 2538 "are 'secure names' associated with secure communications." (Req. at 330.) This is incorrect. Merely associating a domain name with secure communications, as asserted by the Request and the Office Action, does not disclose anything about what the domain name itself comprises. (Keromytis Decl. ¶ 104.) In particular, just because a domain name is "associated with secure communications" does not mean that the domain name includes an indication that a domain name system supports establishing a secure communication link. (*Id.*) In fact, RFC 2538 does not disclose domain names that include any indication of the capabilities of the alleged domain name service system in RFC 2538, much less an indication that the

alleged domain name service system supports establishing a secure communication link. (*Id.*) Thus, RFC 2538 does not disclose the features of claims 24 and 48.

RFC 920 does not make up for the above-noted deficiencies of RFC 2538. The Request relies on RFC 920 as "including general criteria for establishing new domain names." (Req. at 351-52.) But, as discussed, the "general criteria" in RFC 920 do not disclose a domain name that comprises an indication that the domain name service system supports establishing a secure communication link. (Keromytis Decl. ¶ 105.) Nor do the Request and the Office Action assert that it does. (Req. at 351-52.)

Thus, RFC 2538 and RFC 920, alone or in combination, do not disclose or render obvious the subject matter of claims 24 and 48, and the rejections should be withdrawn.

J. Dependent Claims 26 and 50 Are Patentable over the Cited References

Dependent claim 26 recites "at least one of the plurality of domain names enables establishment of a secure communication link," and dependent claim 50 recites "at least one of the plurality of domain names is configured so as to enable establishment of a secure communication link." The Office Action rejects claims 26 and 50 on several grounds. Dependent claims 18 and 42 depend from independent claims 1 and 36, respectively, and are therefore also allowable at least by virtue of their dependence from these allowable claims. Thus, the rejections of claims 18 and 42 should be withdrawn for the reasons discussed above with regard to the independent claims. In addition, the rejections should be withdrawn and the claims should be confirmed for at least the reasons discussed below.

1. Rejections Based on *Solana* (Grounds 1 and 5)

The Office Action rejects dependent claims 26 and 50 as anticipated by *Solana* (Ground 1), and as being obvious over *Solana* in view of RFC 2504 (Ground 5). (OA at 5-6.) *Solana* and RFC 2504, either alone or in combination, do not disclose or suggest the additional features of claims 26 and 50, for the reasons discussed below. Thus, the alleged combinations of *Solana* and RFC 2504 do not disclose or suggest the elements of these claims.

The Request and the Office Action generally assert that *Solana* discloses UNIs to designate principals and domains, and that the UNI is used when establishing the alleged secure communication link. (*See, e.g.*, Req. at 53, citing *Solana* 43-46, Figs. 2a-b, 3a-b.) But merely using a UNI when establishing an alleged secure communication link does not mean that the UNI, itself, enables (or is configured so as to enable) establishment of the secure communication link. (Keromytis Decl. ¶ 106.) As discussed, *Solana* discloses two exemplary UNIs in connection with

Fig. 1: xyz@S and abc@D. (*Solana* 43, Fig. 1.) But *Solana* does not disclose that these exemplary UNIs enable establishment of a secure communication link. (Keromytis Decl. ¶ 106.)

RFC 2504 does not make up for the above-noted deficiencies of *Solana*. In particular, RFC 2504 also does not disclose, and is not relied upon as allegedly disclosing, these features of claims 26 and 50. (Req. at 96, 104.) Accordingly *Solana* and RFC 2504, alone or in combination, do not disclose or suggest the features of claims 26 and 50, and the rejections of these claims should be withdrawn.

2. Rejections Based on *Provino* (Grounds 9, 13, and 17)

The Office Action rejects dependent claims 26 and 50 as anticipated by *Provino* (Ground 9), and as being obvious over *Provino* in view of one or more combinations of RFC 2230 and RFC 2504 (Grounds 13 and 17). (OA at 7-8.) *Provino*, RFC 2230, and/or RFC 2504, either alone or in combination, do not disclose the additional features of claims 26 and 50, for the reasons discussed below. Thus, the alleged combinations of *Provino*, RFC 2230, and/or RFC 2504 do not disclose or suggest the features of these claims.

In the rejections of claims 26 and 50, the Request and the Office Action allege that *Provino* discloses that "at least one of the plurality of domain names enables [or is configured so as to enable] establishment of a secure communication link," as recited in the claims, because "[t]he domain names and Internet addresses maintained in name server 32 are used to establish virtual private networks, which are secure communication links." (*See, e.g.*, Req. at 129.) This is incorrect.

But merely *using* a domain name when establishing an alleged secure communication link does not mean that the domain name, itself, *enables* establishment of the secure communication link. (Keromytis Decl. ¶ 108.) *Provino* is silent regarding the content of the alleged domain names (human-readable addresses), and certainly does not disclose that they include anything special that "enables [or is configured so as to enable] establishment of a secure communication link," as recited in claims 26 and 50. (*Id.*) Accordingly, *Provino* fails to disclose or suggest that "at least one of the plurality of domain names enables establishment of a secure communication link," as recited in claim 26, or that "at least one of the plurality of domain names is configured so as to enable establishment of a secure communication link," as recited in claim 50.

RFC 2230 and RFC 2504 do not make up for the above-noted deficiencies of *Provino*. Nor do the Request and the Office Action assert that they do. (*See, e.g.*, Req. at 171, 203.) Accordingly, *Provino*, RFC 2230, and RFC 2504, alone or in combination, do not disclose or suggest the features of claims 26 and 50, and the rejections of these claims should be withdrawn.

3. Rejections Based on *Beser* (Ground 21)

The Office Action rejects dependent claims 26 and 50 as being anticipated by *Beser* (Ground 21). (OA at 9.) *Beser* does not disclose the additional features of claims 26 and 50, for the reasons discussed below.

The Request and the Office Action assert that *Beser* discloses that at least one of the plurality of domain names enables (or is configured so as to enable) establishment of a secure communication link because *Beser* "discloses systems in which a unique identifier, which may be a domain name, *is used to* establish a secure communication link." (*See, e.g.*, Req. at 239, emphasis added.) But merely *using* a domain name when establishing an alleged secure communication link does not mean that the domain name, itself, *enables* establishment of the secure communication link. (Keromytis Decl. ¶ 109.) In fact, *Beser* does not disclose that the unique identifiers *enable* (or are configured so as to enable) establishment of a secure communication link, and thus does not anticipate claims 26 and 50. (*Id.*) Accordingly, the rejection of these claims should be withdrawn.

4. Rejections Based on RFC 2230 (Ground 25)

The Office Action rejects dependent claims 26 and 50 as being anticipated by RFC 2230 (Ground 25). (OA at 10.) RFC 2230 does not disclose the additional features of claims 26 and 50, for the reasons discussed below.

In the rejection of claims 26 and 50, the Request and the Office Action allege that RFC 2230 discloses that "at least one of the plurality of domain names enables [or is configured so as to enable] establishment of a secure communication link," as recited in the claims, because RFC 2230 discloses secure communication links between R1 and R2 and between R1 and D. (*See, e.g.*, Req. at 287.) This is incorrect.

But merely *using* a domain name when establishing an alleged secure communication link does not mean that the domain name, itself, *enables* establishment of the secure communication link. (Keromytis Decl. ¶ 111.) In fact, RFC 2230 does not disclose that the unique identifiers *enable* establishment of a secure communication link, and thus does not anticipate claims 26 and 50. (*Id.*) Accordingly, the rejection of these claims should be withdrawn. As with other references discussed above, RFC 2230 is silent regarding the content of the alleged domain names, and certainly does not disclose that they include anything special that "enables [or is configured so as to enable] establishment of a secure communication link," as recited in claims 26 and 50. (*Id.*)

In addition, as discussed above, before an IPsec node in RFC 2230 even seeks the DNS records of its target domain, it first makes a *policy decision* of whether to provide IPsec services for traffic between given domains. (*See, e.g.*, RFC 2230 at 3, 4, 6; Keromytis Decl. ¶ 112.) Because an

external policy decision determines whether to provide security for packets sent between given domains, it is possible to establish a connection to a domain with *or* without IP Security. (Keromytis Decl. ¶ 112.) Thus, RFC 2230 does not disclose that "at least one of the plurality of *domain names enables* establishment of a secure communication link" (emphasis added), as recited in claim 26, or that "at least one of the plurality of *domain names is configured so as to enable* establishment of a secure communication link" (emphasis added), as recited in claim 50.

For the reasons discussed above, RFC 2230 fails to disclose or suggest the features of claims 26 and 50, and the rejection of these claims based on RFC 2230 should be withdrawn.

5. Rejections Based on RFC 2538 (Ground 30)

The Office Action rejects dependent claims 26 and 50 as being anticipated by RFC 2538 (Ground 30). RFC 2538 does not disclose the additional features of claims 26 and 50, for the reasons discussed below. Thus, RFC 2538 does not disclose the elements of these claims.

The Request and the Office Action assert that RFC 2538 discloses domain names that enable (or is configured so as to enable) establishment of a secure communication link because the domain names in RFC 2538 are associated with a CERT RR. (*See, e.g.*, Req. at 330-31.) But merely associating a domain name with a public key contained in a certificate (the CERT RR) does not mean that the domain name, itself, enables establishment of a secure communication link. (Keromytis Decl. ¶ 113.) That is, merely associating a domain name with a public key has nothing to do with the capabilities of the actual domain name, such as whether the domain name enables establishment of a secure communication link. (*Id.*) Thus, RFC 2538 merely discloses domain names associated with public keys and does not disclose that the domain names enable (or are configured so as to enable) establishment of a secure communication link. (*Id.*) As such, RFC 2538 does not anticipate claims 26 and 50, and the rejection of those claims should be withdrawn.

K. A *Prima Facie* Case of Obviousness Has Not Been Established

In addition to the reasons set forth above, Patent Owner submits that the obviousness rejections should be withdrawn because the Request and the Office Action have not provided sufficient reasons for combining the cited references. Instead of providing the necessary "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness," *KSR*, 550 U.S. at 418, the Request and the Office Action offer conclusory statements for why certain alleged combinations would have been obvious. For example, in the rejection of claim 12 based on *Solana* in view of *Reed*, the Request and the Office Action: (1) state that claim 8 (from which claim 12 depends) is anticipated by *Solana*;(2) describe the

alleged features of *Reed*; and then (3) conclude that "*Solana* in view of *Reed*, thus, would have suggested secure DNS systems used to establish VPNs in which values of data packets between first and second devices are compared to a moving window of valid values. Accordingly, claim 12 would have been obvious" based on *Solana* in view of *Reed*. (Req. at 86.) This and other rejections are insufficient as a matter of law because they are unsupported by any rational underpinning. (*See,* e.g., *id.* at 158, 192, 220, 274.) They are also based on nothing more than hindsight. In addition, for many of the rejections, the obviousness position is not even based on the correct claim language. (*See,* e.g., *id.* at 92, 198-99.) Accordingly, the rejections throughout the Office Action (which adopts the rejections set forth in the Request without offering any additional reasons why the alleged combinations would have been obvious) should be withdrawn, and the respective claims should be confirmed. At a minimum, the Office should clearly articulate the reasons for obviousness and present the Patent Owner with a fair opportunity for response.

L. Secondary Considerations Demonstrate Nonobviousness

Even if the Office had established a *prima facie* case of obviousness regarding any of claims 1-60 (which it has not), there is substantial evidence to rebut any finding of obviousness. As provided in M.P.E.P. § 2145, "[o]ffice personnel should consider all rebuttal arguments and evidence presented by applicants," including evidence relating to the secondary considerations as set forth in *Graham v. John Deere Co.*, 383 U.S. 1 (1966), which can support the nonobviousness of the claimed inventions. Those secondary considerations include commercial success, acceptance by others in the field, long-felt need, failure of others, and praise by others. M.P.E.P. § 2145. Here, evidence related to secondary considerations rebuts any finding of obviousness of the claimed inventions.

Generally, the computer and Internet-security industries have long sought ways to conveniently establish secure communication links, such as VPN communication links. Around the time of the effective filing date of the '504 patent, it was widely recognized that providing secure remote access to a LAN or WAN was extremely difficult for IT support desks. (Short Decl. ¶¶ 8, 11.) Specifically, remote access was "a nightmare for support desks. Staffers never kn[e]w what combination of CPU, modem, operating system and software configuration they [were] going to have to support," and adding the commercially available VPN software only made matters worse. (*Id.* ¶ 11.) The computer and Internet-security industries were forced to choose between ease of use and security, but they could not have both. (*Id.* ¶ 9.) The inventions claimed in the '504 patent, which provide a domain name service for establishing a secure communication link, combine both the ease

of use *and* the security aspects of secure communication links, without sacrificing one or the other. (*Id.*)

Prior to the features claimed in the '504 patent, there was a long-felt need for a system that could establish a secure communication link, such as a VPN communication link, in a simple and straightforward manner because "a solution that was difficult for an end-user to employ would likely have lead to a lack of use or incorrect use." (*Id.* ¶ 3.) As one example of the manifestation of the long-felt need, the Defense Advanced Research Projects Agency ("DARPA") funded various research programs to further the science and technology of information assurance and survivability. (*Id.* ¶¶ 4-5.) One such program, "Next Generation Internet," received approximately $130 million in funding between 1998 and 2000. (*Id.* ¶ 4.)

Recognizing this long-felt need for these inventions, both In-Q-Tel, a venture capital firm that invests in companies developing cutting-edge technology, and SAIC (the original owner of the '504 patent) also spent significant resources on their development. (*Id.* ¶¶ 6-7.) In fact, in the year the inventions claimed in the '504 patent were developed, SAIC spent approximately 85% of its entire research and development budget for that year on developing these and other similar inventions. (*Id.* ¶ 7.)

Other attempts to provide an easy-to-use solution were unsuccessful. For example, the DARPA-funded research programs discussed above fell far short of the claimed inventions of the '504 patent. (*Id.* ¶¶ 4-5, 10.) One such program, "Dynamic Coalitions," was specifically created to address the ability of the Department of Defense to quickly and easily set up secure communications over the Internet. (*Id.* ¶¶ 4-5.) More than fifteen prestigious organizations took part in the "Dynamic Coalitions" research program, but none of them came up with a solution, in the relevant time frame, that was even close to the solutions provided in the claimed inventions of the '504 patent. (*Id.*) That is, they did not develop a solution that provided a domain name service for establishing a secure communication link. (*Id.*) By providing a domain name service for establishing a secure communication link, the inventions of the '504 patent succeeded where others failed. (*Id.* ¶ 11.)

The claimed inventions have also experienced commercial success. In particular, SafeNet, a leading provider of Internet-security technology that is the de facto standard in the VPN industry, entered into a portfolio license in July 2002 with the original owner of the application from which the '504 patent issued. (*Id.* ¶ 12.) SafeNet licensed the patents because of features disclosed and claimed in the patents, including those in the '504 patent. (*Id.*) In addition, Microsoft has entered into a similar license that includes the '504 patent. (*Id.*) Indeed, as noted, Microsoft was found to

willfully infringe two of the patents in the Munger patent family, leading to a damages award of over one hundred million dollars. (*Id.*)

The claimed inventions of the '504 patent were also contrary to the accepted wisdom at the time of the inventions. (*Id.* ¶ 13.) For example, there was a general understanding that reliable security could only be achieved through difficult-to-provision VPNs and that easy-to-set-up connections could not be secure. (*Id.*)

The technology of the '504 patent was also met with skepticism by those skilled in the art who learned of the patented inventions. (*Id.* ¶ 15.) For example, a DARPA program manager informed one of the coinventors of the '504 patent that the technology disclosed in the '504 patent would never be adopted. (*Id.*) Moreover, the IT offices of many large companies and institutions expressed skepticism that secure connections could ever be enabled easily by regular computer users. (*Id.*)

Several events also demonstrate praise for the inventions in the '504 patent by those in the field. As discussed above, SAIC invested a disproportionately large percentage of its internal resources in the technology. (*Id.* ¶ 17.) SafeNet and Microsoft have both licensed the technology. (*Id.*) A study done by CSMG praised the inventions. (*Id.*) Jim Rutt at Network Solutions, which was eventually acquired by Verisign, praised and expressed significant interest in the technology and would have invested but for a change in circumstances at his company. (*Id.*) This evidence showing that the claimed inventions met a long-felt need, succeeded where others have failed, have been commercially successful, were contrary to the accepted wisdom at the time of the invention, were met by skepticism by those skilled in the art, and were praised by others in the field, rebuts any finding that the claimed inventions would have been obvious.

III. CONCLUSION

For at least the reasons set forth above, the rejections of claims 1-60 should be withdrawn. Reconsideration and prompt confirmation of the patentability of claims 1-60 are respectfully requested.

Patent Owner notes that the Request, Order, and Office Action contain a number of assertions and allegations concerning the disclosure, claims, and cited references. Patent Owner does not subscribe to any assertion or allegation in the Request, Order, and Office Action regardless of whether it is addressed specifically herein.

Please charge our Deposit Account No. 501133 for any fees or to 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
McDermott Will & Emery LLP
Attorney 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

Date: March 29, 2012