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:

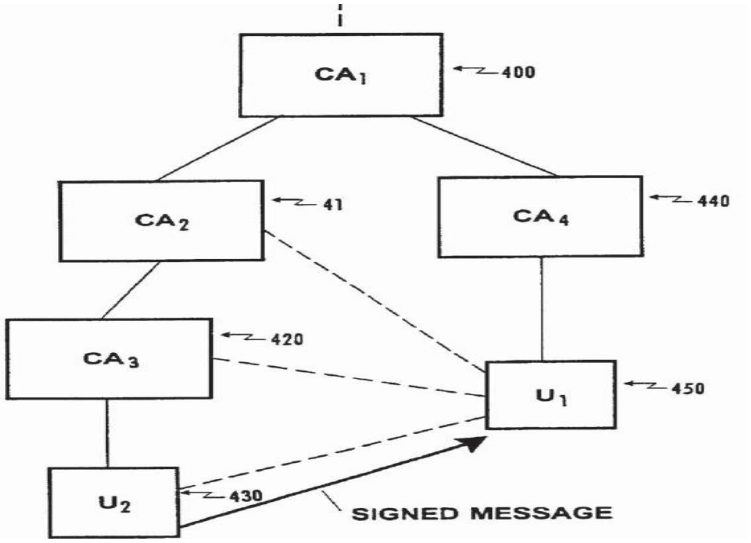

Figure 4 depicts a logical representation of a portion of a hierarchical PKI and one way in which that infrastructure may be used to verify transactions. Ex. 1002, 8:17–29. As can be seen in Figure 4, a hierarchy includes certification authorities (CAs) CA_1–CA_4 and users U_1 and U_2. *Id.* at Fig. 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

node is a CA with subordinate nodes to which it issued signed certificates, the CA must update those certificates. *Id.* at 15:22–25. The CA sends re-signed certificates to each of its subordinate nodes (if any), which results in each subordinate node iteratively receiving a new signed certificate and determining whether that node has subordinate nodes for which it needs to reissue certificates. *Id.* at 15:44–58.

Once a node receives a signed certificate from its issuing CA, other nodes in the PKI may verify and validate the certificate. Ex. 1002, 1:57–65, 3:22–39, 6:65–7:20, 11:66–12:43. Referring back to Figure 4, U_1 may receive a signed message from user U_2. *Id.* at 12:1–2, Fig. 4. U_2 may send a certificate with the signed message or, in cases where U_2 does not send a certificate, U_1 may request the certificate from U_2. *Id.* at 12:7–13. U_1 also may request a certificate from CA_2 and CA_3. *Id.* at 12:12–13. Certificates may be obtained from the owner of the certificate, the CA that issued the certificate, or from a common repository. *Id.* at 13:32–35. Each node may store a certificate for itself and every CA above that node to the highest level node (e.g., a PCA or a Policy Registration Authority (PRA), which is above a PCA in the PKI hierarchy), such that in the example depicted in Figure 4, U_2 may store a certificate for itself and a certificate for each of CA_1, CA_2, and CA_3. *Id.* at 12:2–6. As seen in Figure 4, node CA_1 is the lowest point in the hierarchy in common between U_1 and U_2 and is known as the common point of trust between U_1 and U_2. *Id.* at 12:41–43, Fig. 4.

Upon receiving a response to a request for a certificate from a node (e.g., U_2, CA_2, and CA_3), U_1 extracts, verifies, and stores the certificate. Ex. 1002, 12:17–20. U_1 may then authenticate the received certificates starting at the top of the hierarchy. *Id.* at 12:22–42. U_1 already has a known valid

certificate for CA_1 and uses CA_1's public key to authenticate CA_2's certificate that was issued by CA_1. *Id.* at 12:22–27. The process is iterated using CA_2's public key to authenticate CA_3's certificate, then using CA_3's public key to authenticate U_2's certificate. *Id.* at 12:27–39.

For reliable certification, U_1 should also obtain a CRL to ensure that each certificate has not been revoked. Ex. 1002, 12:65–67. U_1 can send a request to CA_1, CA_2, and CA_3 (or, alternatively, to a common repository) for the CRL maintained by each CA. *Id.* at 12:67–13:3, 13:14–24.

D. Illustrative Claims

Of the challenged claims in the '574 patent, claims 18, 23, 28, 30, and 31 are independent. Claims 18, 23, 28, 30, and 31 each are directed to methods for implementing various portions of the process of using PKE to certify secure communications. Therefore, claims 18, 23, 28, 30, and 31 are illustrative, and recite:

> 18. In a certification system for secure communications containing computer processes arranged in a certification infrastructure, a method of requesting and issuing a public key certificate, comprising:
>
> a. at a requesting computer process, generating a data structure containing the data items required for a public key certificate, including a public key, self-signing the data structure and sending the signed data structure as a certificate signature request to a computer process authorized as an issuing certification authority, and
>
> b. at said computer process authorized as an issuing certification authority, verifying the authenticity of said request, and if authentic, certifying and returning the data structure in a certificate signature reply.

23. In a global network with secure communications containing computer processes arranged in a certification infrastructure, a method of verifying a signed data structure sent from a sender to a receiver, comprising:

a. obtaining a public key certificate for every computer process in the infrastructure between the sender and a common point of trust in the infrastructure and

b. verifying the authenticity of signatures iteratively, beginning with the common point of trust.

28. In a certification system for secure communications containing computer processes arranged in a certification infrastructure, a method of validating public key certificates, comprising:

using the certificate revocation lists of each computer process between a computer process or user whose certificate is being validated and a point of trust in common with the computer process or user which is validating the certificate to ensure the certificates being used in the validation process do not appear on any certificate revocation list.

30. In a computer system for secure communications containing computer processes arranged in a certification infrastructure, a method of updating certificates, comprising:

a. at a first computer process, which possesses a certificates to be updated, updating the current certificate by

a.1. receiving a new signed certificate from a computer process which is authorized to issue the new signed certificate,

a.2. revoking the current certificate previously used for verification of certificates of subordinate computer processes,

a.3. issuing new certificates to all subordinate computer processes for which certificates had been previously signed by the first computer process and copying to all subordinate computer processes the new certificate to be used for verification of new subordinate certificates, and

b. iteratively performing the distribution of the new certificate to all subsequent subordinate computer processes, until all

computer processes subordinate in the infrastructure to said first computer process have the new certificates.

31. In a certification system for secure communications containing computer processes arranged in a certification infrastructure, a method of adding a new computer process to the infrastructure, comprising:

a. adding a new component to a representation of a certification infrastructure at a location indicative of where the said computer process is to be added,

b. creating entries in a certificate storage database at least at both said new computer process and at the computer process authorized to certify the said new process,

c. obtaining a signed certificate for the said new computer process from said computer process authorized to certify the new process and storing it at the said new computer process.

Ex. 1002, 19:47–61, 20:8–16, 20:32–42, 20:46–67, 21:1–14.

E. The Evidence of Record

Petitioner relies upon the following references as its basis for challenging claims 18–31 of the '574 patent.[2]

Reference	**Printed Publication**	**Exhibit**
Kapidzic	Nada Kapidzic & Alan Davidson, *A Certificate Management System: Structure, Functions and Protocols*, Proc. of the Symposium on Network and Distributed System Security, IEEE Computer Society Press, 153–160 (Feb. 16–17, 1995)	1004 ("Kapidzic")
PKI Report	Shimshon Berkovits et al., *Public Key Infrastructure Study: Final Report*, MITRE Report on NIST Request for Study on Policy and Legal Issues Related to the Operation and Management of the PKI (April 1, 1994)	1005 ("PKI Report")

[2] Petitioner also proffers Dr. David Naccache's Declaration. Ex. 1001.

Reference	Printed Publication	Exhibit
RFC 1424	Burton S. Kaliski, Jr., *Request for Comments 1424: Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services*, Network Working Group of the Internet Engineering Task Force (IETF) (1993)	1006 ("RFC 1424")

F. The Asserted Grounds of Unpatentability

The Board instituted *inter partes* review on the following asserted grounds of unpatentability under 35 U.S.C. §§ 102, 103 (Dec. on Inst. 28):

Statutory Ground	Reference[s]	Challenged Claims
§ 102(a)	Kapidzic	18–31
§ 102(b)	PKI Report	23–31
§ 103	PKI Report	25, 29, and 30
§ 103	PKI Report and RFC 1424	18–22

II. ANALYSIS

A. Claim Construction

In an *inter partes* review, claim terms are given their broadest reasonable interpretation in light of the specification in which they appear and the understanding of others skilled in the relevant art. *See* 37 C.F.R. § 42.100(b); *In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1275–79 (Fed. Cir. 2015). Applying that standard, we interpret the claim terms of the '574 patent according to their ordinary and customary meaning in the context of the written description. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007) (quoting *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc)). Patent Owner submits proposed claim constructions for three terms or phrases—process, common certificate repository, and verified by a direct inquiry to the certification authority. PO Resp. 9–13.

"computer process"

Patent Owner argues that "the broadest reasonable interpretation of 'process' . . . include[s] 'computer program instructions running on a computer.'"[3] PO Resp. 9. Patent Owner alleges that its proposed construction is consistent with the specification of the '574 patent because the description of Figure 1A explains that each block in the flow chart "is implemented as a computer process running on a computer." *Id.*

Petitioner argues that, even to the extent Patent Owner's proposed construction is accepted, all of the steps recited in the challenged claims are still performed at a computer process. Reply 3–4. As one example, Petitioner points out that the verifying, certifying, and returning steps recited in claim 18 "clearly take place at a computer running computer instructions because the emails Kapidzic describes require computers running instructions." *Id.* at 4. Petitioner further asserts that the inventor of the '574 patent even "admits Kapidzic teaches claim 18's elements." *Id.* (citing Ex. 2017, 42:25–43:14, 48:20–25, 50:18–22, 51:21–53:5). Petitioner argues that Patent Owner's argument depends on whether the broadest reasonable interpretation of the claims excludes all human or manual interaction with computers or software, which Petitioner asserts is unsupported by the claims and specification of the '574 patent. *Id.* at 4.

[3] The heading for the portion of the Response directed to Patent Owner's arguments addressing the construction of process is similar to, but inconsistent with, arguments made in that section. Specifically, Patent Owner's heading is: "The proper interpretation of 'process' is 'a computer program loaded into memory and executing in a processor.'" The reasons discussed herein for declining to adopt Patent Owner's proposed construction apply equally to the construction identified in the heading.

In particular, Petitioner argues that "certification functions . . . can be invoked by commands or by messages, such as an http command, an email message or program to program communication." Reply 4 (quoting Ex. 1002, 5:65–67). Petitioner further argues the description of Figures 7 through 27 states that the commands and processes described as collectively forming the certification system, functions and infrastructure of the invention "may be invoked either directly by a user or by part of an application process running on the user's or CA's computer." *Id.* at 4–5 (quoting Ex. 1002, 13:53–61). Petitioner also points to the portion of the '574 patent that discloses "[t]he appropriate process can be invoked manually by commands as well." *Id.* at 5 (quoting Ex. 1002, 17:66–67).

Petitioner also argues that Patent Owner's "application of its 'process' argument is based on faulty assumptions by its" declarant, Dr. Frederic T. Chong. Reply 5 (citing PO Resp. 20–23). In particular, Petitioner asserts Dr. Chong's statement that "certification in Kapidzic 'normally require[s] manual intervention'" (Ex. 2012 ¶ 36) is inaccurate because Kapidzic states that verifying the identity of a requester, not the entire certification process, normally requires manual intervention. Reply 5–6 (citing Ex. 1004, 13). Petitioner further argues that Dr. Chong assumed Kapidzic processed emails manually, but that he was unaware of whether the emails could have been automatically processed in December 1995. *Id.* (citing Ex. 1010, 44:9–21, 46:24–47:3).

We find that "process," or more specifically, "computer process," as recited in each of the challenged claims, should be given its plain and ordinary meaning. To the extent that there might have been ambiguity as to the plain and ordinary meaning, the references in the '574 patent to

computer processes support the idea that a skilled artisan would have understood what was meant by the recitation of the term. In particular, the '574 patent discloses that "[e]ach user or certification authority of the infrastructure has access to a computer process which comprises appropriate certification software and storage areas for storing data structures." Ex. 1002, 5:55–57. The '574 patent explains that the invention is directed to a certification system, which:

> includes *computer processes* implementing certification servers, certification clients and certification protocols, in which one or more first computer processes are associated with at least one initial (root) registration authority, one or more second computer processes are associated with policy certification authorities, one or more third computer processes are associated with certification authorities, and one or more end-user computer processes or application computer processes are associated with respective end-users or user applications.

Id. at 6:1–13 (emphasis added); *see id.* at 1:64–66. The '574 patent further explains that the processes are arranged in a hierarchy, that each of these processes may hold certified data structures (i.e., certificates), and that "users and applications of said system are logically located at end-points of certification chains in a certification infrastructure." *Id.* at 6:14–22.

The computer processes use "a common application programming interface [API] for access to encryption and certification services," and the API "is a set of certification functions which can be invoked by commands or by messages, such as an http command, an email message or program to program communication." Ex. 1002, 5:62–67. Figures 7 through 27 of the '574 patent "describe a set of processes which collectively form the certification system, functions, and certification infrastructure of this invention." *Id.* at 13:53–55. "The commands and processes described in

FIGS 7-2[7] thus present a set of protocol and programming primitives which may be invoked either directly by a user or by part of an application process running on the user's or CA's computer." *Id.* at 13:57–61. The '574 patent further explains that a certification server process continuously monitors incoming messages and commands, which may be invoked manually, and determines which of the certification functions described in Figures 7 through 27 should be called. *Id.* at 17:55–67.

Moreover, as discussed above, the '574 patent refers to entities (including PCA, CAs, and users) as being associated with computer processes. *See, e.g.*, Ex. 1002, 1:64–66. Throughout the specification and, in particular in the description of the specific messages and "processes which collectively form the certification system" (*see id.* at 13:53–17:54), the '574 patent refers to entities as sending and receiving messages and executing processes. *See* Reply 5 (citing Ex. 1002, 11:30–65, 13:64–16:50). The '574 patent refers to these processes and entities interchangeably. Ex. 1002, 13:53–17:54.

Thus, an ordinarily skilled artisan would have understood that the recited computer processes are instances of a computer program or programs running on the various computers, each of which may be associated with different nodes or entities (e.g., policy certification authorities, certification authorities, user applications) that carry out the tasks involved in the certification system described by the '574 patent. Functions specifically recited as being performed at or by a computer process obviously exclude performance of that function that does not involve a computer process. Beyond steps explicitly recited as performed at or by a computer process,

however, we find nothing in the recitations of a computer process that would exclude manual invocation or other manual intervention.

"common certificate repository"

Patent Owner argues that the broadest reasonable interpretation of "common certificate repository" is "a repository that stores public key certificates for **all** certification authorities [in the certification infrastructure]." PO Resp. 10 (citing Ex. 2012 ¶¶ 17–19). Patent Owner asserts that the '574 patent, which states that a "common certificate repository may contain public key certificates **for all** certification authorities in the hierarchy," requires a construction that a common certificate repository keeps a certificate for each and every certification authority in the infrastructure. *Id.*

Petitioner argues that the '574 patent discloses that the common certificate repository *may* include public key certificates for all CAs in the hierarchy, and that, because "may" is permissive, the proper construction is not limited as proposed by Patent Owner. Reply 7. Petitioner also asserts that the inventor of the '574 patent admitted that the X.500 directory, disclosed in Kapidzic and relied upon in Petitioner's challenges, is one example of a common certificate repository. *Id.* (citing Ex. 2017, 54:20–55:13).

Because we use the broadest reasonable interpretation for construing claims, we decline to limit the construction of common certificate repository to require storage of public key certificates for *all* CAs, or even all CAs within a hierarchy or infrastructure. Other than declining to adopt Patent Owner's proposed narrowing of the plain and ordinary meaning of a

common certificate repository, we do not find it necessary to provide an explicit construction of the term.

Whether recitation of a method step introduced by "may" further limits a claim

Before we address the parties' arguments regarding the construction of "verified by a direct inquiry to the certification authority," recited in claim 25, we must first address the use of "may" to introduce limitations in claims 25–27. "[O]ptional elements do not narrow the claim because they can always be omitted." *In re Johnston*, 435 F.3d 1381, 1384 (Fed. Cir. 2006). Claims that use the term "may" to introduce a limitation are permissive and, thus, do not narrow the scope of the claim. *Id.* Thus, the use of the term "may" or "may also" in claims 25–27 is not limiting. Specifically, claims 25–27, which recite "[t]he method of verifying of claim 23 in which a public key certificate . . . may" be obtained or verified by various steps, do not further limit claim 23, from which they depend.

We are not persuaded by Patent Owner's argument that claim 25, which recites that the method of claim 23 "may also be verified by a direct inquiry," "provides an alternative" approach to the iterative approach recited in claim 23. PO Resp. 12; *see Johnston*, 435 F.3d at 1385. Therefore, for purposes of this *inter partes* review, we construe claims 25–27 to be of the same scope as, and stand or fall with, independent claim 23.

With respect to claim 22, which recites in part that "the new certificate may contain either the existing or a new public key," the parties appear to agree that the recited language *requires* the certificate to have *either* the existing public key *or* a new public key. However, we find that the permissive language in claim 22 also fails to further limit the claim. The

claim could have recited that the certificate *contains* (as opposed to may contain) either the existing or a new public key. Therefore, we find the scope of claim 22 to be the same as if the claim recited: "The method of claim 18, performed upon expiration of an existing certificate."

"verified by a direct inquiry to the certification authority"

The parties dispute the proper construction of this phrase. However, we need not reach this issue because the disputed phrase is recited only in claim 25 as part of a non-limiting clause. As discussed above, we construe claims 25–27 to be of the same scope as claim 23.

B. The Asserted Grounds

1. Anticipation of Claims 18–31 by Kapidzic

Petitioner asserts claims 18–31 are unpatentable as anticipated by Kapidzic, and provides a chart showing where Kapidzic allegedly discloses each limitation. Pet. 15–34. As explained below, we conclude that Petitioner has met its burden to show, by a preponderance of the evidence, as required by 35 U.S.C. § 316(e), that claims 18–21 and 23–31 are unpatentable as anticipated by Kapidzic. Petitioner, however, has not met its burden to show, by a preponderance of the evidence, that claim 22 is unpatentable as anticipated by Kapidzic.

a. *Kapidzic (Ex. 1004)*

Kapidzic is one paper in a collection of papers, which were the subject of a symposium on network and distributed system security. Ex. 1004, 1–4, 10. Kapidzic discloses a "Certificate Management System (CMS)," which "is a networked system for generation, distribution, storage and verification of certificates for use in a variety of security enhanced applications." *Id.* at 10.

Figure 1 of Kapidzic is reproduced below:

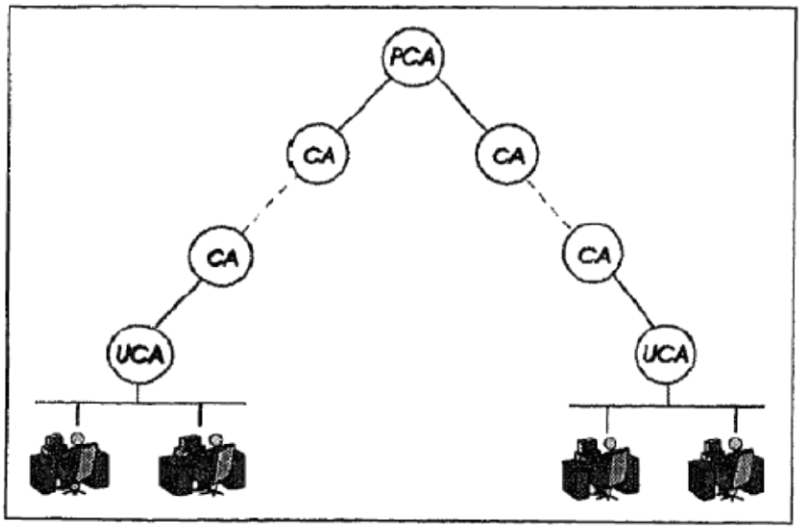

Figure 1 - A Certificate Management System

Figure 1 depicts a logical representation of a hierarchy within a public key infrastructure of the CMS disclosed by Kapidzic. Ex. 1004, 11.

b. *Whether Kapidzic Is Prior Art*

Patent Owner argues that Kapidzic is not prior art under § 102(a) because "to the extent that Kapidzic discloses any of the concepts of claims 18-31 of the '574 patent, these concepts were derived from Dr. Sead Muftic, the sole inventor of those concepts." PO Resp. 16 (citing Ex. 2010 ¶ 13). Specifically, Patent Owner asserts that "Dr. Muftic conceived of the concepts claimed in the '574 patent," and "[t]he concepts described in Kapidzic also originated from Dr. Muftic." *Id.* at 18.

Dr. Muftic testifies that: (1) he conceived of all the concepts described in Kapidzic; (2) Dr. Nada Kapidzic was his Ph.D. student from about 1992 to 1997; (3) Mr. Alan Davidson was his Licentiate student from about 1992 to 1995; (4) he explained the details of the concepts in Kapidzic to Dr. Kapidzic, who wrote about them under Dr. Muftic's direction and

supervision; (5) Mr. Davidson wrote a computer program prototype implementing the concepts of the system described in Kapidzic, and Mr. Davidson assisted Dr. Kapidzic in writing Kapidzic; (6) he omitted his name from Kapidzic to allow Dr. Kapidzic and Mr. Davidson to receive publication credit to help build their academic careers; (7) he has had a similar practice in other situations to aid students in building their academic careers and attend conferences; (8) he had already co-authored two papers (Exs. 2007, 2009, collectively "the two co-authored articles") in the same area and multiple articles in the field of computer security and "did not deem it important to list himself as an author on the Kapidzic article"; and (9) the contributions in Kapidzic are his contributions, not Dr. Kapidzic's or Mr. Davidson's. PO Resp. 18–20; Ex. 2010 ¶¶ 13–16, 19–22, 25–33. Patent Owner submits that Dr. Muftic's testimony is supported by circumstantial evidence, namely: (1) the co-authors of Kapidzic (i.e., Nada Kapidzic and Alan Davidson) were Dr. Muftic's graduate students; (2) Dr. Muftic is listed as co-author, with Dr. Kapidzic, on a paper published around the same time as Kapidzic and relating to the same area (Ex. 2007); and (3) Dr. Muftic is listed as co-author, with Dr. Kapidzic and Mr. Davidson, on another paper published around the same time and relating to the same area (Ex. 2009). PO Resp. 18–19; IPR2014-00660, Paper 57 ("'660 Tr."), 29:8–23, 30:18–31:2, 39:17–40:2.

Patent Owner argues an inventor need not be listed as an author on a reference in order to disqualify that reference as prior art. PO Resp. 17 (citing *Pictometry Int'l Corp. v. Geospan Corp.*, No. 2011-010700, 2011 WL 4857918 (BPAI Oct. 7, 2011)). Patent Owner also asserts that a declaration from an inventor is sufficient to remove a reference as prior art

and that declarations from co-authors supporting an inventor's testimony are not required. *Id.* at 16–17 (citing *In re Katz*, 687 F.2d 450, 454–55 (CCPA 1982)). At oral hearing for IPR2014-00660, which involves the same patent and a similar challenge based on Kapidzic, Patent Owner acknowledged that corroboration is necessary. *See Int'l Bus. Machs. Corp. v. Intellectual Ventures II LLC,* IPR2014–00660, Paper 57, 28:11–29:12, 34:20–24, 37:16–38:5 (August 24, 2015). Specifically, Patent Owner acknowledged that testimony of the inventor of the '574 patent is not, by itself, enough to show conception, and that Patent Owner must provide sufficient corroborative evidence that all of the ideas in Kapidzic are attributable to Dr. Muftic. *Id.* Patent Owner also acknowledged that, in order to be disqualified as a prior art reference under § 102(a), Kapidzic needs to be *only* Dr. Muftic's work. *Id.* at 41:5–19.

Petitioner argues that Patent Owner has only uncorroborated testimony from Dr. Muftic that the ideas in Kapidzic all originated from Dr. Muftic. Reply 1–3. Petitioner asserts that Patent Owner must establish that Kapidzic was solely Dr. Muftic's work. Reply 1 (citing *Allergan v. Apotex Inc.*, 754 F.3d 952 (Fed. Cir. 2014)). Petitioner argues Patent Owner's analogy to *Pictometry* is inapplicable because, in *Pictometry*, it was clear that the author of the article was writing about another's work. *Id.* at 1–2. Petitioner distinguishes *Katz*, cited by Patent Owner, by pointing out that the inventor was a co-author on the publication he sought to remove as prior art. *Id.* at 2. Petitioner argues that Dr. Muftic's testimony, by itself, is not enough to make the necessary showing that Kapidziz, which is not co-authored by Dr. Muftic, does not qualify as prior art. *Id.* Petitioner further argues that the Kapidzic article itself, and Dr. Kapidzic's thesis (Ex. 2011)

contradict Dr. Muftic's testimony that Kapidzic is Dr. Muftic's work. *Id.* (citing Ex. 2011, 3–4). Finally, Petitioner argues Dr. Muftic is unable to separate his contributions from those of Dr. Kapidzic and Mr. Davidson or from the prior art, leaving no evidence in the record showing "what in Kapidzic allegedly constitutes [Dr.] Muftic's sole work versus the work of the named authors or authors of the prior-art RFCs." *Id.* at 3 (citing Ex. 2017, 90:21–91:23, 95:16–97:22, 98:20–100:9).

The requirement for corroboration of inventor testimony "arose out of a concern that inventors testifying in patent infringement cases would be tempted to remember facts favorable to their case by the lure of protecting their patent or defeating another's patent." *Mahurkar v. C.R. Bard, Inc.*, 79 F.3d 1572, 1577 (Fed. Cir. 1996). Looking to Dr. Kapidzic's doctoral thesis, the "Publications Overview" section of Dr. Kapidzic's thesis indicates that she "was the main designer of the overall CMS system, as well as of the CMS Client [and t]he functionality of CMS servers (CAs) was designed by the author in co-operation with Alan Davidson." Ex. 2011, 3–4. That section further indicates that Kapidzic, referred to in the thesis as "KAP2," was "published as the result of the author's work," "presents the overall design of CMS (*done by the author*), as well as its functions and protocols (*done by the author in co-operation with Alan Davidson*)," and "represents the bases for *Chapter 3* of this thesis." *Id.* at 4 (emphases added).

Although we agree that authorship of articles is not necessarily determinative of whose ideas are present in a paper, we do not find Patent Owner has sufficiently corroborated Dr. Muftic's testimony to establish that the *entirety* of Kapidzic can be attributed *solely* to Dr. Muftic. Our

reviewing court has stated that "sufficient circumstantial evidence *of an independent nature* can satisfy the corroboration requirement." *Cooper v. Goldfarb*, 154 F.3d 1321, 1330 (Fed. Cir. 1998) (emphasis added). We find Patent Owner has not submitted sufficient *independent* circumstantial evidence corroborating Dr. Muftic's testimony that the entirety of the ideas in Kapidzic originated with Dr. Muftic.

Other than Dr. Muftic's own testimony, there is no evidence on record regarding which aspects of either of the two co-authored articles were his. *See* Reply 3. Even looking to Dr. Muftic's testimony, Patent Owner has not established sufficiently which aspects of Kapidzic it alleges originated with Dr. Muftic. *See* Ex. 2010 ¶¶ 13, 17, 24–26, 33. In fact, Dr. Kapidzic's doctoral thesis, as discussed above, directly contradicts Dr. Muftic's testimony, and states that the ideas in Kapidzic were those of only Dr. Kapidzic and Mr. Davidson. Ex. 2011, 3. Dr. Kapidzic's thesis was submitted approximately two years after Kapidzic was published, whereas Dr. Muftic's testimony is nearly two decades later. *Id.* at page B. Moreover, Dr. Muftic was Dr. Kapidzic's advisor and, presumably, had an opportunity to review the thesis. Weighing the submitted evidence, we find Patent Owner has not established that Kapidzic is entirely the work of Dr. Muftic. Therefore, Patent Owner has not established that Kapidzic should be disqualified as prior art.

c. *Claims 18, 19, and 21*

Kapidzic discloses a requester in a CMS sending a certificate request message to a certificate authority (CA) and the CA sending back a message with a signed certificate, which Petitioner maps to "a method of requesting and issuing a public key certificate," as recited in the preamble of

independent claim 18. Pet. 17–18, 21 (citing Ex. 1004, 10–13). Kapidzic further discloses a CA generating a pair of keys (public and private), and sending a self-signed certificate created from the public key to a parent CA. Ex. 1004, 10, 12–13. Petitioner maps that disclosure of Kapidzic to the first method step reciting that one process generates a certificate with a public key, self-signs the certificate, and sends the self-signed certificate in a request to an issuing CA. Pet. 17–18, 21–22. Kapidzic also discloses the parent CA verifying the request, signing the certificate, and sending a reply back to the requester, which Petitioner maps to the recited step of the issuing CA process "verifying the authenticity of said request, and . . . certifying and returning the" certificate to the requesting process in a reply. *Id.* at 18, 22 (citing Ex. 1004, 10, 12–13).

The description of Kapidzic's certification process that is cited as disclosing the method recited in independent claim 18 is supported by Figure 2 of Kapidzic. Figure 2 of Kapidzic is reproduced below:

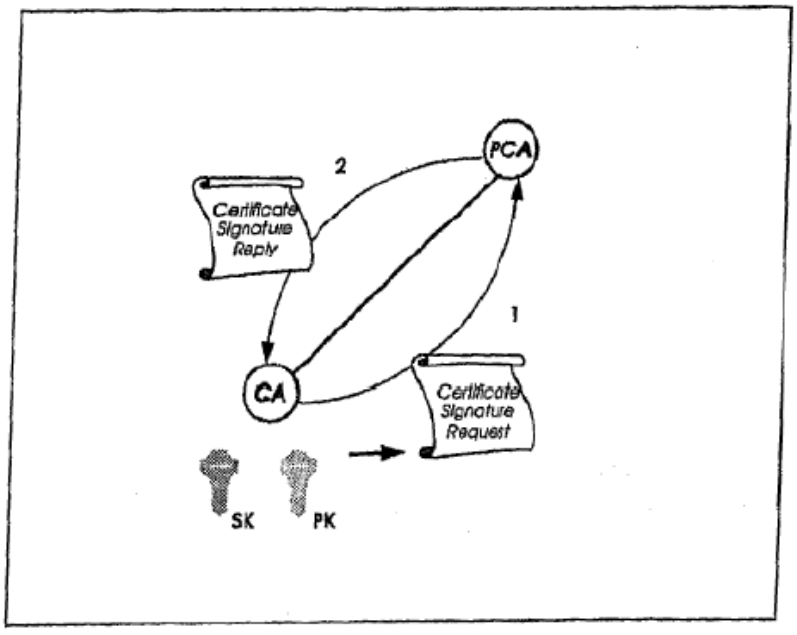

Figure 2 - Certification of a CA

Figure 2 depicts an example of a certification process of a CA by its parent CA (in this case a PCA) in the CMS disclosed by Kapidzic. Ex. 1004, 12.

Patent Owner argues that "Kapidzic does not state anywhere that the certification authorities (CAs) or other components of the CMS are processes that perform these features." PO Resp. 20. Patent Owner asserts that Kapidzic's certification process, which Patent Owner submits requires manual intervention, does not meet the method recited in claim 18, which includes "at said computer process . . . verifying the authenticity of said [certificate signature] request, and if authentic, certifying and returning the data structure in a certificate signature reply." *Id.* at 20–21. Patent Owner specifically points to the portions of Kapidzic that disclose the certificate signature request and reply messages being sent as "e-mail letters" and that verifying the identity of a requester "will normally require manual intervention," arguing that sending email messages cannot be used to automate certification because it requires manual inspection. *Id.* at 21–22 (quoting Ex. 1004, 12–13).

As previously addressed, Petitioner argues Patent Owner's proposed construction of processes, or more specifically the recited computer processes, are improperly narrow, excluding manual intervention notwithstanding disclosures in the '574 patent that contemplate manual intervention. *See* Reply 3–6. Petitioner further asserts the '574 patent describes the CAs and users as being associated with and having access to computers with software and storage for carrying out the PKI functions. *Id.* at 5 (citing Ex. 1002, 5:55–61, 9:8–10:10).

As discussed above, we do not find persuasive Patent Owner's claim construction argument that all manual intervention is excluded by the claim.

Nevertheless, we evaluate Petitioner's arguments as applied to the properly construed claims to ascertain whether Kapidzic discloses performing the recited step as claimed. The steps that claim 18 recites as being performed "at a computer process" are "generating a data structure," "sending the signed data structure," "verifying the authenticity of said [certificate signature] request," and "certifying and returning the data structure." In the context of Kapidzic, it is clear that generating a data structure, which includes generating RSA keys and which is subsequently sent via email, sending the signed data structure, which is done via email, and returning the data structure, which is also done via email, are all steps that involve computer processes. *See* Ex. 1004, 12–13. Thus, our focus is on whether Kapidzic discloses verifying the authenticity and certifying the data structure "at a computer process."

With respect to the certifying step, Kapidzic explains that "[i]f all the checks verify successfully, the parent CA signs the certificate and . . . creates a *Certificate Signature Reply* that contains the signed certificate." Ex. 1004, 13. This description indicates that the certification done by the parent CA includes "signing" the electronic data structure and, thus, involves a computer process. The verifying the authenticity step also requires a computer process. For example, even if verifying an identity is required and such verification is done manually, the issuing CA at least needs to be able to read the data structure it received by email as part of the process of verifying an identity. Thus, we find that Kapidzic discloses "at said computer process . . . verifying the authenticity of said request." Moreover, Kapidzic discloses in Section 8 that the integration of signing and storage/retrieval protocols "opens the opportunity for the CMS to *fully*

automate the process of certificate retrieval and verification, independently of any other system," and that "CMS UAs provide APIs [7], which enable different security enhanced applications to be easily interfaced with the CMS, supplying them with verified certificates." Ex. 1004, 16 (emphasis added). That disclosure appears to indicate that Kapidzic contemplates an entirely automated certificate management system, such that every process disclosed by Kapidzic, not just the processes relied upon by Petitioner for disclosing the subject matter recited in the challenged claims, could be done at a computer process.

Claim 19 depends from claim 18 and further recites "storing the received signed certificate at said requesting computer process." Claim 21 depends from claim 18 and recites performing the method of claim 18 "when adding a new entity to a certification infrastructure, which entity may be [a] policy certification authority, certification authority, application[,] or end-user." Petitioner points to Kapidzic's disclosure of storing the received certificate (Pet. 23 (quoting Ex. 1004, 13)) and performing the method of claim 18 when registering a new CA (Pet. 24 (quoting Ex. 1004, 12)). Patent Owner only argues that claims 19 and 21, which depend from claim 18, are patentable for the same reasons as argued with respect to claim 18. PO Resp. 23, 24. For the reasons discussed above, we find Petitioner has demonstrated, by a preponderance of the evidence, that claims 18, 19, and 21 are anticipated by Kapidzic.

d. *Claim 20*

Claim 20 depends from claim 18 and further recites "storing the received signed certificate or copy of a signed certificate at a common certificate repository." Petitioner maps the additional limitation recited in

claim 20 to Kapidzic's disclosure of CAs keeping "local copies of all the certificates in its certificate verification path, as well as the certificates of all its immediate subordinates," and each CA being "ready to respond to retrieval requests" for those certificates it is storing (i.e., that CA's subordinates' certificates). Pet. 23 (quoting Ex. 1004, 11, 13). Petitioner also points to the X.500 directories referenced in Kapidzic as meeting the common certificate repository, but that argument was raised for the first time in Petitioner's Reply and, therefore, we decline to consider it. Reply 7.

Patent Owner argues that keeping local copies of certificates is the opposite of having a common repository storing certificates for all CAs. PO Resp. 24. As discussed above, we find that a common certificate repository does not need to store a certificate for *every* certificate in the PKI. Therefore, under the plain and ordinary meaning of a common certificate repository, we find Kapidzic's disclosure of each CA maintaining a certificate for all of the certificates it has issued to its direct subordinates meets the recited common certificate repository because each CA is a common storage location for the certificate of each subordinate processes (CAs and/or users). Therefore, we find Petitioner has demonstrated, by a preponderance of the evidence, that claim 20 is anticipated by Kapidzic.

e. *Claim 22*

Claim 22 depends from claim 18 and further recites performing the method of claim 18 "upon expiration of an existing certificate, where the new certificate may contain either the existing or a new public key." Ex. 1002, 20:5–7. Patent Owner argues that Kapidzic discloses performing the process that Petitioner maps to the subject matter of claim 18 "when a current pair of ***keys*** expires," not when the *certificate* expires. PO Resp. 24–

25. Patent Owner argues expiration of keys is not the same as the expiration of a certificate. *Id.* at 25. Petitioner argues Kapidzic discloses this limitation because the same certification procedure discussed above is followed when a CA's key pair expires requiring the CA to change its keys. Pet. 24. Petitioner further argues "Dr. Chong offered no explanation for why key expiration is not the same as certificate expiration," and asserts PKI Study describes a certificate expiring when its keys expire. Reply 7–8 (citing Ex. 1005, 71–72, 134–36).

Notwithstanding Petitioner's assertion that Patent Owner has not explained why key expiration is not the same as certificate expiration, the burden is on Petitioner to demonstrate the claim elements are disclosed by Kapidzic. Petitioner merely cites to PKI Report, which it alleges demonstrates that a skilled artisan would understand that key expiration results in certificate expiration. Petitioner, however, does not provide sufficient testimony to support its attorney argument. *See* Pet. 14; Reply 8. Thus, Petitioner has not met its burden in demonstrating anticipation of claim 22 by Kapidzic. Accordingly, we find Petitioner has not demonstrated, by a preponderance of the evidence, that claim 22 is anticipated by Kapidzic.

f. *Claims 23–27*

Kapidzic discloses a CA sending a "Certificate Reply" message "contain[ing] the requested certificate as well as all the certificates in the certificate verification path, up to the top of the hierarchy," which Petitioner maps to "obtaining a public key certificate for every computer process in the infrastructure between the sender and a common point of trust in the infrastructure," as recited in independent claim 23. Pet. 25–26 (citing Ex.

1004, 13–14). Kapidzic also discloses "verif[ying] the signatures of the certificates from the message, starting from the PCA's certificate" down to the lowest level certificate in the message, which Petitioner maps to "verifying the authenticity of signatures iteratively, beginning with the common point of trust," as recited in claim 23. *Id.* at 26 (citing Ex. 1004, 13). The portions of Kapidzic cited by Petitioner explain that the verification process, when requesting a certificate, is the same process used when initially receiving a signed certificate. Ex. 1004, 13.

Patent Owner argues that Kapidzic does not explain how the certificate "of a second user" that is being verified was received and, thus, Kapidzic does not disclose verifying the certificate *of a sender*. PO Resp. 26–27. Patent Owner further argues that, because Kapidzic does not disclose "processes," claim 23 is not anticipated by Kapidzic. *Id.* at 27–28.

Petitioner points out that Patent Owner argues in its Response "that Kapidzic teaches requesting and issuing certificates via email communications, so every signed data structure in Kapidzic is therefore from 'a sender' (i.e., each certificate request and issued certificate was sent by some entity via email) and thus clearly meets claim 23's requirement." Reply 8. Petitioner further asserts that Kapidzic clearly describes a scenario where a UCA is a "sender." *Id.* (citing Ex. 1004, 13).

We have already discussed above that Kapidzic discloses computer processes generally. Moreover, as discussed above, the '574 patent explains that each of the entities in a hierarchy is associated with a process. Given the context of how the '574 patent informs a proper construction of performing the recited steps at or by a computer process, we find unpersuasive Patent Owner's arguments that Kapidzic lacks processes or

that Kapidzic does not obtain public key certificates for each process. In view of the disclosure of the '574 patent, we find Kapidzic's chain of certificates returned to a requester meets the recited certificates for each computer process.

Claims 24–27 depend from claim 23. Claim 24 further recites that "a public key certificate for every computer process in the infrastructure between the sender and a common point of trust is also verified against all relevant certificate revocation lists." Petitioner points to Kapidzic's disclosure of checking each certificate being verified against CRLs. Pet. 27 (quoting Ex. 1004, 15–16). Patent Owner only argues that claim 24 is patentable for the same reasons as argued with respect to claim 23. PO Resp. 28. As discussed above, we find the scope of claims 25–27 to be the same as claim 23. Thus, for the reasons discussed above, we find Petitioner has demonstrated by a preponderance of the evidence that claims 23–27 are anticipated by Kapidzic.

g. *Claims 28 and 29*

Kapidzic discloses "[t]he certificate verification process must therefore include a check that the otherwise seemingly valid certificate has not been revoked." Ex. 1004, 15. Kapidzic also discloses "check[ing] the certificate against the current CRL of the same issuer" for every certificate being verified. *Id.* Petitioner maps those disclosures of Kapidzic to the method of validating a public key including using CRLs "of each computer process between a computer process or user whose certificate is being validated and a point of trust in common with the computer process or user which is validating the certificate," as recited in independent claim 28. Pet. 29. Kapidzic also discloses storing CRLs for later use in verification after

retrieval of CRLs and obtaining CRLs if they are not available locally, which Petitioner maps to "[t]he method of claim 28 in which retrieved certificate revocation lists are stored locally in the computer at which the certificate is being validated," as recited in dependent claim 29. *Id.* (citing Ex. 1004, 15–16).

Patent Owner again argues that Kapidzic does not disclose computer processes. PO Resp. 33–34. Patent Owner also asserts that Kapidzic merely discloses checking each certificate against a current CRL of the same issuer. *Id.* at 32–33. Patent Owner appears to argue that each certificate must be checked against multiple CRLs. *Id.* Patent Owner only argues that claim 29, which depends from claim 28, is patentable for the same reasons as argued with respect to claim 28. *Id.* at 34.

Petitioner interprets Patent Owner's argument as asserting "that Kapidzic is not explicit about using every CRL in the chain between a point of trust and the user whose certificate is being validated." Reply 10. Petitioner argues that Patent Owner's declarant, Dr. Chong, could not explain the argument regarding checking every CRL and could not identify which CRLs are not checked in a simple three-node chain of trust example. *Id.* (citing Ex. 1010, 75:23–76:14). To the extent Patent Owner argues that there are CRLs in a chain of trust that are not checked against at least one certificate, we disagree. Petitioner pointed to portions of Kapidzic that disclose checking each certificate associated with each CA in the chain of trust against a CRL maintained by that respective CA. *See* Pet. 29 (quoting Ex. 1004, 15).

To the extent Patent Owner argues each certificate needs to be checked against multiple CRLs, we disagree with such an implicit

construction. The appropriate construction of claim 28, in light of the specification, includes using the CRL created at each CA to ensure that each certificate issued by that respective CA does not appear on that CRL, i.e., the CRL retrieved from the respective issuing CA. We have already addressed Patent Owner's assertion that Kapidzic does not disclose processes generally and find that each CRL is associated with a particular CA and its processes. Therefore, we find Petitioner has demonstrated, by a preponderance of the evidence, that claims 28 and 29 are anticipated by Kapidzic.

h. *Claim 30*

Kapidzic discloses that a new key pair may need to be generated when the key expires or is believed to be compromised and that "[w]hen a new key pair is generated by some CA, the same procedure is followed as in the original certification." Ex. 1004, 13–14. Kapidzic also discloses that "when a certificate is updated, the old certificate must be revoked" and the CA needs to re-sign all certificates it has issued with its new key and inform its subordinates of the change so that the entire sub-hierarchy can be updated iteratively. *Id.* at 12, 14. Petitioner maps those disclosures of Kapidzic to the method of updating certificates recited in independent claim 30. Pet. 30–32 (citing Ex. 1004, 10–15).

Patent Owner argues that Kapidzic does not disclose several of the steps of claim 30. PO Resp. 34–40. For clarity in analyzing Patent Owner's arguments, we provide an explanation of how the method of claim 30 is performed using a simple exemplary infrastructure wherein process A has subordinate processes M and N, and process M has subordinate processes X and Y. In this example, M is the recited "first computer process," A is the recited "computer process which is authorized to issue the new signed

certificate," and X and Y are the recited "subordinate computer processes [of process M]." In this example, therefore, M "possesses a certificate[] to be updated." According to the process recited in claim 30, M's certificate is updated by "receiving a new signed certificate [MC2] from" A, and revoking M's "current certificate [MC1] previously used for verification of certificates of" X and Y. The receiving step is not disputed by Patent Owner as being disclosed by Kapidzic.

Patent Owner argues that, even though Kapidzic discloses revoking a certificate when its keys change, Kapidzic does not disclose the next step—revoking certificates that were previously used for verification—because no reference to revoking certificates in Kapidzic explicitly states that the certificate to be revoked was used to verify certificates of subordinate computers. PO Resp. 35–36. Patent Owner's argument is unpersuasive. Kapidzic discloses revoking a certificate that was used to verify subordinate processes' certificates. In fact, in Patent Owner's subsequent argument, it cites one of the passages in Kapidzic explaining that changing keys of a CA "affects the certification hierarchy, since all certificates of direct subordinates *have been signed with the old secret key*." PO Resp. 37 (quoting Ex. 1004, 14 (emphasis added)). In our example, that passage of Kapidzic discloses that, prior to revocation of M's current certificate (MC1), certificates of M's direct subordinates, X and Y, "have been signed with" MC1. Thus, when revoking MC1, Kapidzic discloses revoking a certificate that was previously used for verification.

The next recited step is "issuing new certificates [XC2 and YC2] to all subordinate computer processes [X and Y, respectively] for which certificates had been previously signed by the first computer process [M]."

Patent Owner does not appear to dispute that Kapidzic discloses this step of claim 30. Regardless, Petitioner points to Kapidzic's disclosure of the process that occurs in response to updating keys in a certificate. Pet. 31 (quoting Ex. 1004, 12–15). In particular, Petitioner points to the explanation in Kapidzic of sending "*Certificate Re-Sign*" messages using the same format as the "*Certificate Signature Reply*" messages. *Id.* We agree that Kapidzic discloses the recited step of issuing new certificates to subordinate processes.

The next recited steps, which Patent Owner argues are not disclosed by Kapidzic, are "copying to all subordinate computer processes the new certificate to be used for verification of new subordinate certificates" and iteratively distributing new certificates. PO Resp. 36–38. Patent Owner argues claim 30 recites copying a newly issued certificate (which is used to verify subordinate computers' certificates) to the subordinate computers, whereas Kapidzic discloses using the newly-issued certificate to certify new certificates for each of its subordinate computers that are copied to each respective subordinate computer and will, in turn, be used by those subordinates to certify each of their subordinate computers' certificates. *Id.* at 37. Patent Owner argues the recited "iteratively performing the distribution" step also relates to distributing the newly signed certificate, which we refer to in this example as MC2. *Id.* at 38. We agree with Patent Owner regarding the disclosure of Kapidzic. We disagree, however, with Patent Owner's implicit claim construction, which we find inconsistent with what the '574 patent discloses.

In our example, Patent Owner argues that claim 30 requires copying MC2 (M's newly issued certificate) to each of its subordinate processes, X

and Y (and iteratively to further subordinate processes of X and Y). A review of the claim, in light of the specification, leads us to a different construction. Continuing with our example, we construe the claim to require copying XC2 to X and copying YC2 to Y. Initially, looking at the language of the claim, we note that step "a.1" recites "receiving a new *signed* certificate [MC2]," and step "a.3" recites "issuing new certificates [XC2 and YC2] to all subordinate computer processes." Ex. 1002, 20:51–58 (emphasis added). The disputed copying step recites "copying to all subordinate computer processes the *new certificate to be used* for verification." *Id.* at 20:59–61 (emphasis added). Thus, the claim language refers back to the "new certificates" (i.e., XC2 and YC2) rather than referring to the "new signed certificate" (i.e., MC2), supporting a construction that "the new certificate" being copied to a subordinate computer process is a respective new certificate that is "to be used" by that process to verify its subordinate processes' certificates.

Moreover, a review of the processes described in the '574 patent supports this construction. Ex. 1002, Figs. 8, 9, 12, 13, 15, 16, 14:24–53, 15:4–32, 15:44–58. Specifically, the "Update__CA" process described in the '574 patent, which invokes additional processes and sends various messages, describes copying a newly issued certificate to each subordinate computer process (through a "Certificate__Resign__Reply" message) so that each respective subordinate computer process may use that certificate to certify its subordinate computer processes. *Id.* The process may then repeat if the subordinate computer process has its own subordinate computer processes. *Id.* at 15:48–51. The process disclosed does not describe copying a newly issued parent certificate (MC2 in our example) to one of its

subordinate computer processes (X and Y in our example). Therefore, we are persuaded that Kapidzic discloses the recited copying and iterative distribution steps.

Patent Owner also repeats its argument that Kapidzic does not teach processes. Patent Owner's argument regarding Kapidzic's processes already has been addressed above. Therefore, we find Petitioner has demonstrated, by a preponderance of the evidence, that claim 30 is anticipated by Kapidzic.

i. *Claim 31*

Kapidzic discloses that "[t]he certification hierarchy is established top-down, starting with the PCA," which is responsible for the administration of the hierarchy structure. Ex. 1004, 11–12. Kapidzic further discloses that establishment of a CA includes two phases, specifically registration and certification (the request for and signing of a certificate discussed above) and that "[n]o CA can be added to the hierarchy without first registering its DN with the PCA." *Id.* In order to register itself, a CA may provide a suggested "relative distinguished name" and the name of its parent CA, which specifies its place in the CMS hierarchy. *Id.* at 12. Upon receipt of that information, the PCA may generate a unique distinguished name (DN) for the CA and "[t]he PCA updates its local database with the CA's DN, address and its position in the hierarchy." *Id.* Petitioner maps the disclosures of Kapidzic related to registration of a CA to "adding a new component to a representation of a certification infrastructure at a location indicative of where the said computer process is to be added," as recited in independent claim 31. Pet. 33 (citing Ex. 1004, 10–12).

As part of the certification process in the CMS, Kapidzic discloses that the parent CA verifies a request from a CA desiring certification, signs

the certificate, *stores a local copy*, and sends a reply with the signed certificate back to the requesting CA. Ex. 1004, 13. Kapidzic also discloses that the requesting CA verifies the signatures of the certificates from the reply message (including its own requested certificate) and stores the certificates in a local database. *Id.* Petitioner maps those disclosures to "creating entries in a certificate storage database at least at both said new computer process and at the computer process authorized to certify the said new process," and "obtaining a signed certificate for the said new computer process from said computer process authorized to certify the new process and storing it at the said new computer process," as recited in independent claim 31. Pet. 33–34 (citing Ex. 1004, 12–14).

Patent Owner argues only that Kapidzic does not disclose that CAs or other CMS components are processes. For the reasons discussed in the claim construction section, we find Kapidzic discloses computer processes. Moreover, we find that those processes are associated with the various CMS entities or components and that the portions of Kapidzic pointed to by Petitioner disclose the recited steps of claim 31. Therefore, we find Petitioner has demonstrated, by a preponderance of the evidence, that claim 31 is anticipated by Kapidzic.

2. Anticipation of Claims 23–31 by PKI Report, Obviousness of Claims 25, 29, and 30 over PKI Report, and Obviousness of Claims 18–22 over PKI Report and RFC 1424

Petitioner asserts claims 23–31 are unpatentable as anticipated by PKI Report, claims 25, 29, and 30 would have been obvious in view of PKI Report, and claims 18–22 would have been obvious in view of PKI Report and RFC 1424. Pet. 34–59. Petitioner provides a chart showing where PKI Report allegedly discloses or teaches each limitation of claims 23–31 and

where the PKI Report or RFC 1424 teaches each limitation of claims 18–22. *Id.* at 40–59. As described below, we conclude that Petitioner has met its burden to show, by a preponderance of the evidence, as required by 35 U.S.C. § 316(e), that claims 18–30 are unpatentable as anticipated by, or obvious in view of, PKI Report or the combination of PKI Report and RFC 1424. We further conclude, however, that Petitioner has not met its burden to show, by a preponderance of the evidence, that claim 31 is unpatentable as anticipated by PKI Report.

a. *PKI Report (Ex. 1005)*

PKI Report is the result of a study requested by the NIST (National Institute of Standards and Technology) and conducted by the MITRE Corporation to study "alternatives for *automated* management of public keys and of the associated public key certificates for the Federal Government." Ex. 1005, 5, 7 (emphasis added). PKI Report addresses issues of a public key infrastructure (PKI) for automatically managing public keys using public key certificates. *Id.* at 7. PKI Report includes user and technical "requirements that relate to the generation and distribution of keys, to the obtaining of public key certificates and to the distribution of" CRLs. *Id.* The entities within the PKI may be arranged in a hierarchical structure. *Id.* at 8.

The PKI described in PKI Report may be used for encrypting messages to ensure confidentiality, but the focus of PKI Report is verifying the sender of a message. Ex. 1005, 22. In order to verify the signature on a message, a recipient must be confident in the integrity of the public key used to decrypt the signed message. *Id.* at 22, 26. The verifier may have confidence in the integrity of the key used to decrypt a message "because it

was manually delivered [or the verifier] obtained it from a certificate signed by an entity for which he holds a public key he trusts." *Id.* at 26. Thus, the verifier must hold a chain of trusted keys back to a common point of trust, for which the verifier obtained a key "in a trusted 'out-of-band' manner." *Id.* This chain of trust is called a certification path (*id.* at 27) and allows for a hierarchical system of validating a certificate by starting with the common point of trust and iteratively obtaining the key at the next level until the sender's certificate may be verified using the issuing CA's key. *Id.* at 26, 27. In particular, a "certification path is a sequence of CAs, the first being a CA for which the verifier holds a trusted copy of the public key and the last being the CA that issued the certificate certifying the needed PKI entity's public key." *Id.* at 27.

Recognizing that keys in global systems may originate from anywhere in the world, PKI Report studied alternatives for establishing an *automated* system to manage and distribute keys *electronically*, namely a PKI. Ex. 1005, 23. The purposes of the desired PKI include generating public key certificates binding the identity of users to their public keys, providing users with easy access to other users' certificates, and providing users with timely information regarding revocation of certificates. *Id.*

b. *RFC 1424 (Ex. 1006)*

RFC 1424 describes "key certification, certificate-revocation list (CRL) storage, and CRL retrieval," which are services supporting privacy enhanced mail, as required by a CA. Ex. 1006, 1.

c. *Obviousness of Claims 18–22 over PKI Report and RFC 1424*

Petitioner argues that PKI Report discloses each limitation of independent claim 18 and dependent claims 19–22. Pet. at 38. Petitioner states that PKI Report "is not explicit that the requester 'self-signs' a data structure that it sends to the issuing authority to request a certificate in a certificate request message and that the issuing authority returns the data structure in a certificate signature reply" because PKI Report's disclosure of those aspects is summarizing disclosures of RFC 1424. *Id.* However, Petitioner asserts RFC 1424 clearly discloses those limitations (as well as the entirety of limitations "a" and "b" of independent claim 18) and that PKI Report summarizes those disclosures. *Id.* at 38–39 (citing Ex. 1006, 2–3; Ex. 1005, 129).

PKI Report explains that a goal of the study is to "design [a public key] infrastructure that will allow users to establish chains of trust" and "to facilitate trusted electronic correspondence beyond those users with whom one has manually exchanged public keys." Ex. 1005, 27. Petitioner points to those, and various other disclosures in PKI Report relating to the implementation of the disclosed PKI regarding managing public keys in a hierarchical certificate management infrastructure, and argues that PKI Report teaches the method of requesting and issuing public key certificates in a secure certification system as recited in claim 18. Pet. 40.

PKI Report and RFC 1424 further describe a process for a user or CA to obtain a public key certificate including sending a self-signed request including the public key to an issuing CA and the issuing CA verifying the signature on the request, generating and signing a certificate using its private

key, and sending the signed certificate back to the requester. Ex. 1005, 30, 65–66, 73, 129, 134; Ex. 1006, 2–5. Petitioner maps those disclosures of PKI Report and RFC 1424 to the method steps of requesting and issuing a public key certificate recited in independent claim 18. Pet. 40–43.

Petitioner asserts it would have been obvious to combine PKI Report with RFC 1424 because PKI Report discloses an electronic transaction of a requester requesting a certificate and an issuing CA returning a certificate to the requester, and RFC 1424, which offers a known way of executing the described transactions, is identified in PKI Report as a standard reviewed in drafting PKI Report. Pet. 39 (citing Ex. 1005, 129). Therefore, Petitioner asserts implementing the transactions disclosed by PKI Report with "the specific certificate request and issuance features described by RFC 1424 would have been nothing more than applying a known technique to address the mechanics of electronic requesting and issuing of a certificate," and a skilled artisan would have learned of RFC 1424 from PKI Report, such that it would have at least been obvious to try such a solution. *Id.* at 40 (citing Ex. 1001 ¶¶ 106–108).

Patent Owner argues neither PKI Report nor RFC 1424 discloses that the components of the certification infrastructure are processes, and that certification according to PKI Report and RFC 1424 requires manual processing of certificates. PO Resp. 42–46. Patent Owner also argues that Petitioner's declarant, Dr. Naccache, testified that "RFC 1424 does not disclose the data structure described in" claim 18. PO Resp. 46 (quoting Ex. 2014, 74:3–6). Dr. Naccache, however, was asked a different question—namely "[i]s it your testimony that *the self-signed certificate* of RFC 1424 corresponds with the recited data structure?" *Id.* (emphasis added) (quoting

Ex. 2014, 74:3–6). Prior to the quoted question and answer, Dr. Naccache testified that RFC 1424 does disclose a data structure and that RFC 1424 also discloses self-signing that data structure as part of the certification process. Ex. 1011, 73:8–74:15. Thus, Patent Owner's argument regarding Dr. Naccache's testimony is based on, at best, a misreading of that testimony.

Petitioner argues "occasional human assistance [in PKI Report] is irrelevant given the clear disclosures of using emails and computer processes in the certification process." Reply 12. Petitioner also points to the portion of PKI Report disclosing that the "term entity is used in this section to mean any component of the PKI be they human or machine and include: users, process, CAs, ORAs, CA operators and ORA operators." Reply 11–12 (emphasis omitted).

We disagree with Patent Owner's construction of performing a step "at a computer process," as excluding manual invocation or other human intervention. For the reasons discussed above with respect to the disclosure of the '574 patent, our construction of computer process, and the disclosures of PKI Report and RFC 1424, we find PKI Report and RFC 1424 disclose using computer processes as part of the certification infrastructure. Thus, as discussed above, the relevant inquiry is whether PKI Report teaches using the computer processes as recited in the challenged claims.

As disclosed by PKI Report, one point of the study was to establish an automated system for managing and distributing keys electronically. Ex. 1005, 23. Moreover, PKI report generally discloses that CAs (or other entities) generate keys and verify and certify subordinates' certificates. *Id.* at 66. These disclosures of executing procedures regarding the generation

and analysis of electronic data structures involve the use of computer processes. *See, e.g., id.* ("it was assumed that the user had either software or hardware that was capable of generating the key pair for the user"). Because PKI Report and RFC 1424 teach that generating a data structure, self-signing the data structure, sending the signed data structure as a certificate signature request, verifying the authenticity of the request, and certifying and returning the data structure are functions involving computer processes to create, modify, and transmit electronic data structures, Petitioner has demonstrated, by a preponderance of the evidence, that the combination of PKI Report and RFC 1424 teaches performing the method of claim 18.

Petitioner also provides arguments mapping various disclosures of PKI Report to the additional limitations recited in claims 19–22, which depend from claim 18. Pet. 43–45 (citing Ex. 1005, 31, 36, 38, 42, 44, 54, 55, 66, 71, 73, 74, 117). With respect to claim 19, Patent Owner only argues patentability for the same reasons argued with respect to claim 18. PO Resp. 46.

Patent Owner asserts claim 20 is patentable because PKI Report teaches each CA depositing certificates at different directory servers, which is the opposite of a common repository. *Id.* at 46–47 (citing Ex. 1005, 54). Patent Owner's argument, however, is directed to a portion of PKI Report discussing backup servers – i.e., the existence of multiple directory servers to increase system reliability in case one directory server goes down. *See* Ex. 1005, 54. That same section explains that a system employing a "hot backup," which holds "exactly the same information as the primary server," might have only one (replicated) repository for certificates. *Id.* Thus, even under Patent Owner's proposed construction, PKI Report discloses a

common repository. Moreover, even assuming that two directory servers are not identical, PKI report teaches that each directory server could hold multiple certificates and would therefore meet the broadest reasonable construction of the recited common repository.

Patent Owner argues Petitioner has not established that the certification process recited in claim 18 is performed when adding a new entity to the infrastructure, as recited in claim 21. PO Resp. 47–48. Patent Owner argues claim 22, which depends from claim 21, is patentable for the same reasons as asserted with respect to claim 21. *Id.* at 48. Petitioner asserts PKI Report teaches that new CAs may be required, and that addition of a new CA requires certification from an appropriate PCA. Pet. 44–45; Reply 13. We are persuaded by Petitioner's argument.

Therefore, for the reasons discussed above, we find Petitioner has demonstrated, by a preponderance of the evidence, that the subject matter of claims 18–22 would have been obvious in view of PKI Report and RFC 1424.

d. *Anticipation of Claims 23–27 by PKI Report or Obviousness of Claim 25 over PKI Report*

PKI Report discloses that a recipient may receive a certification path from the sender along with the signed document received. Ex. 1005, 67. As discussed above, a certification path includes each CA in the path between the sender and the common point of trust. *Id.* at 27. Based on those disclosures, Petitioner maps the receipt of the certification path to "obtaining a public key certificate for every computer process in the infrastructure between the sender and a common point of trust in the infrastructure," as recited in claim 23. Pet. 46–47 (citing Ex. 1005, 26, 27, 35, 66, 67). PKI

Report further discloses verifying each certificate in the path, starting with the certificate signed by the common point of trust and iteratively using the decrypted key to verify the certificate at the next lower level in the hierarchy until the certificate of the CA that signed the sender's certificate is verified. Ex. 1005, 67–68. Petitioner maps that disclosure of PKI Report and other disclosures to "verifying the authenticity of signatures iteratively, beginning with the common point of trust," as recited in claim 23. Pet. 47–48 (citing Ex. 1005, 26, 37, 67–68, 72, 127, 132).

Patent Owner argues PKI Report does not anticipate claim 23 because PKI Report does not teach that CAs are processes and only teaches obtaining "one or more" additional certificates to verify a sender's certificate. PO Resp. 48–49. We do not agree with Patent Owner regarding its assertion about processes for the reasons already discussed above. We also are not persuaded by Patent Owner's assertions that PKI Report's disclosure of obtaining "one or more" additional certificates does not meet the recited step of obtaining a certificate for every process between the sender and the common point of trust.

First, in the simple case where there are no intervening processes between the sender and the common point of trust, PKI Report explicitly indicates that it would obtain a certificate for every process. Second, it is clear from the context that the reference in PKI Report to the possible need for a recipient to "obtain one or more additional certificates . . . in order to verify the signature on the sender's certificate" is a general statement that the sender's certificate (unless it is the common point of trust) will not be enough to verify the signature on the sender's certificate. Ex. 1005, 67. PKI Report explains that a certification path includes every process between the

sender and a common point of trust and that, a recipient receives a certification path along with a signed document and must obtain all certificates within the certification path. *Id.* at 27, 67–68.

Claims 24–27 depend from claim 23. Claim 24 further recites that "a public key certificate for every computer process in the infrastructure between the sender and a common point of trust is also verified against all relevant certificate revocation lists." Petitioner points to PKI Report's disclosure of checking each certificate being verified against CRLs. Pet. 48 (quoting Ex. 1005, 67–68, 72). Patent Owner only argues that claim 24 is patentable for the same reasons as argued with respect to claim 23. PO Resp. 49. As discussed above, we find the scope of claims 25–27 to be the same as the scope of claim 23. Thus, for the reasons discussed above, we find Petitioner has demonstrated, by a preponderance of the evidence, that claims 23–27 are anticipated by PKI Report. For the same reasons, we also find Petitioner has demonstrated, by a preponderance of the evidence, that claim 25 would have been obvious[4] in view of PKI Report.

e. Anticipation of Claims 28 and 29 by PKI Report or Obviousness of Claim 29 over PKI Report

PKI Report discloses checking each certificate against the appropriate CRL before using it, which Petitioner maps to the method of validating a public key certificate using CRLs, as recited in claim 28. Pet. 51–52 (citing

[4] Petitioner alternatively challenges claim 25 as obvious in view of PKI Report. Because we determine it is of the same scope as claim 23, and we find claim 23 is anticipated by PKI Report, it follows that claim 25 would have been obvious in view of PKI Report. *See, e.g., Cohesive Techs., Inc. v. Waters Corp.*, 543 F.3d 1351, 1364–65 (Fed. Cir. 2008) (explaining distinctions between anticipation and obviousness, but noting that "prior art references that anticipate a claim will usually render that claim obvious").

Ex. 1005, 23, 27, 67–68, 72–73). PKI Report also discloses that a user may store CRLs locally, which Petitioner maps to "retrieved certificate revocation lists are stored locally in the computer at which the certificate is being validated," as recited in dependent claim 29. *Id.* at 52 (citing Ex. 1005, 70, 118, 161, 169). Petitioner further argues that, "[t]o the extent it is determined that PKI Study does not disclose local storage of retrieved CRLs at the computer at which the certificate is being validated as recited in claim 29, that additional limitation would have been obvious to the skilled person." *Id.* at 52–53 (citing Ex. 1001 ¶ 116). In particular, Petitioner argues storing the CRL locally would have been a design choice and that is one of a finite number of solutions (storing CRLs locally, consulting a remote database). *Id.* at 53. Petitioner asserts that storing the CRLs locally, at least while executing the validation process, would have been a preferred design choice in order to avoid working with a remote database during the validation process. *Id.*

With respect to claim 28, Patent Owner argues PKI Report does not disclose that CAs or other certification infrastructure components are processes, so it does not disclose using CRLs "of each computer process." PO Resp. 53–54. PKI Report discloses that each CA is responsible for generating CRLs for all of the certificates it issues and, as Petitioner argues, PKI Report discloses checking appropriate CRLs. Pet. 51–52; *see* Ex. 1005, 27, 44–45, 67, 70. PKI Report discusses various ways of storing and retrieving CRLs, but regardless of the chosen implementation, a CRL associated with a CA in PKI Report meets the recited limitation of a CRL of a computer process because the processes executing the CA function are the processes that would create and maintain the CRL associated with that CA.

Thus, because each CA has an associated CRL and every certificate between the sender and a common point of trust is verified against an appropriate CRL, it follows that PKI Report discloses checking the CRL for each process between the sender and a common point of trust. *See* Ex. 1005, 27, 44–45, 67, 70.

Patent Owner argues only that claim 29, which depends from claim 28, is patentable for at least the same reasons as asserted with respect to claim 28. PO Resp. 54. For the reasons discussed above, we find Petitioner has demonstrated, by a preponderance of the evidence, that claims 28 and 29 are anticipated by PKI Report. For the same reasons, we also find Petitioner has demonstrated, by a preponderance of the evidence, that claim 29 would have been obvious[5] in view of PKI Report.

f. Anticipation of Claim 30 by PKI Report or Obviousness of Claim 30 over PKI Report

PKI Report's disclosure of iteratively updating certificates is similar to the iterative update procedure disclosed in Kapidzic and the '574 patent. Specifically, PKI Report recognizes that certificates may expire or become compromised, resulting in revocation of certificates, which will require the entities to generate new keys and request new signed certificates from an issuing CA. Ex. 1005, 69–71. PKI Report also recognizes the need for a CA with a compromised key to reissue all certificates it generated using its new key. *Id.* at 70. Thus, for each subordinate CA, the process would be

[5] Petitioner alternatively challenges claim 29 as obvious in view of PKI Report. Because we determine Petitioner has demonstrated that claim 29 is anticipated by PKI Report, it follows that claim 29 also would have been obvious in view of PKI Report. *See, e.g.*, *Cohesive Techs.*, 543 F.3d at 1364–65.

repeated until all subordinates in the hierarchy were updated. PKI Report further discloses that an entity with a compromised certificate will notify its parent CA, which will place the compromised certificate on a CRL. *Id.* at 69. Petitioner maps those disclosures, and others, of PKI Report to the method of updating certificates recited in claim 30. Pet. 53–56 (citing Ex. 1005, 22, 27, 69–71, 134, 162–67). Petitioner further argues that, to the extent PKI Report does not explicitly disclose iteratively distributing new certificates until all subordinate processes have been updated, as recited in claim 30, it would have been obvious to an ordinarily skilled artisan. *Id.* at 56–57 (citing Ex. 1001 ¶ 120). Petitioner argues that PKI Report explicitly discloses updating a child process (the entities for which a CA with a newly registered certificate issues certificates), and that a skilled artisan would have understood that, if any of those child processes also were CAs that issued certificates to their respective subordinates, those certificates would need to be reissued as well in order to maintain proper certification paths. *Id.* at 56–57.

Patent Owner argues claim 30 is patentable over PKI Report for essentially the same reasons asserted with respect to the challenge based on Kapidzic – i.e., PKI Report does not disclose processes and PKI Report does not disclose copying the new certificate to all subordinate processes. PO Resp. 54–57. Patent Owner also argues Petitioner's obviousness analysis is "defective as a matter of law," because the Petition "use[s] 'common sense' to supply a missing element not taught in any reference of record rather than as rationale for combining references." *Id.* at 57 (citing *K/S HIMPP v. Hear-Wear Techs., LLC*, 751 F.3d 1362, 1365–66 (Fed. Cir. 2014)).

For the same reasons discussed above, we disagree with Patent Owner's implicit construction of claim 30. We find Petitioner has demonstrated, by a preponderance of the evidence, that claim 30 is anticipated by PKI Report. We also disagree with Patent Owner's application of *K/S HIMPP*. *See* PO Resp. 57. We agree with Petitioner's statement that the Petition's application of "common sense" was in support of a rationale for modifying PKI Report to include distributing a certificate to *all* subordinates, to the extent that was not explicitly disclosed. *See* Reply 14–15. Because Petitioner has presented a sufficient rationale, supported by testimony (*see* Ex. 1001 ¶ 120), for modifying PKI Report to the extent necessary, we further find Petitioner has demonstrated, by a preponderance of the evidence, that claim 30 would have been obvious in view of PKI Report.

g. Anticipation of Claim 31 by PKI Report

As discussed above, PKI Report describes adding new CAs to the hierarchy and storing certificates at both an issuing CA and the entity (a user or CA) that requested a signed certificate. Ex. 1005, 55. PKI Report discusses various hierarchical arrangements of a certificate management system. *Id.* at 22, 27, 36–38, 42, 44–45, 48–51. PKI Report also discloses creating and signing certificates, and storing those certificates at various points in the hierarchy. *Id.* at 44–45, 66, 73, 117, 134. Petitioner maps those disclosures of PKI Report to the method of adding a new process to the infrastructure recited in claim 31. Pet. 57–59.

Patent Owner argues PKI Report teaches adding a PCA and new CAs but does not teach "adding a new component to a ***representation*** of a certification infrastructure," as recited in claim 31. PO Resp. 57–58. Patent

Owner also argues that PKI Report "does not disclose a certificate storage database at any CA," and PKI Report does not teach processes. *Id.* at 59–60.

Petitioner argues PKI Report states that each entity has a unique name that distinguishes it from every other PKI entity. Reply 15. PKI Report explains that the unique names may be "formed by concatenating a sequence of locally unique names of some hierarchical substructure of the PKI." *Id.* (citing Ex. 1005, 27, 55 n.4). Petitioner, therefore, argues "the name alone is a representation of the location where the entity is added." *Id.*

We agree with Petitioner that PKI Report discloses processes and a certificate storage database at CAs. *See* Pet. 58 (quoting Ex. 1005, 117 ("the CA will need to store and retrieve the certificates it generates")). Moreover, we agree with Petitioner that the naming convention disclosed in PKI represents the location of that particular entity in the infrastructure. *See* Reply 15. However, we find Petitioner has not pointed to anything in PKI Report that discloses "adding a new component *to a representation* of a certification infrastructure." Specifically, although Petitioner points to a portion of PKI Report that discloses adding an entity to the infrastructure, and the assigned unique name may indicate the location of the entity within the infrastructure, Petitioner does not point to a disclosure of adding a component to a *representation* of the certification. As an analogy, if a parent has a daughter and names her by appending "Jill" to a concatenation of the child's ancestors' names, Jill is added to the family and has a unique name indicating her lineage, but Jill is not added to a representation of the family (e.g., a family tree diagram) merely by the assignment of a unique name. Adding Jill to her family tree diagram is a separate step. Therefore, on this record, we find Petitioner has not demonstrated, by a preponderance

of the evidence, that the subject matter of claim 31 is anticipated by PKI Report.

C. Patent Owner's Motions to Exclude Evidence

Patent Owner moves to exclude, under 37 C.F.R. § 42.64(c), PKI Report and RFC 1424 (Exhibits 1005, 1006, respectively) and Exhibits I–O attached to the Declaration of Mr. Jeffrey White. Paper 32 ("Mot."). First, we address Patent Owner's motion with respect to Exhibits I–O, which are attached to Mr. White's Declaration, as inadmissible hearsay offered to prove the truth of the alleged publication date of PKI Report and RFC 1424. *Id.* at 7–8; Paper 38, 5 ("PO Reply").

Petitioner suggests Patent Owner's Motion to Exclude with respect to portions of Mr. White's Declaration can be dismissed as moot because, to the extent Petitioner has established the admissibility of PKI Report and RFC 1424, the Declaration is unnecessary. Paper 36, 10 ("Opp."). Nevertheless, Petitioner argues all of Patent Owner's objections to Mr. White's Declaration are based on an assertion that the dates in Exhibits I–O of the Declaration are offered to prove the truth of the publication dates. *Id.* at 10–11.

Petitioner argues the date in Exhibit K is not being offered to prove the publication date of PKI Report, but rather as evidence that Defense Technical Information Center ("DTIC") indexed and catalogued PKI Report in a manner assigning it a date of April 1994. Opp. 12. Petitioner asserts Exhibit K provides circumstantial evidence of public availability prior to December 1995. *Id.*

Exhibit K to Mr. White's Declaration is offered merely to support Mr. White's testimony that a document identical to PKI Report is currently

publicly available on the DTIC website and that the document is marked with a date of April 1, 1994. *See* Ex. 1012 ¶¶ 19–20; Opp. 12. Because the document is not being offered to prove PKI Report actually was published on April 1, 1994, or for the truth of any statement made in the document, we deny Patent Owner's Motion to Exclude with respect to Exhibit K to Mr. White's declaration.

Exhibits I (a copy of Ex. 1005 - PKI Report) and J (a copy of allegedly the same report downloaded from the DTIC website) are not offered to prove any statement made within those documents, but rather to serve as a basis for Mr. White's testimony that PKI Report is identical to Exhibit J. *See* Ex. 1012 ¶¶ 16–20. Therefore, we deny Patent Owner's Motion to Exclude with respect to Exhibits I and J because the statements are not hearsay.

Petitioner argues Exhibits N and O are being offered to demonstrate "that the RFC Editor maintains an index and record of RFC 1424 (N-1) and that an RFC publication process exists (O-1-O-3)." Opp. 12. Petitioner asserts Exhibits N and O are offered to show "that RFCs are intended to be published at all and an RFC document completed in February 1993 would have been publically available prior to December 1995." *Id.*

Exhibit N is offered as evidence to support Mr. White's testimony that RFC 1424 is currently publicly available at the RFC Editor website – i.e., http://www.rfc-editor.org/rfc/pdfrfc/rfc1424.txt.pdf, and that the document is marked with a date of February 1993. *See* Ex. 1012 ¶ 23, p. N-1; Opp. 12. Because Exhibit N is not being offered to prove RFC 1424 actually was published in February 1993, or for the truth of any statement made in the

document, we deny Patent Owner's Motion to Exclude with respect to Exhibit N to Mr. White's declaration.

Exhibit O is offered as evidence that RFCs are intended to be published and that an RFC completed in February 1993 would have been publicly available before December 1995. Accordingly, the statements Petitioner relies on in Exhibit O are statements asserted for the truth of the matter asserted. *See* Ex. 1012 ¶ 24; Opp. 12. Because Petitioner relies on statements in Exhibit O regarding publication procedures in support of its assertion that RFC 1424 was publicly available as of February 1993, we grant Patent Owner's Motion to Exclude with respect to Exhibit O to Mr. White's declaration.

Exhibits L (a copy of Ex. 1006 - RFC 1424) and M (a copy of RFC 1424 downloaded from the RFC Editor website) are not offered to prove any statement made within those documents. *See* Ex. 1012 ¶¶ 21–23. Therefore, we deny Patent Owner's Motion to Exclude with respect to Exhibits L and M.

Patent Owner moves to exclude PKI Report and RFC 1424 for lack of foundation, because the references have not been shown to be a prior art printed publication. Mot. 1, 4. Specifically, Patent Owner argues Petitioner has not explained how PKI Report or RFC 1424 is prior art and that Petitioner's supplemental evidence does not cure Patent Owner's objection. *Id.* at 2, 4–5. Patent Owner argues a patent owner may argue both admissibility in a motion to exclude and sufficiency in a patent owner response, and that the right to argue sufficiency of evidence is not waived by failure to object to the admissibility of evidence. PO Reply 1–2, 5.

Petitioner responds that Patent Owner's foundation objections to PKI Report and RFC 1424 are merely an attempt to argue the sufficiency of Petitioner's evidence in support of whether PKI Report and RFC 1424 are printed publications as of the alleged date, which Petitioner argues Patent Owner waived by not raising in the Patent Owner Response. Opp. 2–4, 7–8.

Patent Owner is correct that it may argue sufficiency of evidence in a Patent Owner Response and inadmissibility of evidence in a motion to exclude. Petitioner, however, is not arguing that Patent Owner waived its right argue admissibility of PKI Report or RFC 1424. *See* Opp. 3 ("Moreover, IV's 'foundation' argument is not really about the admissibility of evidence but is actually *an attempt to argue the sufficiency* of the evidence" (emphasis added)), 7. Importantly, Patent Owner never challenged the sufficiency of the evidence in its Patent Owner Response. Thus, Patent Owner's Motion to Exclude is improper to the extent it asserts Petitioner has not sufficiently demonstrated public accessibility of either PKI Report or RFC 1424.

Patent Owner also asserts statements made within PKI Report and RFC 1424, upon which Petitioner relies to establish the publication date of the references, are statements made outside of this trial and, accordingly, constitute hearsay that should be excluded. Mot. 3, 6. Additionally, Patent Owner argues that, although it waived its authenticity objection to PKI Report and RFC 1424, it did not concede that the documents are authentic. PO Reply 1, 5. In particular, Patent Owner asserts Petitioner still has the burden to establish authenticity for the ancient document hearsay exception to apply. *Id.* at 2–3, 5.

Petitioner argues Patent Owner conceded that PKI Report and RFC 1424 are both relevant and authentic by failing to object to their relevance and failing to move to exclude the documents after making an objection to their authenticity. Opp. 2, 8. Petitioner further argues that PKI Report and RFC 1424 are authentic and subject to hearsay exceptions because they are both ancient documents under Rule 803(16) of the Federal Rules of Evidence. *Id.* at 4. Although Petitioner states that Patent Owner conceded authenticity, Petitioner asserts the evidence establishes authenticity of the documents under Federal Rule of Evidence Rule 901(b)(8). *Id.* at 4 n.1, 8 n.3.

We agree with Patent Owner that its failure move to exclude PKI Report and RFC 1424 as authentic does not obviate the requirement to determine that the documents are authentic before we may apply the ancient document exception to hearsay. *See* Fed. R. Evid. 803(16) ("a document . . . whose authenticity is established"). Nevertheless, we find both PKI Report and RFC 1424 to be authentic. The evidence submitted supports the authenticity of PKI Report. In particular, each of PKI Report and RFC 1424 is "in a condition that creates no suspicion about its authenticity." *See* Fed. R. Evid. 901(8)(A). Both documents appear consistent with their citation to other articles or papers that are contemporaneous to the time at which they are alleged to have been published. Furthermore, we do not find anything in the content of either paper or any odd markings to cast doubt on the authenticity of the documents. Additionally, PKI Report is available for download at a page on the DTIC website, which is a place where PKI Report would likely be, if authentic. *See* Fed. R. Evid. 901(8)(B). Similarly, RFC 1424 is available for download at a page on the RFC Editor website, which

is a place where RFC 1424 would likely be, if authentic. *See id.* Finally, the same evidence already discussed regarding contemporaneous documents and uncontested dates of other documents, particularly Kapidzic, that reference PKI Report and RFC 1424 provide circumstantial evidence regarding the fact that the document is 20 years old. Additionally, the evidence supports a finding that PKI Report is authentic because it is a document recorded in a public office (DTIC) and is a purported record from the DTIC, which authenticates the document as a public record. *See* Fed. R. Evid. 901(7).

Patent Owner further argues that every basis Petitioner asserts to establish that PKI Report and RFC 1424 are 20 years old, and subject to the hearsay exception for ancient documents, is itself a hearsay statement. PO Reply 3–5. Patent Owner also argues the residual hearsay exception should not apply in this case because it is reserved for exceptional circumstances and because Petitioner did not "give reasonable notice before the trial or hearing under FRE 807(b) because it cited these exhibits in the Reply." *Id.* at 4.

As mentioned above, Petitioner argues PKI Report and RFC1424 are admissible under the ancient document hearsay exception. Opp. 4. Petitioner argues PKI Report and RFC 1424 are "admissible under the residual exception in FRE 807 . . . [because Patent Owner] had reasonable notice under FRE 807(b), and all the requirements of FRE 807(a) are met." *Id.* at 6, 9. Petitioner points to the SF298 included in PKI Report and online records from the DTIC associating PKI Report with an April 1994 date as statements of material fact having equivalent circumstantial guarantees of trustworthiness and being "the most probative of the point for which they are offered" regarding PKI Report. *Id.* at 6–7 (citing Ex. 1012 ¶¶ 18–20, K-1).

Petitioner points to statements in Kapidzic and PKI Report that RFC 1424 was published in February 1993 as statements of material fact having equivalent circumstantial guarantees of trustworthiness and being "the most probative of the point for which [they are] offered" regarding RFC 1424. *Id.* at 9–10 (citing Ex. 1012 ¶¶ 22–24, N-1).

With respect to RFC 1424, Petitioner further argues references in Kapidzic and PKI Report to RFC 1424 establish that RFC 1424 was available before both Kapidzic and PKI Report. Opp. 8–9. Petitioner asserts the statements concerning RFC 1424 are admissible because the statements: are offered for the non-hearsay purpose of proving RFC 1424 was available prior to December 1995; qualify as an exception to hearsay under Federal Rule of Evidence 803(16); and were not objected to by Patent Owner as hearsay. *Id.* at 9.

We agree with Petitioner that, the dates in PKI Report and RFC 1424 are admissible as an exception to hearsay under both the ancient documents exception and the residual exception for all of the reasons asserted by Petitioner. Moreover, we find PKI Report is admissible as an exception to hearsay under the public records exception. *See* Fed. R. Evid. 803(8). Specifically, we find the evidence supports a finding that PKI Report and RFC 1424 are authentic ancient documents and, therefore, the statements in those documents are admissible under the ancient document exception to hearsay. *See* Fed. R. Evid. 803(16). We also agree with Petitioner that the circumstantial evidence summarized herein provide the sufficient circumstantial evidence that the documents are what they purport to be and were produced at the time indicated in the respective document. Moreover, we do not agree with Patent Owner's position that it did not receive

sufficient notice that Petitioner intended to rely on the dates that Patent Owner now moves to exclude as hearsay. In particular, the Petition asserted that PKI Report was published in April 1994 and RFC 1424 was published in February 1993, qualifying each document as prior art under 35 U.S.C. § 102(b). Pet. 4–5. Finally, as discussed above, we find PKI Report is a public record because it sets out the activities carried out by DTIC in researching PKI alternatives, and Patent Owner does direct us to any indication that the information sources or any other circumstances lack trustworthiness. *See* Fed. R. Evid. 803(8).

Accordingly, we deny Patent Owner's Motion to Exclude Evidence with respect to Exhibits 1005 (PKI Report) and 1006 (RFC 1424).

III.CONCLUSION

For the foregoing reasons, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 18–21 and 23–31 of the '574 patent are unpatentable as anticipated by Kapidzic, claims 18–22 are unpatentable as obvious over PKI Report and RFC 1424, claims 23–30 are anticipated by PKI Report, and claims 25, 29, and 30 are unpatentable as obvious over PKI Report.

IV. ORDER

Accordingly, it is:

ORDERED that claims 18–31 of the '574 patent are determined to be *unpatentable*;

FURTHER ORDERED that Patent Owner's Motion to Exclude Evidence is *granted* with respect to White Declaration Exhibit O;

FURTHER ORDERED that Patent Owner's Motion to Exclude Evidence is *denied* with respect to Exhibits 1005, 1006, and the White Declaration Exhibits I–N; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Geoffrey Gavin
ggavin@jonesday.com

Joseph Melnik
jmelnik@jonesday.com

Marc Vander Tuig
mvandertuig@senniger.com

Jason Jackson
jason.jackson@kutakrock.com

PATENT OWNER:

Brenton Babcock
2brb@knobbe.com

Ted Cannon
2tmc@knobbe.com

Scott Raevsky
2sxr@knobbe.com

Bridget Smith
2bzs@knobbe.com

Donald Coulman
dcoulman@intven.com

Tim Seeley
tim@intven.com