Trials@uspto.gov
Tel: 571-272-7822

Paper 41
Entered: November 5, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

COMPASS BANK, COMMERCE BANCSHARES, INC., and
FIRST NATIONAL BANK OF OMAHA,
Petitioner,

v.

INTELLECTUAL VENTURES II LLC,
Patent Owner.

Case IPR2014-00724
Patent 5,745,574

Before KRISTEN L. DROESCH, JENNIFER S. BISK, and
JUSTIN BUSCH, *Administrative Patent Judges.*

BUSCH, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

A. Background

Compass Bank, Commerce Bancshares, Inc., and First National Bank of Omaha (collectively, "Petitioner") filed a petition requesting an *inter partes* review of claims 18–31 (the "challenged claims") of U.S. Patent No. 5,745,574 (Ex. 1002, "the '574 patent") under 35 U.S.C. §§ 311–319. Paper 1 ("Petition" or "Pet."). On November 6, 2014, we instituted an *inter partes* review of the challenged claims. Paper 12 ("Decision" or "Dec. on Inst."). Intellectual Ventures II LLC ("Patent Owner") filed a Patent Owner Response. Paper 19 ("PO Resp."). Petitioner filed a Reply. Paper 29 ("Reply"). An oral hearing was held on June 11, 2015.[1]

We have jurisdiction under 35 U.S.C. § 6(c), and this Final Written Decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons that follow, we determine Petitioner has shown by a preponderance of the evidence that claims 18–31 are unpatentable.

B. Related Proceedings

Petitioner indicates the '574 patent is at issue in several district court proceedings involving numerous parties. Pet. 1–2; Paper 11, 2–4. The '574 patent also was the subject of *inter partes* review Case IPR2014-00660. Pet. 2; Paper 11, 4.

C. The '574 Patent

The '574 patent relates to public key encryption (PKE), which is used for securing and authenticating transmissions over unsecure networks. Ex. 1002, 1:6–8, 1:10–2:9. To use PKE for authenticating transmissions, a transmitted message is encrypted with a sender's private encryption key (a

[1] The record includes a transcript of the oral hearing. Paper 40 ("Tr.").

key known only to the sender, sometimes referred to as a "secret key") that can only be decrypted by the sender's public encryption key (freely available), ensuring that the message was sent by the sender. *Id.* at 1:57–65. A public key infrastructure (PKI), with a hierarchical system of encrypting lower nodes' public keys, allows for a common point of trust between two parties who wish to communicate with each other. *Id.* at 3:16–39. The '574 patent explains that some of the problems with conventional PKE systems include that such systems do not have a "consistent public key infrastructure which can actually and automatically provide the certifications required for a public key system[, a] hierarchical arrangement of certifying authorities which can cross policy certifying authority boundaries[, or a convenient and transparent] way for permitting secure transactions to cross organizational boundaries." *Id.* at 4:41–51. The '574 patent purports to "provid[e] a full, correct, consistent and very general security infrastructure which will support global secure electronic transactions across organizational, political and policy certifying authority boundaries." *Id.* at 4:55–59. The challenged claims recite various processes used within a PKI system to request, issue, and update public key certificates, add nodes or entities to the hierarchy, and verify and validate certificates received.

Figure 4 of the ’574 patent is reproduced below:

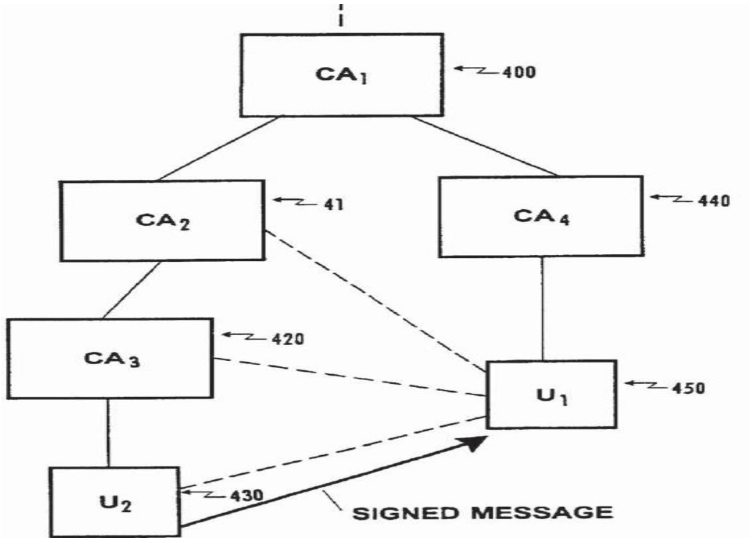

Figure 4 depicts a logical representation of a portion of a hierarchical PKI and one way in which that infrastructure may be used to verify transactions. Ex. 1002, 8:17–29. As can be seen in Figure 4, a hierarchy includes certification authorities (CAs) CA_1–CA_4 and users U_1 and U_2. *Id.* at Fig. 4. Not depicted in Figure 4, at a level above CA_1, is a policy certifying authority (PCA), “which defines a particular set of certification policies [and] set[s] the standards for their particular certification sub-hierarchies.” *Id.* at 9:26–30. Each of the CAs follows the policies set by the PCA they fall under and can then certify subordinate CAs “in a hierarchical fashion until ultimately the end users are certified at the bottom of the hierarchy.” *Id.* at 9:37–42.

In order for U_2 to be added to the hierarchy and obtain a public key certificate, which will allow U_2 to send communications that can be verified and validated by a recipient, U_2 would send an application for registration to the PCA. Ex. 1002, 13:65–67. Any other node would follow the same procedure in order to participate in the PKI and obtain certificates, so that CAs may certify other nodes, and users may send communications that can be verified and validated by a recipient. The PCA may accept or reject the application for registration. *Id.* at 14:1–7. If the PCA accepts the application, the new node is added to a network map certification infrastructure database, and the node performs steps to obtain a certificate. *Id.* at 15:59–67.

A CA or user obtains a certificate by generating new public and private keys, generating a certificate including the newly generated public key and any other information required by the policies established by the PCA, self-signing the certificate, and sending the certificate in a message to the issuing CA (the CA above it in the hierarchy) to request a signature from that CA. Ex. 1002, 14:24–34, 15:4–9. The CA uses policies established by the PCA to authenticate the request. *Id.* at 14:35–41. If authenticated, the CA signs the certificate, stores a copy and/or sends a copy to a certificate repository, and issues the certificate by sending the signed certificate back to the CA or user in a reply message. *Id.* at 14:47–52.

When a node's certificate expires, the node follows a similar process of generating new keys and requesting issuance of a new certificate from its issuing CA. If the issuing CA determines that the requesting node is an already-existing node, the issuing CA also marks the node's old certificate as revoked and adds it to a certificate revocation list (CRL). Ex. 1002, 14:43–47.

The requesting node authenticates the reply message received from the issuing CA by comparing the public key in the signed certificate with the public key that corresponds to the private key used for signing the message sent from the node to the issuing CA. Ex. 1002, 14:54–60, 15:10–22. If the keys match, the node stores the signed certificate. *Id.* at 14:54–63. If the

Explore Litigation Insights

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

Real-Time Litigation Alerts

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

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

Advanced Docket Research

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

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

Analytics At Your Fingertips

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

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

API

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

LAW FIRMS

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

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

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE