UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner

v.

ACHATES REFERENCE PUBLISHING, INC.
Patent Owner

Case IPR2013-00080
Patent 6,173,403 B1

Before HOWARD B. BLANKENSHIP, JUSTIN T. ARBES, and GREGG I. ANDERSON, *Administrative Patent Judges.*

ARBES, *Administrative Patent Judge.*

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

I. BACKGROUND

Petitioner Apple Inc. ("Apple") filed a Petition (Paper 2) ("Pet.) seeking *inter partes* review of claims 1-12 and 17-19 of U.S. Patent No. 6,173,403 B1 ("the '403 patent") pursuant to 35 U.S.C. §§ 311-19. On June 3, 2013, we instituted an *inter partes* review of claims 1-12 and 17-19 on six grounds of unpatentability (Paper 22) ("Dec. on Inst.").

Patent Owner Achates Reference Publishing, Inc. ("Achates") filed a Patent Owner Response (Paper 39) ("PO Resp."), which included a statement of material facts. Apple filed a Reply (Paper 58) ("Pet. Reply") and a response (Paper 59) ("Pet. SOF Resp.") to the statement of material facts.

Achates filed a Motion to Exclude[1] (Paper 69) ("Mot. to Exclude") certain testimony and evidence submitted by Apple in the proceeding, and included a statement of material facts. Apple filed an Opposition to the Motion to Exclude (Paper 70) ("Exclude Opp.") and a response (Paper 71) ("Exclude SOF Resp.") to the statement of material facts. Achates filed a Reply (Paper 72) ("Exclude Reply").

Apple filed a Motion for Observation (Paper 74) ("Obs.") on certain email communications (Exhibits 1067 and 1068) between Achates's two declarants, Mr. Dmitry Radbel and Dr. Xin Wang. Achates filed a response (Paper 79) ("Obs. Resp."). Achates also filed a Motion to Seal (Paper 78) ("Mot. to Seal") the email communications, and Apple filed an opposition (Paper 84) ("Seal Opp.").

[1] Achates's original motion was improper, and Achates was permitted to re-file its motion. *See* Paper 68.

An oral hearing was held on February 26, 2014, and a transcript of the hearing is included in the record (Paper 89) ("Tr.").

We have jurisdiction under 35 U.S.C. § 6(c). This final written decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

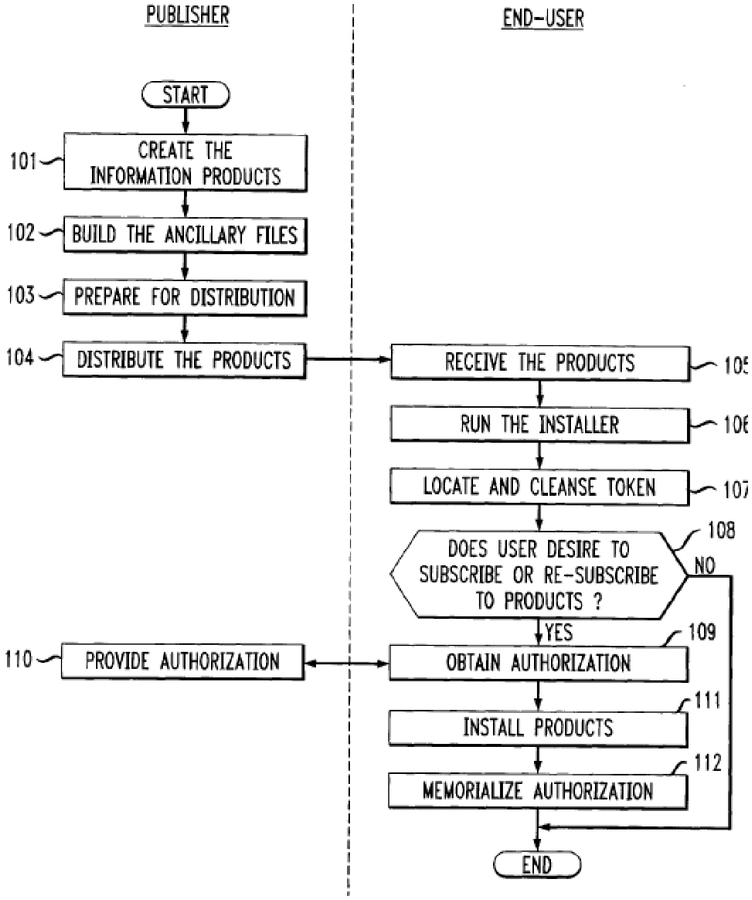
For the reasons that follow, we determine that Apple has shown by a preponderance of the evidence that claims 1-12 and 17-19 of the '403 patent are unpatentable.

A. The '403 Patent

The '403 patent[2] relates to "distributing and installing computer programs and data." Ex. 1039, col. 1, ll. 10-13. The '403 patent describes a need in the art to prevent piracy of information products, such as, for example, when a user obtains a computer program improperly or when a user purchases one copy of a program and installs it on multiple computers without authorization. *Id*. at col. 1, ll. 16-64. The '403 patent discloses methods of "distributing one or more information products together . . . while reserving to the publisher the ability to control which products are actually installed on an end-user's computer." *Id*. at col. 2, ll. 2-7.

[2] The '403 patent is a continuation-in-part of U.S. Patent Application No. 08/845,805, which issued as U.S. Patent No. 5,982,889 ("the '889 patent"). The '889 patent is the subject of related Case IPR2013-00081.

Figure 1 of the '403 patent, reproduced below, depicts the interaction between a publisher and end-user (e.g., an individual purchasing a piece of software).



As shown in Figure 1, in steps 101-102, the publisher creates a set of information products and other files. *Id*. at col. 3, ll. 32-38; col. 5, ll. 29-34. The '403 patent describes a "plurality of web pages that constitute some of the legislative, administrative and judicial materials associated with patent law," where the web pages include hyperlinks to each other, as an exemplary information product. *Id*. at col. 2, l. 64-col. 3, l. 1; col. 4, ll. 4-9. In step 103, the publisher encrypts the information products with a string as the encryption key. *Id*. at col. 7, ll. 33-42. In step 104, the information products are distributed to the end-user (e.g., on a CD-ROM or electronically over the

Internet) along with an "installer" program that runs on the end-user's computer and allows the publisher to "control how and under what circumstances the information products are installed on the end-user's computer." *Id*. at col. 2, ll. 37-47; col. 7, ll. 61-67. The installer knows the cryptosystem and key for decrypting the information products. *Id*. at col. 7, ll. 53-57.

In steps 105-106, the end-user receives the information products and runs the installer. *Id*. at col. 8, ll. 1-12. In step 107, the installer checks to see whether the end-user's computer has a previously-stored, encrypted "token" indicating that the publisher granted authorization earlier to install the information products (e.g., when an end-user has a subscription to receive multiple products over time). *Id*. at col. 8, ll. 13-27. In step 108, the end-user is asked whether he or she wants to subscribe to the information products. *Id*. at col. 9, ll. 51-57. If so, in steps 109-110, the end-user "acquires the installer's cooperation to decrypt and install the respective information products" by transmitting information to the publisher, receiving a "launch code" from the publisher in response, and entering the "launch code" into the installer. *Id*. at col. 9, l. 58-col. 10, l. 4; Fig. 4. Specifically, the end-user contacts the publisher (e.g., via telephone or the Internet) and provides (1) the end-user's name and address; (2) the end-user's method of payment; (3) the name of the requested information products; and (4) a serial number R generated by the installer. *Id*. at col. 10, ll. 5-28.

After verifying the payment, the publisher provides to the end-user a "launch code" comprising "(1) an authentication code; (2) an indicium of the name of the end-user; (3) a list of the information products to which the end-user has been granted access; and (4) an indicium of when the authorization for each information product expires," encrypted using R as the key. *Id*. at col. 10, ll. 29-44. The end-user enters the launch code into the installer, and the installer decrypts the launch code using R as the key to extract the authentication code contained therein. *Id*. at col. 10, ll. 42-49. If the authentication code matches what the installer expects, the launch code is authentic. *Id*. at col. 10, ll. 45-60; col. 11, ll. 16-37. The information products can be installed in step 111 and, if necessary, the encrypted "token" on the end-user's computer is updated in step 112 (the "token" contains the same four pieces of information as the launch code). *Id*.; col. 8, ll. 36-43. By generating a new R each time the installer requests a launch code, the disclosed method "prevent[s] the end-user from using a single launch code to install the information products on multiple computers." *Id*. at col. 10, ll. 61-64.

B. Illustrative Claims

Claims 1 and 17 of the '403 patent are the only independent claims at issue:

> 1. A method comprising:
>
> receiving an encrypted launch code;
>
> decrypting said encrypted launch code with a string, R, as the key to recover a first candidate authentication code and an indicium of a first information product; and
>
> installing said first information product onto said computer when said candidate authorization code matches a first known authorization code.

> 17. A method comprising:
>
> reading an encrypted token from a computer;
>
> decrypting said encrypted token with a string, T, as the key to recover a token that comprises an indicium of a first information product;
>
> modifying said token to comprise an indicium of a second information product;
>
> encrypting said token with said string, T, as the key to create a newly encrypted token; and
>
> storing said newly encrypted token on said computer.

C. Prior Art

The pending grounds of unpatentability in this *inter partes* review are based on the following prior art:

> 1. U.S. Patent No. 5,864,620, filed Apr. 24, 1996, issued Jan. 26, 1999 ("Pettitt") (Ex. 1006);
>
> 2. U.S. Patent No. 5,933,497, filed Jan. 29, 1993, issued Aug. 3, 1999 ("Beetcher") (Ex. 1007) (claims priority to U.S. Patent Application No. 07/629,295, filed Dec. 14, 1990);
>
> 3. U.S. Patent No. 5,949,876, filed Jan. 8, 1997, issued Sept. 7, 1999 ("Ginter") (Ex. 1005) (claims priority to U.S. Patent Application No. 08/388,107, filed Feb. 13, 1995); and
>
> 4. U.S. Patent No. 6,134,324, filed May 29, 1997, issued Oct. 17, 2000 ("Bohannon") (Ex. 1008) (claims priority to U.S. Patent Application No. 07/739,206, filed July 31, 1991).

D. Pending Grounds of Unpatentability

This *inter partes* review involves the following grounds of unpatentability:

Reference(s)	Basis	Claim(s)
Pettitt	35 U.S.C. § 102(e)	1
Pettitt and Beetcher	35 U.S.C. § 103(a)	2, 4, 5, 7, and 9
Beetcher	35 U.S.C. § 102(e)	17-19
Beetcher, Ginter, and Bohannon	35 U.S.C. § 103(a)	1-12
Ginter	35 U.S.C. § 102(e)	1-7, 9-12, and 17-19
Ginter and Beetcher	35 U.S.C. § 103(a)	8

II. ANALYSIS

A. Claim Interpretation

In the Decision on Institution, we interpreted various claim terms of the ’403 patent as follows:

Term	Interpretation
“authentication code” (claim 1)	a code for authenticating data
“candidate authorization code” (claim 1)	candidate authentication code
“known authorization code” (claim 1)	known authentication code
“installing” (claim 1)	placing in a position so as to be ready for use
“launch code” (claim 1)	password
“token” (claims 4 and 17)	a data structure indicating that an end-user’s computer is granted access to certain information products

Dec. on Inst. 8-14. The parties agree with these interpretations, *see* PO Resp. 1, and we incorporate our previous analysis for purposes of this decision.

B. Section 315(b)

Achates argues in its Patent Owner Response that Apple's Petition is time-barred under 35 U.S.C. § 315(b), which provides that an *inter partes* review may not be instituted based on a petition "filed more than 1 year after the date on which the petitioner, real party in interest, or privy of the petitioner is served with a complaint alleging infringement of the patent." PO Resp. 46-52. Achates contends that QuickOffice, Inc. ("QuickOffice"), one of Apple's co-defendants in *Achates Reference Publishing, Inc. v. Symantec Corp.*, Case No. 2:11-cv-00294-JRG-RSP (E.D. Tex.) ("the related litigation"), was served with a complaint alleging infringement of the '403 patent on June 20, 2011—more than one year before December 14, 2012, the filing date of the Petition in this proceeding. PO Resp. 46, 57. Achates made a substantially similar argument in its Preliminary Response, and we concluded that the Petition was not time-barred. *See* Paper 14 at 6-21; Dec. on Inst. 14-21. We reach the same conclusion now.[3]

Whether a non-party is a "privy" for purposes of an *inter partes* review proceeding is a "highly fact-dependent question" that takes into account how courts generally have used the term to "describe relationships and considerations sufficient to justify applying conventional principles of estoppel and preclusion." Office Patent Trial Practice Guide, 77 Fed. Reg.

[3] Also, in an earlier Order, we denied Achates's request for additional discovery on the Section 315(b) issue. Paper 18.

48,756, 48,759 (Aug. 14, 2012) ("Trial Practice Guide"). Whether parties are in privity depends on whether the relationship between a party and its alleged privy is "sufficiently close such that both should be bound by the trial outcome and related estoppels." *Id*. Depending on the circumstances, a number of factors may be relevant to the analysis, including whether the non-party "exercised or could have exercised control over a party's participation in a proceeding" or whether the non-party is responsible for funding and directing the proceeding. *Id*. at 48,759-60. We also find guidance in the Supreme Court's decision in *Taylor v. Sturgell*, 553 U.S. 880 (2008), which sets forth the general rule under federal common law that a person not a party to a lawsuit is not bound by a judgment in that suit, subject to certain exceptions, including the following:

> [N]onparty preclusion may be justified based on a variety of pre-existing "substantive legal relationship[s]" between the person to be bound and a party to the judgment. Qualifying relationships include, but are not limited to, preceding and succeeding owners of property, bailee and bailor, and assignee and assignor. These exceptions originated "as much from the needs of property law as from the values of preclusion by judgment."

553 U.S. at 894 (citations omitted); *see* Trial Practice Guide at 48,759 (citing *Taylor*).

Achates contends that QuickOffice had a pre-existing substantive legal relationship with Apple and, therefore, is a privy of Apple under *Taylor*. PO Resp. 46-52. In support of its position, Achates cites a publicly available software development kit (SDK) agreement that Apple allegedly enters into with iPhone application developers like QuickOffice. *Id*. at 48. The SDK agreement includes a clause requiring the developer to indemnify Apple for third party patent infringement claims:

> To the extent permitted by law, *You agree to indemnify, defend and hold harmless Apple, its directors, officers, employees, independent contractors and agents (each an "Apple Indemnified Party") from any and all claims, losses, liabilities, damages, expenses and costs (including without limitation attorneys fees and court costs) (collectively "Losses") incurred by an Apple Indemnified Party as a result of* Your breach of this Agreement, a breach of any certification, covenant, representation or warranty made by You in this Agreement, *any claims that Your Applications violate or infringe any third party intellectual property* or proprietary rights, or otherwise related to or arising from Your use of the SDK, Your Application(s) or Your development of Applications.
>
> . . .
>
> *In no event may You enter into any settlement or like agreement with a third party that affects Apple's rights or binds Apple in any way, without the prior written consent of Apple.*

Ex. 2006 § 6 (emphasis added). According to Achates, the fact that co-defendant QuickOffice would be obligated to indemnify Apple for infringement claims against the "same accused instrumentality" (i.e., a QuickOffice application), and would be prevented from settling in the litigation without Apple's consent, means that QuickOffice and Apple are in privity with each other. PO Resp. 47-52. Apple acknowledges that it entered into "at least one form of an agreement related to app[lication] development with [QuickOffice]," but does not admit that the agreement included the indemnification provision cited by Achates. Pet. SOF Resp. ¶¶ 129-30.

We first note that Achates provides no evidence that QuickOffice had any role in the filing or funding of the Petition in this proceeding, or that QuickOffice exercised control or could have exercised control over Apple's participation in this proceeding. *See* Trial Practice Guide, 77 Fed. Reg. at 48,759. Achates's sole evidence is the indemnification language in the SDK agreement and the fact that Apple and QuickOffice were co-defendants.

Even assuming that the specific indemnification provision of the SDK agreement applies to QuickOffice (and Achates has not shown that it does), we are not persuaded that the provision is indicative of QuickOffice being a privy of Apple. The agreement does not give the developer the right to intervene or control Apple's defense to any charge of patent infringement, nor has Achates argued that to be the case for QuickOffice in the related litigation. Notably, indemnification is not one of the "substantive legal relationships" cited in *Taylor* (e.g., assignee-assignor), and is significantly different from those relationships, which involve successive interests in the same property.

Further, as Apple points out, Achates's actions in the related litigation refute its allegations of privity. *See* Pet. Reply 15. Achates accuses Apple of infringing the '403 patent based on Apple's own actions as well as those of QuickOffice, and likewise accused QuickOffice of infringement based on activities relating to the Apple App Store as well as other systems (e.g., the Amazon Appstore for Android). *See* Ex. 1037 ¶¶ 51-52; Ex. 1038 at 84-90. Achates also is continuing to assert the '403 patent against Apple in the related litigation even after settling with the co-defendant application developers, including QuickOffice. *See* PO Resp. 58. Thus, at least according to Achates, there is a distinct basis for liability against Apple, different from that against the developers. As such, it does not appear that Apple would be estopped by any judgment against the developers. For instance, even if a judgment were obtained against one or more of the developers, Apple would still be exposed to an adverse judgment based on its own actions and would assert its own defenses independent of the developers. This further indicates that the relationship between Apple and the developers, such as QuickOffice, is not of the type that would make the developers privies of Apple.

We are not persuaded that the Petition is time-barred under Section 315(b) on the basis that QuickOffice is a privy of Apple.

C. Credibility of Mr. Schneier

As an initial matter, Achates in its Patent Owner Response challenges the credibility of Apple's declarant, Bruce Schneier. PO Resp. 52-56. Mr. Schneier provided testimony regarding the '403 patent and the prior art in a declaration submitted with Apple's Petition. Ex. 1041.[4] Achates argues that Mr. Schneier is not credible for two reasons. First, Mr. Schneier billed Apple for less than 45 hours of work, which is "nowhere near enough time to read and analyze all of the references cited in his declarations at the level of diligence that this proceeding requires," according to Achates. PO Resp. 52-54. For instance, Achates points to the size of Ginter (324 pages) and the declarations themselves (931 numbered paragraphs) to argue that Mr. Schneier "could not have performed his obligation to this matter conscientiously in the time spent." *Id*. Achates's estimate of 45 hours,

[4] Apple submitted its Petition, and Exhibits 1003 and 1041 (declarations from Mr. Schneier regarding the '403 patent and related '889 patent), on December 14, 2012. In response to an instruction from Board administrative staff that documents should be in portrait rather than landscape orientation, Apple submitted revised copies on December 17, 2012, also numbered as Exhibits 1003 and 1041. *See* Paper 4. To ensure the clarity of the record, the original versions filed on December 14, 2012 will be expunged.

however, is based on an estimate from Mr. Schneier as to the total amount Mr. Schneier *billed* to Apple. Ex. 1045 at 63:15-24; *see* PO Resp. 53. Achates does not point to any statement from Mr. Schneier regarding the number of hours he actually spent reviewing the prior art and performing the analysis in his declaration. Mr. Schneier testified that he read the prior art references at issue (Ginter, Pettitt, Beetcher, and Bohannon) multiple times and fully understood them. Ex. 1045 at 76:16-22, 77:21-78:5. Moreover, Achates's contention is not that Mr. Schneier lacks knowledge of the prior art or did not in fact perform the analysis in his declaration—just that Mr. Schneier did not spend sufficient time on the matter. We decline Achates's invitation to give Mr. Schneier's testimony less weight on that basis.

Second, Achates argues that Mr. Schneier has "hostility towards the patent system" and is a member of the Electronic Frontier Foundation (EFF), which shows a "level[] of bias that should be more than sufficient to raise concerns about his qualifications to serve as an unbiased technology expert." PO Resp. 54-56 (citing a book co-authored by Mr. Schneier, Ex. 2016, and various EFF web pages, Exs. 2017-2020). We have reviewed Mr. Schneier's curriculum vitae (Exhibit 1004) and find that he is well qualified to testify regarding the matters addressed in his declaration (Exhibit 1041). Indeed, Achates's declarant, Mr. Radbel, testified that Mr. Schneier is a "top cryptologist" and has a "great reputation as a cryptologist." Ex. 2032 at 167:9-25. As explained herein, we find Mr. Schneier's testimony persuasive and give it substantial weight. We do not give it less weight based on a purported bias against patents in general.

D. Level of Ordinary Skill in the Art

In its Petition, Apple contends that a person of ordinary skill in the art at the time of the ’403 patent (April 1997, when the application that issued as the parent ’889 patent was filed) would have had “extensive familiarity with cryptographic techniques published in the literature and known in the field,” and “would have gained this level of familiarity through graduate level studies in mathematics, engineering or computer science, or through work experience in academia (either as a professor or a graduate student), for a technology company or for a government,” relying on the testimony of Mr. Schneier. Pet. 4 (citing Ex. 1041 ¶¶ 37-39). Achates does not dispute this argument in its Patent Owner Response.[5] Mr. Radbel, however, concludes that a person of ordinary skill in the art would have had “the ability to select and make use of well-known cryptographic techniques at a high level,” but not “comprehensive knowledge of cryptography, including Mr. Schneier’s book on the subject.” Ex. 2013 ¶¶ 17, 19. Mr. Radbel further testifies that a person of ordinary skill in the art would have had “an undergraduate degree in engineering or computer science plus two years of experience in software engineering,” but not necessarily “graduate level training.” *Id.* Dr. Wang agrees with Mr. Radbel’s assessment of the level of ordinary skill. Ex. 2014 ¶ 8.

[5] Achates argued in its Preliminary Response that “the proper level of skill should be a person with at least five years of experience and[/]or academic training in professional software development having experience with client-server software and operating systems, and at least a basic working knowledge of computer security and cryptography.” Paper 14 at 23.

The parties’ declarants appear to agree that the person of ordinary skill in the art would have been familiar with the basic cryptographic techniques of the time, but dispute the depth of that knowledge. A skilled artisan would have been aware of basic cryptographic techniques and also the predominant literature on cryptography of the time. *See In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (“The person of ordinary skill in the art is a hypothetical person who is presumed to know the relevant prior art.”). As to that person’s level of education or equivalent experience, we are persuaded that Mr. Radbel understates the appropriate level of skill. The ’403 patent describes various problems with software piracy and various technical solutions to such problems. Ex. 1039, col. 1, ll. 16-63. It also assumes a fairly deep knowledge of encryption, decryption, and the use of keys for performing those functions. *See id.* at col. 7, l. 32-col. 11, l. 37. Contrary to Mr. Radbel’s assertion that a person of ordinary skill only would have needed a “high level” knowledge of cryptographic techniques, sufficient, for example, to call software routines “without necessarily understanding how such routines work,” *see* Ex. 2013 ¶ 17, a skilled artisan would need some knowledge of how the cryptographic techniques work to choose the appropriate techniques and properly use them. We also take into account the sophistication of the technology at the time, as exemplified by the prior art references of record and Mr. Schneier’s book from 1996 (Exhibit 1024). Based on all of the evidence, we conclude that a person of ordinary skill in the art at the time of the ’403 patent would have been familiar with the basic cryptographic techniques and literature of the time, and would have had some graduate-level or equivalent experience working with such techniques.

E. Grounds Based on Pettitt

With respect to the alleged grounds of unpatentability based on Pettitt, we have reviewed Apple's Petition, Achates's Patent Owner Response, and Apple's Reply, as well as the evidence discussed in each of those papers. We are persuaded, by a preponderance of the evidence, that claim 1 is anticipated by Pettitt under 35 U.S.C. § 102(e), and claims 2, 4, 5, 7, and 9 are unpatentable over Pettitt and Beetcher under 35 U.S.C. § 103(a).

1. Pettitt

Pettitt discloses a system for "controlling distribution of software in a multitiered distribution chain" and "distinguishing authorized users from unauthorized users." Ex. 1006, col. 1, ll. 7-10. Figure 2 of Pettitt is reproduced below.

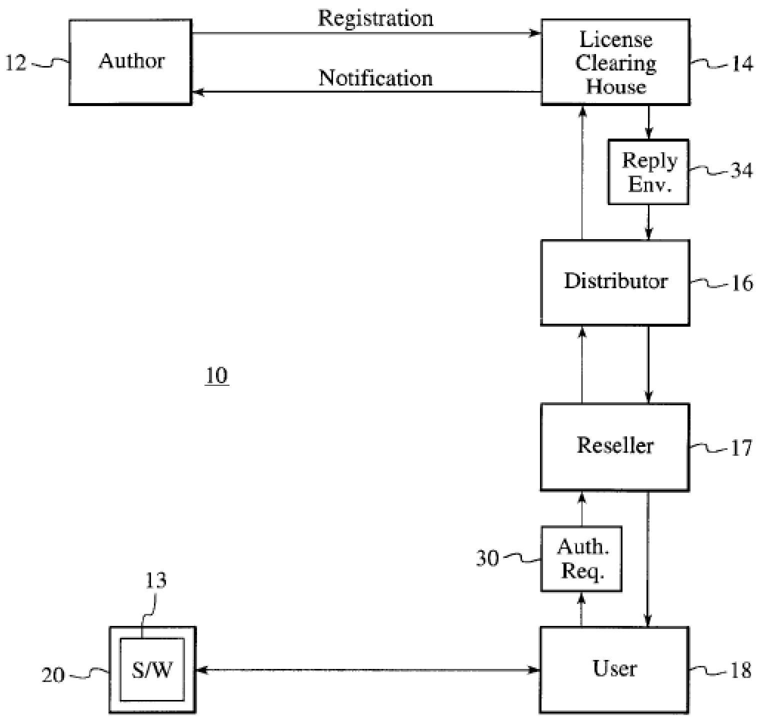


FIG. 2

Figure 2 depicts the entities involved in providing software 13: author 12, license clearing house (LCH) 14, distributor 16, reseller 17, and user 18. Software 13 is packed into a digital shipping container 20, encrypted with a master key, and provided to user 18 (e.g., sold by reseller 17 to the public). *Id*. at col. 3, ll. 28-56. To purchase a license and unlock the container, user 18 sends authorization request 30, which includes information identifying the software, user, and desired method of payment. *Id*. at col. 4, ll. 10-19. The distribution entities communicate with each other to validate the user's payment and authorize the transaction. *Id*. at col. 4, ll. 20-62. If authorized, LCH 14 creates a reply envelope 34 including:

1. information identifying the software,
2. information identifying the user,
3. the digital signature of the reseller,
4. the digital signature of the distributor,
5. a master key that unlocks the software container 20 (if the transaction has been authorized), and
6. a digital authorization certificate.

Id. at col. 4, l. 63-col. 5, l. 5.

LCH 14 encrypts the contents of the reply envelope with the reseller's public key and "digitally signs the envelope with the signature of LCH 14 by hashing the contents of the reply envelope and encrypting the result of the hash with the LCH's private key." *Id*. at col. 5, ll. 14-24. LCH 14 then sends the reply envelope back through the distribution chain. *Id*. at col. 5, ll. 24-28. Reseller 17 authenticates the digital signature, decrypts the reply envelope using the reseller's public key, and sends the contents of the reply envelope to user 18. *Id*. at col. 5, ll. 45-55. User 18 then "uses the authorization certificate and the master key to unlock the software container

20 and install the software." *Id*. at col. 5, ll. 56-63. Because the digital authorization certificate is derived from the user's information and, therefore, is different for each user, possession of the digital authorization certificate is "the user's proof of purchase, and proof that s/he is an authorized user." *Id*. at col. 5, ll. 58-63.

2. Claim 1 is Anticipated by Pettitt

Pettitt discloses receiving and decrypting an encrypted "launch code" (the reply envelope) with a "string, R" (the reseller's public key) to recover an "indicium of a first information product" (information identifying the software), and installing the first information product, as recited in claim 1. *See* Pet. 26-28. Achates does not argue these limitations of claim 1, but contends that Pettitt fails to disclose "decrypting said encrypted launch code . . . to recover a first candidate authentication code." PO Resp. 3-9. Achates argues that the LCH digital signature, cited by Apple in the Petition as a "first candidate authentication code," is not recovered by decrypting the reply envelope because (1) the LCH digital signature is not included within the reply envelope, (2) the LCH digital signature is available to the reseller before and independently of the decryption of the reply envelope, and (3) the reply envelope is encrypted before the LCH digital signature of the reply envelope is created. *Id*.

Apple responds that it identified two "first candidate authentication codes" in Pettitt in its Petition—the LCH digital signature and the digital authorization certificate—and Achates overlooks the latter. Pet. Reply 1-2. The primary structure identified by Apple in the Petition is the LCH digital signature, *see, e.g.*, Pet. 27, and we referenced the LCH digital signature in summarizing Apple's allegations in the Decision on Institution, Dec. on Inst. 28. Achates argued at the oral hearing that Apple improperly asserted that the digital authorization certificate was a "first candidate authentication code" for the first time in its Reply, and that the "ground" of unpatentability for this trial is based on the LCH digital signature alone. *See* Tr. 30:17-32:6.

We agree with Apple, however, that the Petition sufficiently identified each of the digital authorization certificate and the LCH digital signature as a "first candidate authentication code." Apple included, as part of the document identified as its Petition, a statement of material facts, two of which are:

> 80. The digital signature of the LCH described in Pettitt is an "authentication code" within Patent Owner's construction of the '403 claims. Ex. 1041 at ¶ 446.
>
> 81. The digital authorization certificate described in Pettitt is an "authentication code" within Patent Owner's construction of the '403 claims. Ex. 1041 at ¶ 447.

Pet., Attachment C ¶¶ 80-81; *see also* 37 C.F.R. § 42.24(a)(1) (statements of material facts, although not required, count against the page limit for the petition). Apple explains in the Petition that the reply envelope includes "information identifying the software, the user, the digital signature of the LCH and a digital authorization certificate," and that the reply envelope is decrypted and its contents passed to the user for unlocking the software product. Pet. 26-27. Apple further cites Mr. Schneier's testimony that the digital authorization certificate is an "authentication code" included in the reply envelope. *See* Pet. 26-27; Ex. 1041 ¶¶ 440-41, 447. The applicable ground of unpatentability in this *inter partes* review is the alleged anticipation of claim 1 by Pettitt, based on the allegations of unpatentability in the Petition. Dec. on Inst. 35-36. It is those allegations to which Achates responded in its Patent Owner Response. *See* 37 C.F.R. § 42.120(a) (a "patent owner may file a response to *the petition*" (emphasis added)). Indeed, Achates denied the two statements of material fact above when it filed its Preliminary Response. Paper 17 at 34. Thus, we consider Apple's assertion of the digital authorization certificate as a "first candidate authentication code."

We are persuaded that Pettitt's decryption of the reply envelope to recover the digital authorization certificate constitutes "decrypting said encrypted launch code . . . to recover a first candidate authentication code," as recited in claim 1. *See* Pet. 26-27; Ex. 1041 ¶ 447. As explained above, we interpret "authentication code" to mean "a code for authenticating data." *See supra* Section II.A. The digital authorization certificate is generated by hashing the other five items identified in Pettitt as being part of the reply envelope and encrypting the result with the private key of the LCH. Ex. 1006, col. 5, ll. 6-8. Therefore, the digital authorization certificate is a digital signature, and a function of a digital signature is to authenticate data, as Dr. Wang agrees. *See* Ex. 2034 at 254:15-21, 257:17-23. Pettitt specifies that the digital authorization certificate is "use[d]" to unlock the software container and install the software. Ex. 1006, col. 5, ll. 56-58. Specifically, the user would validate the digital authorization certificate by decrypting the originally encrypted hash (e.g., with the LCH's public key), generating a new hash from the same five elements used to create the original hash, and comparing the new and original hashes. *See* Pet. Reply 4; Ex. 2034 at 193:3-194:8, 263:10-15. Thus, the digital authorization certificate authenticates the data that has been "digitally signed" with it. Further, the digital authorization certificate is part of the encrypted reply envelope, and is recovered when the reply envelope is decrypted. Ex. 1006, col. 4, l. 63-col. 5, l. 8; col. 5, ll. 51-63 ("reseller 17 decrypts the reply envelope . . . and passes the contents onto the user 18"). Achates acknowledges in related Case IPR2013-00081 that the digital authorization certificate is part of the reply envelope and that the "reseller does *recover* the certificate by decrypting the encrypted reply envelope." IPR2013-00081, Paper 36 at 23.[6]

We are persuaded, by a preponderance of the evidence, that Pettitt discloses all of the limitations of claim 1, including "decrypting said encrypted launch code . . . to recover a first candidate authentication code."

3. Claims 2, 4, 5, 7, and 9 are Unpatentable Over Pettitt and Beetcher

We are persuaded by Apple's arguments and supporting evidence that claims 2, 4, 5, 7, and 9, which depend from claim 1, are unpatentable over Pettitt and Beetcher. *See* Pet. 29-33; Ex. 1041 ¶¶ 475-503. For example, claim 2 recites decrypting the encrypted launch code to recover an indicium of a "second information product" and installing that "second information product" based on an authentication code match. Beetcher teaches the distribution of "multiple software modules on a single generic medium" where each customer receives a "unique entitlement key, enabling the customer to run only those software modules to which he is licensed." Ex. 1007, col. 4, ll. 34-46; col. 6, ll. 20-40 (product entitlement flags 205, "each corresponding to a product number"). Apple persuasively shows that a person of ordinary skill in the art would have been able to modify the

[6] Because we agree with Apple that the digital authorization certificate in Pettitt is a "first candidate authentication code" recovered by the decryption of a launch code, as recited in claim 1, we need not determine whether the LCH digital signature also is a "first candidate authentication code."

Pettitt system to allow for distribution, at once, of multiple software products, as taught by Beetcher, and would have had reason to do so. Pet. 29-30. Mr. Schneier testifies that a person of ordinary skill in the art would have had reason to "include a list of multiple indicia of information products in the same launch code, as doing so would more efficiently identify multiple information products for which the end-user was licensed." Ex. 1041 ¶ 455.

Achates makes three arguments. First, as to all of the challenged dependent claims, Achates contends that Beetcher fails to cure the deficiency of Pettitt regarding recovery of a "first candidate authentication code," as recited in claim 1. PO Resp. 9-10. For the reasons explained above, we find no such deficiency in Pettitt.

Second, Achates asserts that a person of ordinary skill in the art would not have had reason to combine the teachings of Pettitt and Beetcher to arrive at the methods of claim 2, 4, 5, 7, and 9. *Id.* at 10. Achates cites Dr. Wang's declaration in support, but does not explain in its Patent Owner Response why it believes the references would not be combined. *See id.* (citing Ex. 2014 ¶¶ 63-68). We are persuaded by Mr. Schneier's analysis regarding the alleged combination. *See* Ex. 1041 ¶¶ 475-503.

Third, as to claim 4 in particular, Achates argues that a person of ordinary skill in the art would not have had reason to combine Pettitt and Beetcher. PO Resp. 10-12. Claim 4 recites, *inter alia*, "creating a token," "encrypting said token," and "storing said encrypted token on said computer." As explained above, we interpret "token" to mean "a data structure indicating that an end-user's computer is granted access to certain information products." *See supra* Section II.A. In the Petition, Apple contends that when the reseller in Pettitt decrypts the reply envelope, it recreates the unencrypted reply envelope and sends the contents of the reply envelope (a "token") to the user. Pet. 30-32. The contents of the unencrypted reply envelope (e.g., the master key and digital authorization certificate) are stored in the memory of the user's computer because they are used to unlock the software. *Id*. Apple further contends that although Pettitt does not teach encrypting the contents of the reply envelope in memory on the user's computer, doing so would have been obvious based on Beetcher to "help protect the contents of the token from theft," and also because Pettitt itself teaches encrypting the reply envelope at various stages for security. *Id*.; *see* Ex. 1041 ¶¶ 484-89 (citing Beetcher, Ex. 1007, col. 10, ll. 27-31, which teaches local storage of an encrypted entitlement key).

As to the combination of Pettitt and Beetcher, Achates contends that storing the encrypted software container and encrypted reply envelope on the user's computer would not make sense because the encrypted reply envelope is encrypted with the public key of the reseller, so only the reseller, not the user, can decrypt it. PO Resp. 10-11 (citing Ex. 2014 ¶¶ 69-70). Pettitt, however, does not teach that the user ever receives the encrypted reply envelope. *See* Pet. Reply 3-4. Rather, the reseller decrypts the reply envelope and sends the *contents* to the user in unencrypted form. Ex. 1006, col. 5, ll. 51-55. Thus, it is the *contents* of the reply envelope that are stored on the user's computer, and we agree that it would have been obvious based on Beetcher to encrypt those contents when they are stored there. Further, as Apple points out, claim 4 does not require that the encryption key used to create the token be the same as the encryption key used to create the launch code. *See* Pet. Reply 5. Thus, Achates's assertion that the reply envelope would have to be encrypted again with the public key of the reseller is incorrect. The contents of the reply envelope (the "token") could be encrypted with any encryption key (the "string, T").

Achates also asserts that because the reseller sends the master key (along with the other contents of the reply envelope) to the user, there is no reason for the user to back up the reply envelope locally once the user has used the master key to install the software. PO Resp. 11-12 (citing Ex. 2014 ¶ 71). In addition, according to Achates, there is no need to save the encrypted reply envelope because the user can back up the software itself. *Id*. at 12 (citing Ex. 2014 ¶ 72). Again, Achates misstates Apple's position, focusing on the encrypted reply envelope rather than the *contents* of the envelope that the user receives. In Pettitt, all of the contents are sent to the user, the master key and digital authorization certificate are used to unlock and install the software, and thereafter "the possession of the authorization certificate is the user's proof of purchase, and proof that s/he is an authorized user." Ex. 1006, col. 5, ll. 56-63. Thus, there are reasons for the user in Pettitt to store the token, including the digital authorization certificate, locally—namely, to install and unlock the software and provide proof of purchase. *See* Pet. Reply 4; Ex. 1041 ¶¶ 463, 489-90.

We also note that Achates does not dispute the underlying reasons provided by Mr. Schneier for why a person of ordinary skill in the art would have combined the teachings of Pettitt and Beetcher in the manner proposed. Mr. Schneier testifies that encrypting locally stored tokens was well known at the time and that a skilled artisan would have had reason to encrypt the token in Pettitt to ensure its security. Ex. 1041 ¶¶ 485-88. Dr. Wang agrees that it generally is a good practice to encrypt a file stored in nonvolatile storage to "protect the confidentiality of the file." Ex. 2035 at 395:3-15, 400:1-6. We give Mr. Schneier's analysis regarding the combination of Pettitt and Beetcher substantial weight, and conclude that Apple has shown "'some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.'" *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417-18 (2007) (citation omitted).

We are persuaded, by a preponderance of the evidence, that claims 2, 4, 5, 7, and 9 would have been obvious over Pettitt and Beetcher.

4. Conclusion

Based on the record evidence, in light of the arguments presented, Apple has shown, by a preponderance of the evidence, that claim 1 is anticipated by Pettitt, and claims 2, 4, 5, 7, and 9 are unpatentable over Pettitt and Beetcher.

F. Grounds Based on Beetcher

With respect to the alleged grounds of unpatentability based on Beetcher, we have reviewed Apple's Petition, Achates's Patent Owner Response, and Apple's Reply, as well as the evidence discussed in each of those papers. We are persuaded, by a preponderance of the evidence, that claims 17-19 are anticipated by Beetcher under 35 U.S.C. § 102(e), and claims 1-12 are unpatentable over Beetcher, Ginter, and Bohannon under 35 U.S.C. § 103(a).

1. Beetcher

Beetcher discloses a system for “restricting the ability of a computer user to use licensed software in a manner inconsistent with the license.” Ex. 1007, col. 1, ll. 9-12. Figure 1 of Beetcher is reproduced below.

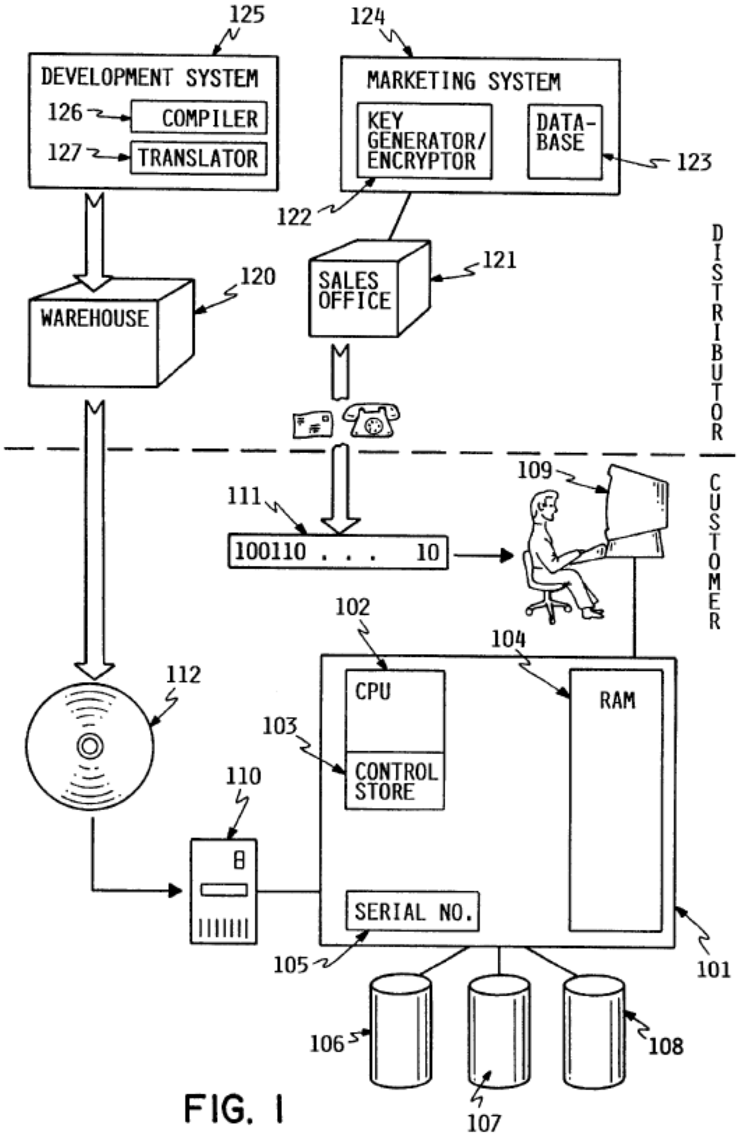


FIG. 1

Figure 1 depicts various distributor and customer devices. The customer’s computer has machine serial number 105. *Id.* at col. 5, ll. 17-23. A “generic set of software modules” stored on software media 112 is distributed to the customer separately from encrypted entitlement key 111, which “contains information enabling system 101 to determine which software modules are entitled to execute on it." *Id*. at col. 5, l. 65-col. 6, l. 7. The customer "load[s] the desired software modules from [software media 112 and] unit 110 into system 101, and store[s] the software modules on storage devices 106-108." *Id*. at col. 6, ll. 11-15. Entitlement key 111 includes certain information, such as software version field 202, machine serial number field 204, and product entitlement flags 205, "each corresponding to a product number" for a product that the customer may be authorized to use. *Id*. at col. 6, ll. 20-40; Fig. 2. Entitlement key 111 is encrypted using a machine key derived from machine serial number 105. *Id*. at col. 5, ll. 44-50; col. 9, ll. 55-60.

The customer receives encrypted entitlement key 111 and enters it into the computer. *Id*. at col. 9, ll. 51-52. The customer's computer then decodes encrypted entitlement key 111 using the machine key, stores the key in an encoded product key table, and stores the key and software version number in a product lock table. *Id*. at col. 6, l. 66-col. 7, l. 42. The encoded product key table and product lock table both are stored in random access memory (RAM), and the encoded product key table also is stored on a non-volatile storage device so that it can be recovered when the system is powered down and then re-initialized (i.e., the encoded product key table is persistent). *Id*. at col. 8, ll. 23-27, 43-46. Products are unlocked "on demand." *Id*. at col. 10, ll. 20-39. "Upon first execution of a previously unentitled software product," an unlock routine "fetches the encrypted entitlement key from the appropriate entry in [the] encoded product key table," "obtains the machine key," "decodes the entitlement key," and sets the product lock table accordingly if the entitlement key indicates that the user is entitled to use the software. *Id*. Upon subsequent executions of the software product, the system checks the product lock table to determine if the software is entitled to execute. *Id*. at col. 10, ll. 48-62.

2. Claims 17-19 are Anticipated by Beetcher

As to independent claim 17, Apple contends that Beetcher discloses reading an encrypted "token" (the product key table), decrypting the encrypted token to recover a token comprising an "indicium of a first information product" (an entitlement flag authorizing use of a specific software product), modifying the token to comprise an "indicium of a second information product" (an entitlement flag authorizing use of another software product), encrypting the token again to create a "newly encrypted token" (the modified product key table after a new entitlement key is received), and storing the new token. Pet. 18-21, 24 (citing Ex. 1041 ¶¶ 420-32). Achates argues that Beetcher fails to disclose the encrypting step of claim 17 because the product key table is not encrypted again after it is modified with a new entitlement key. PO Resp. 33-35. As support, Achates points to paragraph 427 of Mr. Schneier's declaration where he testifies that "[t]he storage of the product key table" satisfies the encrypting step. *Id*. at 34-35 (citing Ex. 1041 ¶ 427). Achates also cites Dr. Wang, who testifies that Beetcher only discloses storing, not encrypting, the product key table. *Id*. (citing Ex. 2014 ¶¶ 24-38).

We are persuaded that the encoded product key table is encrypted after it is updated with a new entitlement key. When a new entitlement key is received, it is treated as "a replacement key for all products it unlocks." Ex. 1007, col. 9, ll. 66-67. The system decodes that entitlement key (using the machine key) and “rebuild[s]” the encoded product key table accordingly. *Id*. at col. 9, l. 55-col. 10, l. 5. The rebuilt encoded product key table then is saved in storage. *Id*. at col. 10, ll. 18-19. As Apple and Mr. Schneier point out, Beetcher explicitly describes the product key table as “encoded,” meaning that the product key table itself is encrypted with a key. *See* Pet. Reply 11; Pet., Attachment C ¶ 71; Ex. 1041 ¶ 387, 420, 426. Importantly, Beetcher uses “decode” and “decrypt,” and “encode” and “encrypt,” each interchangeably to refer to the same thing. For instance, Beetcher describes “us[ing] the machine key to decode the entitlement key 111 at step 903,” but lists step 903 in Figure 9a as “Decrypt Entitlement Key.” *See* Ex. 1007, col. 9, ll. 59-60, Fig. 9a; *see also id*. at col. 4, ll. 10-12 (“decrypt the entitlement key”); col. 8, ll. 60-62 (“decodes and stores entitlement key 111”); col. 10, ll. 27-31 (“decodes the entitlement key”). Dr. Wang agreed that Beetcher uses “decode” and “decrypt” interchangeably. Ex. 2034 at 327:21-328:1. Also, Figure 4 of Beetcher depicts “encoded product key table” 450 and “product lock table” 460, with only the former described as “encoded.” This is understandable, given that the encoded product key table is persistent and would require a greater level of protection.

We are persuaded, by a preponderance of the evidence, that Beetcher discloses all of the limitations of claim 17, including “encrypting said token with said string, T, as the key to create a newly encrypted token,” as well as all of the limitations of dependent claims 18 and 19, which Achates does not argue separately in its Patent Owner Response.

3. Claims 1-12 are Unpatentable Over Beetcher, Ginter, and Bohannon

We are persuaded by Apple's arguments and supporting evidence that claims 1-12 are unpatentable over Beetcher, Ginter, and Bohannon. *See* Pet. 18-26; Ex. 1041 ¶¶ 308-419. As to claim 1, Apple contends that Beetcher discloses receiving and decrypting an encrypted "launch code" (the entitlement key) with a "string, R" (the machine key) to recover the software version number, machine serial number, and an "indicium of a first information product" (an entitlement flag). Pet. 18-19. Apple relies on Ginter for the "first candidate authentication code" limitation of claim 1, arguing that a person of ordinary skill in the art would have had reason to modify the Beetcher system to use a digital signature as taught by Ginter. *Id*. at 25. Apple relies on Bohannon for the "installing" limitation of claim 1, arguing that a person of ordinary skill in the art would have had reason to modify the Beetcher system to "require a user to input the entitlement key before copying the software onto the computer system" as taught by Bohannon. *Id*. at 26. In both cases, Apple cites the analysis of Mr. Schneier. *See* Ex. 1041 ¶¶ 331-37, 365-67.

Achates argues that claim 1 would not have been obvious based on the combination of Beetcher, Ginter, and Bohannon for four reasons. First, Achates argues that the references do not teach "decrypting said encrypted launch code . . . to recover a first candidate authentication code," as recited in claim 1, because Ginter's permissions record (PERC) does not include a digital signature that can be recovered by decrypting the PERC. PO Resp. 36-39. Ginter discloses receiving and decrypting a PERC, where one of the items included in the PERC may be a digital signature. *See* Pet. 9-10; Ex. 1041 ¶¶ 159, 162-66; Ex. 1005, col. 12, ll. 27-33. Figure 75D depicts user rights table (URT) 3160 as including a digital signature, and Ginter states that URT 3160 "may itself be a PERC 808." Ex. 1005, col. 248, ll. 36-38, Fig. 75D. Thus, Achates's factual assertion that the PERC in Ginter lacks a digital signature is not correct. *See* Tr. 47:24-48:5 (acknowledging the description of Figure 75D in Ginter). Mr. Radbel also acknowledged that the PERC could have a digital signature in the "particular construct" shown in Figure 75D. Ex. 2032 at 279:14-18.

Further, Achates's argument is directed to Ginter individually, but Apple's position regarding the recited "decrypting" step is premised on the combination of Beetcher and Ginter. Apple relies on Beetcher for the underlying teaching of decrypting an encrypted "launch code" (the entitlement key) to recover the software version number and machine serial number, and, because those two values are not authentication codes, relies on Ginter's teaching of a digital signature within an encrypted "launch code" (the PERC). *See* Pet. 25; Ex. 1041 ¶¶ 331-37. Given Ginter's teaching of a digital signature within a PERC, Achates does not explain sufficiently why the substitution proposed by Apple would not result in the recited "decrypting" step. *See In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986) ("Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references.").

Second, Achates argues that a person of ordinary skill in the art in 1997 would not have been motivated to include a digital signature in the entitlement key of Beetcher. PO Resp. 41-43. Achates contends that "public key cryptography was patented and the owner of the dominant patent was known to be litigious and the cost of its licenses high," citing a 1997 article regarding U.S. Patent No. 4,405,829. *Id*. (citing Ex. 2015). Achates also points to the following testimony from Mr. Schneier:

> Q. Does the fact that the digital signatures were all patents in the 1997 time frame create a motivation not to use digital signatures?
>
> A. Of course.

Ex. 1046 at 484:5-9.

We first note that Mr. Schneier later testified during redirect examination that he "may have made a mistake" regarding the testimony cited above because at least one digital signature algorithm of the time was in the public domain. *Id*. at 494:4-495:7. Moreover, even assuming that Achates is correct, Achates's argument is not that it would have been technically infeasible, or even technically difficult, for a person of ordinary skill in the art to use a digital signature in the context of Beetcher—just that the financial cost of doing so would have been high. We do not consider this to be a sufficient impediment to dissuade a skilled artisan from using digital signatures. Indeed, Mr. Schneier testifies that digital signatures were "widely used in April 1997" in systems analogous to that of Beetcher, and provides detailed reasons why a person of ordinary skill in the art would have wanted to use a digital signature. *See* Ex. 1041 ¶¶ 331-37. Achates gives no basis for believing that testimony to be incorrect.

Third, Achates argues that adding a digital signature to the entitlement key of Beetcher would frustrate Beetcher's objective to have a "user-friendly entitlement key." PO Resp. 43-45. Achates points to the following statements in Beetcher:

> Encrypted entitlement key 111 is sent from the software distributor to the customer by mail, *telephone*, or other appropriate means. While it is possible to transmit the key

> electronically or on magnetic media such as a diskette, *the key is sufficiently brief that an operator can enter it into system 101 by typing the key on console 109*.
>
> . . .
>
> Although key 111 is shown in FIG. 1 as a plurality of binary bits, it may be presented to the customer in some other form, such as hexadecimal digits or alphanumeric equivalents of groups of binary bits, in order to *simplify the task of entering the key from a keyboard*.

Ex. 1007, col. 5, ll. 59-64; col. 9, ll. 43-48 (emphasis added). Achates asserts that the entitlement key in Beetcher is 128 bits, which, when converted to American Standard Code for Information Interchange (ASCII) format, would be 16 characters for the user to hear and type, but if Ginter's digital signature were added, it would "at least double or triple" the size of the entitlement key and be too much to read over the telephone. PO Resp. 44-45; *see* Ex. 2014 ¶¶ 76-78 (Dr. Wang testifying that the entitlement key would "at least double or triple in size").

Achates's argument is not persuasive. Again, Achates makes no assertion that it would be technically infeasible or difficult to include a digital signature—just that it would be inconvenient for the user to have to enter more characters. Even assuming that Achates is correct that the entitlement key would "double or triple" in size if it had a digital signature (e.g., 32 or 48 characters instead of 16, based on Dr. Wang's statement), we do not consider this to be such a large difference that a skilled artisan would be dissuaded from using a digital signature, particularly given the advantages of using digital signatures cited by Mr. Schneier. During his deposition, Apple questioned Dr. Wang about the Windows XP installer software, which Dr. Wang acknowledged required the user to enter 42 characters. *See* Ex. 2035 at 387:8-388:10; Ex. 1055 at 6 ("The confirmation ID is a 42-digit integer containing the activation key and check digits that aid in error handling."). Windows XP was introduced in 2001, after the 1997 filing date of the '889 patent, as Apple acknowledged after filing its Reply.[7] *See* Mot. to Exclude 9-10 (citing Exs. 2041, 2042); Exclude Opp. 13-14. Nevertheless, given that the issue is one of practicality and not patentability, and given Windows XP's proximity in time to 1997 and undeniable commercial success, Windows XP is of at least some relevance in determining whether it would have been too burdensome on a user of the Beetcher system to enter more than 16 characters.

Achates's argument suffers from another flaw, however. Although Achates is correct that Beetcher expresses a desire to simplify the user's task of entering the entitlement key on a keyboard, Beetcher expressly contemplates other mechanisms of receiving and entering the entitlement key, including sending the entitlement key by "mail" (in which case the user simply could read the characters from the mailing and type them in to the keyboard) or transmitting it "electronically" (in which case the user may not even need to enter the entitlement key at all). *See* Ex. 1007, col. 5, ll. 59-64. Thus, we are not persuaded by Achates's argument that a person of ordinary skill in the art would have been dissuaded from using a digital signature in the entitlement key of Beetcher.

Fourth, Achates asserts that the object of the invention in Beetcher is to protect the software from unauthorized use, while at the same time allowing authorized users to freely copy and back up the software. PO Resp.

[7] Achates's Motion to Exclude the Windows XP evidence submitted by Apple is addressed below. *See infra* Section II.I.3.

39-41 (citing Ex. 1007, col. 3, ll. 58-61); *see* Ex. 2014 ¶¶ 79-80. According to Achates, this objective would be "completely defeated by combining Bohannon's prerequisite-to-installation technique" with Beetcher and Ginter. PO Resp. 40. We are persuaded, however, by Mr. Schneier's testimony that incorporating installation functionality, such as the "loader module" described in Bohannon, into the system of Beetcher, such that a user would input the entitlement key before copying the software onto the user's computer, would have been obvious. Mr. Schneier testifies that "the processes described in Beetcher will include operations such as placing the software in a permanent position from which it will be executed," and "[a] person of ordinary skill in the art, after obtaining and processing the entitlement key, would have had every reason to install the software, as the ultimate use of the software is the point of obtaining and processing the entitlement key in the first place." Ex. 1041 ¶¶ 56, 365-66. Thus, according to Mr. Schneier, incorporating the installation functionality of Bohannon into the system of Beetcher would be "the use of an old element to perform the same function it had been known to perform in the prior art without any new or unexpected result." *See id.* ¶ 367 (citing Ex. 1008, col. 3, ll. 24-37). The statements in Beetcher identified by Achates do not refute Mr. Schneier's reasons for combining the references. They only show that it was one goal of Beetcher to allow free distribution of the software (because the authorization check can be performed at run time). It is not necessary, however, that all of the objectives of a prior art reference be achieved for it to be properly combinable with another reference.

We are persuaded, by a preponderance of the evidence, that claim 1, as well as dependent claims 2-12, which Achates does not argue separately in its Patent Owner Response, would have been obvious over Beetcher, Ginter, and Bohannon.

4. Conclusion

Based on the record evidence, in light of the arguments presented, Apple has shown, by a preponderance of the evidence, that claims 17-19 are anticipated by Beetcher, and claims 1-12 are unpatentable over Beetcher, Ginter, and Bohannon.

G. Grounds Based on Ginter

With respect to the alleged grounds of unpatentability based on Ginter, we have reviewed Apple's Petition, Achates's Patent Owner Response, and Apple's Reply, as well as the evidence discussed in each of those papers. We are persuaded, by a preponderance of the evidence, that claims 17-19 are anticipated by Ginter under 35 U.S.C. § 102(e). We are not persuaded, by a preponderance of the evidence, that claims 1-7 and 9-12 are anticipated by Ginter under 35 U.S.C. § 102(e), or that claim 8 is unpatentable over Ginter and Beetcher under 35 U.S.C. § 103(a).

1. Ginter

Ginter discloses computer systems providing a "distributed virtual distribution environment (VDE)" that "help[s] to ensure that information is accessed and used only in authorized ways." Ex. 1005, Abstract. Electronic content is stored in "objects" (also called "containers") for distribution to users, and access to the content is regulated via a permissions record (PERC) associated with the content and provided to the user (separately or with the object). *Id*. at col. 13, l. 46-col. 14, l. 20; col. 58, l. 61-col. 59, l. 11; Fig. 5A; col. 147, ll. 33-59 ("no end user may use or access a VDE object unless a permissions record 808 has been delivered to the end user"). PERC 808 "specifies the rights associated with the object 300 such as, for example, who can open the container 302, who can use the object's contents, who can distribute the object, and what other control mechanisms must be active." *Id*. at col. 58, l. 67-col. 59, l. 5. "For example, permissions record 808 may specify a user's rights to use, distribute and/or administer the container 302 and its content." *Id*. at col. 59, ll. 5-7. For certain types of objects, the PERC is encrypted along with the object using a symmetric key and later decrypted on the user's machine. *Id*. at col. 199, ll. 1-6; col. 129, ll. 50-54; col. 133, ll. 50-53; col. 208, l. 65-col. 209, l. 20. Ginter discloses that the PERC can contain an "Object ID" that identifies the VDE object, as well as multiple "key blocks" that store decryption keys utilized to access content in "data blocks" within the object. *Id*. at col. 127, l. 45-col. 128, l. 2; col. 151, ll. 9-35; Fig. 26A. Ginter also discloses the use of a "validation tag" for "confirming the identity and correctness of received, VDE protected, information," and a "digital signature" to be verified against an expected digital signature. *Id*. at col. 12, ll. 27-33; col. 151, ll. 9-35; col. 215, ll. 7-63.

2. Claims 17-19 are Anticipated by Ginter

As to independent claim 17, Apple contends that Ginter discloses reading an encrypted "token" (the PERC), decrypting the encrypted token to recover a token comprising an "indicium of a first information product" (the Object ID or key block), modifying the token to comprise an "indicium of a second information product" (a modified Object ID or key block), encrypting the token again to create a "newly encrypted token," and storing the new token. Pet. 9-11, 16 (citing Ex. 1041 ¶¶ 294-302).

Achates argues that the PERC in Ginter does not comprise an "indicium" of a first information product, as recited in claim 17 (and claim 1). PO Resp. 21-26, 29 (citing Ex. 2013 ¶¶ 55-64). Apple's position is that the Object ID and key blocks in the PERC both satisfy the "indicium" limitations. Pet. 9-11, 16. As to the Object ID, Achates contends that (1) Object ID field 940 identifies the "totality" of elements in the VDE object container, not "just" information content 304, and (2) Object ID field 940 has the same datum regardless of whether the container's content is changed or deleted, which shows that Object ID field 940 is not an "indicium" of a particular information product. PO Resp. 22-24. As to the key blocks, Achates argues that (1) the VDE accesses the datum in the key block to use as a key to decrypt the corresponding data blocks, not "as a pointer to—or indicium of—the data block," and (2) Ginter permits two key blocks to have the same key, which shows that the key block is not an "indicium" of a particular information product. *Id*. at 24-26.

Achates's arguments are not persuasive, as they are based on the incorrect premise that an "indicium" of an information product can *only* identify content within a file and must uniquely identify *only one* information product. *See* Pet. Reply 8-9. There is no prohibition in claim 17 on the indicium indicating other things, and the indicium need not be a "pointer." *See* Ex. 2032 at 304:18-305:2 (Mr. Radbel stating that he does not "consider indicium to be a pointer"). The only requirement is that it be an "indicium," or "indication," of an information product. Mr. Radbel acknowledged that the Object ID in Ginter is used to find the correct content, Ex. 2031 at 45:12-17, and the key blocks are associated with and used to access the data in the correct data block, Ex. 1005 at 127:45-128:2. We are persuaded by Mr. Schneier's testimony that the key blocks and Object ID in Ginter each are an "indicium" of an information product, and that the PERC can be updated to add or modify the authorizations for information products as necessary. *See* Pet. 9-11, 16; Ex. 1041 ¶¶ 167-73, 182, 299; Ex. 1005, col. 161, ll. 52-57 ("This updating might, for example, comprise replacing an expired PERC 808 with a fresh one, modifying a PERC to provide additional (or lesser) rights, etc.").

Achates further argues that Object ID field 940 in Ginter is a single field that identifies the VDE object and, therefore, cannot be an indicium of a first information product and an indicium of a second information product. PO Resp. 29-32. Achates bases this conclusion on its reading of the claim, arguing that "[t]he fact that the encrypted token as it exists before it is modified comprises an indicium of [a] first information product and as it exists after it is modified comprises an indicium of a second information product mandates that the claim be construed to require *two distinct indicia*." *Id*. at 29 (emphasis added). We do not agree. Claim 17 requires decrypting the encrypted token to recover a token comprising an "indicium of a first information product" and modifying the *token* to comprise an "indicium of a second information product." The claim does not require that the particular content of the "indici[a]" be different from each other, or that the indicium of the first information product be retained after the token is modified. Further, even if Achates was correct as to the Object ID field, the argument does not account for the key blocks (the other asserted "indici[a]" of claim 17 according to Apple). We are persuaded by Mr. Schneier's testimony regarding the updating of the key blocks and Object ID in Ginter. *See* Pet. 16; Ex. 1041 ¶¶ 167-74, 297-300; Ex. 1005, col. 161, ll. 52-57.

Finally, Achates is incorrect in its assertion that Apple's analysis is based on "disjoint parts of Ginter without regard to their relationship." PO Resp. 13-14. Achates does not develop this argument with respect to the particular limitations of claims 17-19 or explain sufficiently why the particular portions of Ginter cited for the limitations of these claims relate to different embodiments, rather than the same preferred embodiment.

We are persuaded, by a preponderance of the evidence, that Ginter discloses all of the limitations of claim 17, and all of the limitations of dependent claims 18 and 19, which Achates does not argue separately in its Patent Owner Response.

3. Apple Has Not Shown Claims 1-7 and 9-12 to be Anticipated by Ginter

With respect to claim 1, Apple contends that Ginter discloses receiving and decrypting an encrypted "launch code" (the PERC) with a "string, R" (a decryption key) to recover a "first candidate authentication code" (digital signature or validation tag) and an "indicium of a first information product" (Object ID or key block), as recited in claim 1. Pet. 9-11. Apple further argues that Ginter discloses the "installing" step of claim 1 because "Ginter shows actions that occur if a PERC is found valid by matching of authentication codes in the PERC. These actions may include, *inter alia*, registration of the VDE object associated with the PERC or the storage of the VDE object in the object repository." *Id.* at 11 (citations omitted). With respect to the "when" clause of the "installing" step, Apple relies on the following testimony from Mr. Schneier:

> Ginter explains that the installation of the VDE object associated with the PERC is only accomplished after the validation information associated with the PERC, for example, validation tags, are "correlate[d] . . . to ensure that they are authentic and match." *See* ¶¶ 159-161, *supra*; Ex. 1005 at 112:44-47. Ginter also explains that, for example, . . . "digital signatures" must be "compared favorably," Ex. 1005 at 223:01-8. *See* ¶¶ 162-166, *supra*.

Ex. 1041 ¶ 196. As explained above, we interpret "installing" to mean "placing in a position so as to be ready for use." *See supra* Section II.A.

Achates argues that Ginter does not disclose "installing said first information product onto said computer *when said candidate authorization code matches a first known authorization code*," as recited in claim 1 (emphasis added), relying on the testimony of Mr. Radbel in support. PO Resp. 19-21 (citing Ex. 2013 ¶¶ 36-38, 51-53). Achates correctly points out that validation tag 948, shown in Figure 26A, is the only "validation tag" that Ginter teaches is inside the PERC. *Id*. at 19. According to Achates, "Ginter does not teach when validation tag 948 is verified or how it is verified, but most importantly, Ginter does not teach what the consequences are of the successful verification of validation tag 948 or a failure of verification." *Id*.

Having reviewed Apple's contentions regarding the "installing" step, we agree with Achates and are not persuaded, by a preponderance of the evidence, that Ginter discloses installing a first information product *when* there is a validation tag or digital signature match. As Achates points out, the portion of Ginter cited by Mr. Schneier regarding correlation of a validation tag pertains to the run time task of opening a "channel" that "provides event processing for a particular VDE object 300, a particular user, and a particular 'right' (i.e., type of event)." *See* Ex. 1005, col. 112, ll. 23-47, Fig. 15B; PO Resp. 20; Ex. 1041 ¶ 196. The "open channel" disclosure is not tied directly to validation tag 948, does not disclose expressly verifying validation tag 948 in the PERC, and does not disclose expressly registering or storing a VDE object when there is a match. We find Mr. Radbel's testimony persuasive on this point. *See* Ex. 2013 ¶¶ 51-53. Similarly, the portion of Ginter cited by Mr. Schneier regarding digital signatures pertains to a "firmware download process" to "load externally provided firmware and/or data elements into the PPE [Protected Processing Environment]." *See* Ex. 1005, col. 222, l. 40-col. 223, l. 8; PO Resp. 21; Ex. 1041 ¶ 196. Again, the cited portion does not disclose expressly verifying a digital signature in the PERC and registering or storing a VDE object when there is a match. The two cited portions appear to disclose verification of validation tags and digital signatures in general, and Apple does not explain sufficiently why they allegedly satisfy the required condition for "installing" in claim 1—namely, installing *when* there is a validation tag or digital signature match.

In its Reply, Apple cites general disclosures from Ginter regarding matching validation tags and the use of "[c]ontrol structures" to prevent tampering, and argues that Mr. Radbel "could identify nothing in Ginter suggesting that 'validation tag 948' was used differently than the other Ginter validation tags." Pet. Reply 8. It is not Achates's burden to show that validation tag 948 is *not* used like other validation tags in Ginter, however. Rather, it is Apple's burden to show that Ginter discloses, expressly or inherently, installing *when* there is a validation tag or digital signature match. That burden is not satisfied by citing unrelated portions of Ginter pertaining to the use of validation tags and digital signatures in general, or by assuming that validation tag 948 operates like other validation tags. Apple has not pointed to sufficiently specific disclosure in Ginter to demonstrate that the full "installing" step of claim 1 is performed.

Apple has not shown that Ginter discloses, expressly or inherently, "installing said first information product onto said computer when said candidate authorization code matches a first known authorization code," as recited in claim 1.[8] We are not persuaded, by a preponderance of the evidence, that claim 1, as well as dependent claims 2-7 and 9-12, are anticipated by Ginter.

4. Apple Has Not Shown Claim 8 to be Unpatentable Over Ginter and Beetcher

Apple asserts that claim 8 would have been obvious over Ginter and Beetcher. Pet. 16-17. For the reasons explained above, we agree with Achates that Ginter fails to teach the "installing" step of claim 1. Apple does not rely on Beetcher for this limitation in its analysis of the asserted combination of Ginter and Beetcher. *See id.* Accordingly, we are not persuaded that claim 8 would have been obvious over Ginter and Beetcher.

5. Conclusion

Based on the record evidence, in light of the arguments presented, Apple has shown, by a preponderance of the evidence, that claims 17-19 are anticipated by Ginter, but has not shown claims 1-7 and 9-12 to be

[8] Because we agree with Achates regarding the "installing" step, we need not reach Achates's other arguments regarding claim 1. *See* PO Resp. 15-18, 21-28.

anticipated by Ginter or shown claim 8 to be unpatentable over Ginter and Beetcher.

H. Apple's Motion for Observation on Email Communications and Achates's Motion to Seal

Apple's Motion for Observation on email communications between Mr. Radbel and Dr. Wang pertains to certain statements the witnesses made regarding the term "authentication code" used in the claims. *See* Obs. 1-3 (citing Exs. 1067, 1068). We note that Achates does not argue in its Patent Owner Response in this proceeding that the digital authorization certificate in Pettitt is not a "first candidate authentication code." To the extent the communications relate to other alleged "first candidate authentication codes" in the prior art (e.g., the validation tag in Ginter), we have considered Apple's observations and Achates's response. *See* Obs. 1-3; Obs. Resp. 1-4.

Achates also moves to seal the email communications (Exhibits 1067 and 1068), as well as Apple's Motion for Observation (Paper 74)[9] and Achates's response (Paper 79). Mot. to Seal 2-4. In previous Orders, we ordered Achates to produce the emails, authorized Apple to file them as exhibits in this proceeding, and authorized Achates to file a motion to seal. *See* Papers 44, 49, 66, 73.

There is a strong public policy in favor of making information filed in an *inter partes* review open to the public, especially because the proceeding determines the patentability of claims in an issued patent and, therefore, affects the rights of the public. Under 35 U.S.C. § 316(a)(1) and 37 C.F.R.

[9] Apple's exhibit list (Paper 75), filed with its Motion for Observation, also was filed under seal.

§ 42.14, the default rule is that all papers filed in an *inter partes* review are open and available for access by the public; a party, however, may file a motion to seal and the information at issue is sealed pending the outcome of the motion. It is, however, only "confidential information" that is protected from disclosure. 35 U.S.C. § 316(a)(7). In that regard, the Trial Practice Guide, 77 Fed. Reg. at 48,760, provides:

> The rules aim to strike a balance between the public's interest in maintaining a complete and understandable file history and the parties' interest in protecting truly sensitive information.
>
> . . .
>
> *Confidential Information*: The rules identify confidential information in a manner consistent with Federal Rule of Civil Procedure 26(c)(1)(G), which provides for protective orders for trade secret or other confidential research, development, or commercial information. § 42.54.

The standard for granting a motion to seal is "for good cause." 37 C.F.R. § 42.54(a). Achates, as movant, bears the burden of proof in showing entitlement to the requested relief. 37 C.F.R. § 42.20(c). Achates must explain why the information sought to be sealed constitutes "confidential information."

Achates has not met its burden to show that the emails, and the papers citing the emails, contain "confidential information." The emails contain discussions between Achates's two declarants, Mr. Radbel and Dr. Wang, regarding their opinions on the prior art at issue in this proceeding. *See* Exs. 1067, 1068. They do not appear to contain any trade secrets, research information, or information that would be commercially sensitive.

Achates makes three arguments in its Motion to Seal. First, Achates argues that the parties agreed not to permit discovery regarding the "process" of producing declarations and, therefore, had a "shared expectation that such information would be maintained confidentially and certainly not be made available to the public." Mot. to Seal 2-3. We addressed this issue in ruling on Apple's motion for additional discovery, and were not persuaded by Achates's argument regarding an alleged agreement between the parties. *See* Paper 66 at 8. For the same reasons, we are not persuaded that the emails should be sealed as "confidential information" based on the alleged agreement.

Second, Achates argues that the emails contain "confidential communications with and at the direction of counsel," and are "immune from discovery at least under the doctrine of work-product immunity." Mot. to Seal 3 & n.1. Similar to the argument it made in connection with Apple's motion for additional discovery, Achates does not cite any case law or explain in any detail *why* it believes the emails are privileged. *See* Paper 66 at 8. Moreover, Achates did not seek rehearing of our decision granting the motion for additional discovery, and produced the emails to Apple. We also note that, contrary to Achates's assertion that the emails are confidential communications "with" counsel, the emails at issue are "directly" between Mr. Radbel and Dr. Wang, in accordance with the limited additional discovery we authorized. *See id*. at 9; Exs. 1067, 1068.

Third, Achates contends that because Apple's observations are "rank speculation and offer no insights into the credibility" of Mr. Radbel and Dr. Wang, the Board should not review them in its analysis and "there is no need to make [the emails] available to the public." Mot. to Seal 3-4. Whether an opposing party's position regarding a document ultimately has merit, however, is not the test for determining whether the document should be sealed. The test is whether the material contains "confidential information," and Achates has not shown that the emails do.

As Achates provides no basis for deeming the emails to contain "confidential information," its Motion to Seal is denied. Papers 74, 75, and 79, and Exhibits 1067 and 1068, will be unsealed, and access to the materials in the Patent Review Processing System (PRPS) will be changed from "Parties and Board Only" to "Public."

I. Achates's Motion to Exclude

In its Motion to Exclude, Achates seeks to exclude (1) the declaration of Mr. Schneier (Exhibit 1041) submitted by Apple with the Petition, (2) part of the cross-examination deposition testimony of Achates's declarant, Dr. Wang (Exhibits 2034 and 2035), and (3) Exhibits 1055 and 1056 submitted by Apple. For the reasons discussed below, the motion is denied.

1. Schneier Declaration (Exhibit 1041)

With few exceptions, the Federal Rules of Evidence apply to *inter partes* review proceedings. 37 C.F.R. § 42.62(a). The rules governing *inter partes* review set forth the proper procedure for objecting to, and moving to exclude, evidence when appropriate. When a party objects to evidence that was submitted during a preliminary proceeding, such an objection must be served within ten business days of the institution of trial. 37 C.F.R. § 42.64(b)(1). The objection to the evidence must identify the grounds for the objection with sufficient particularity to allow correction in the form of supplemental evidence. *Id*. This process allows the party relying on the evidence to which an objection is served timely the opportunity to correct, by serving supplemental evidence within ten business days of the service of the objection. *See* 37 C.F.R. §§ 42.64(b)(1), 42.64(b)(2). If, upon receiving the supplemental evidence, the opposing party is still of the opinion that the evidence is inadmissible, the opposing party may file a motion to exclude such evidence. 37 C.F.R. § 42.64(c).

Achates alleges various reasons why Mr. Schneier's declaration (Exhibit 1041) should be excluded. Mot. to Exclude 1-8. The declaration, however, was submitted by Apple with its Petition for *inter partes* review (Paper 2). Because the evidence was submitted during a preliminary proceeding, any objection to such evidence must have been served within ten business days of the institution of the trial. 37 C.F.R. § 42.64(b)(1). Achates does not allege that Apple was served with any objection within ten business days of the institution of trial (Paper 22, dated June 3, 2013) or at any other time. Instead, Achates submits that 37 C.F.R. § 42.64 does not apply "because the bases of the objections arose when [Apple] failed to update Mr. Schneier's declaration as part of its Reply." Mot. to Exclude 7. Achates does not point to any rule or authority in support of the theory that Apple had a duty to "update" a declaration that was submitted with the Petition for *inter partes* review. Moreover, Apple would have had the right to serve supplemental evidence for the purpose of correcting any evidentiary deficiencies in the declaration, had Apple been provided with proper and timely notice, as required by 37 C.F.R. § 42.64. Thus, we are not persuaded that Mr. Schneier's declaration should be excluded.

2. Dr. Wang's Deposition Testimony (Exhibits 2034 and 2035)

Achates moves to exclude certain testimony of its own declarant, Dr. Wang, from his deposition that took place on November 19-20, 2013. Mot. to Exclude 8-9, 11-14. An objection to deposition evidence, however, must be made during the deposition. 37 C.F.R. § 42.64(a). Achates does not point to any objections to the lines of questioning or to the testimony in the transcript of the deposition. Moreover, Achates could have dealt with testimony it believed inadmissible with redirect examination of the witness, but did not do so. *See* 37 C.F.R. § 42.53(c)(2). Thus, we are not persuaded that Dr. Wang's deposition testimony should be excluded.

3. Exhibits 1055 and 1056

Achates moves to exclude two documents relating to the Windows XP operating system that were produced by Apple at the deposition of Dr. Wang. Exhibits 1055 and 1056 were introduced by Apple during Dr. Wang's deposition on November 20, 2013. Ex. 2035 at 374:20-375:11. According to Achates, it objected to the exhibits "within the time period allowed for objections to supplemental evidence." Mot. to Exclude 11 n.1. Achates refers to its Exhibits 2046 and 2047. *Id.* Exhibit 2046 appears to be a reproduction of an email communication from Achates's counsel to Apple's counsel on November 27, 2013 that refers to "enclose[d]" objections to evidence recently brought to Achates's attention by Apple. Exhibit 2047 is a paper styled "Patent Owner Objection to Evidence Pursuant to 37 C.F.R. § 42.64," dated November 27, 2013.

Apple responds that Achates waived any objections to Exhibits 1055 and 1056 because it did not object to them when they were introduced at the deposition, citing 37 C.F.R. §§ 42.53(f)(8) and 42.64(a). Exclude Opp. 10-11. However, 37 C.F.R. § 42.53(f)(8) does not apply because the rule refers to waiver of objection to the "content, form, or manner of taking the deposition," as opposed to documents introduced during the deposition. Pursuant to 37 C.F.R. § 42.53(f)(4), "[a]ll objections made at the time of the deposition to the qualifications of the officer taking the deposition, the manner of taking it, *the evidence presented*, the conduct of any party, and any other objection to the deposition shall be noted on the record by the officer" (emphasis added). We need not determine, however, whether exclusion of an exhibit introduced at a deposition (37 C.F.R. § 42.53(f)(3)) requires an objection during the deposition, or may be objected to within five business days, in accordance with 37 C.F.R. § 42.64(b)(1). First, Achates does not point to any objection directed to the exhibits in the deposition transcript. Second, even assuming that objection may be made after the deposition, in accordance with Achates's theory, Achates has not shown that the exhibits must be excluded.

Once a trial has been instituted, any objection must be served within five business days of service of evidence to which the objection is directed. 37 C.F.R. § 42.64(b)(1). The objection must "identify the grounds for the objection with sufficient particularity to allow correction in the form of supplemental evidence." *Id*.

Achates's Motion to Exclude sets forth two bases as to why Exhibits 1055 and 1056 should be excluded. First, Achates contends that the exhibits should be excluded as irrelevant because the documents are not prior art. Mot. to Exclude 11. As acknowledged by Achates, however, Apple does not rely on the documents as representing prior art. *See* Exclude Opp. 11;

Exclude Reply 4. The mere fact that the documents are not prior art does not merit their exclusion. *See, e.g.*, *In re Wilson*, 311 F.2d 266, 268-69 (CCPA 1962) (publication that was not cited as a prior art reference or as suggesting the claimed invention was cited properly to show a state of fact); *Ex parte Erlich*, 22 U.S.P.Q.2d 1463, 1465, 1992 WL 93132, at *3 (BPAI Jan. 16, 1992) (publication that was not prior art properly was relied upon as establishing the level of ordinary skill in the art at and around the time of the invention).

Achates's second basis for exclusion set forth in the Motion to Exclude is that Apple failed to authenticate the exhibits. Mot. to Exclude 11. Achates does not, however, point to where the objection (Exhibit 2047) identified that ground with sufficient particularity, which would have, thus, enabled a response by Apple to correct any such deficiency by serving supplemental evidence. As such, the allegation of failure to authenticate the exhibits is not timely and was not preserved by the objection served on Apple. *See* 37 C.F.R. §§ 42.64(b), 42.64(c).

III. ORDER

Apple has demonstrated, by a preponderance of the evidence, that:

(1) claim 1 is anticipated by Pettitt under 35 U.S.C. § 102(e);

(2) claims 2, 4, 5, 7, and 9 are unpatentable over Pettitt and Beetcher under 35 U.S.C. § 103(a);

(3) claims 17-19 are anticipated by Beetcher under 35 U.S.C. § 102(e);

(4) claims 1-12 are unpatentable over Beetcher, Ginter, and Bohannon under 35 U.S.C. § 103(a); and

(5) claims 17-19 are anticipated by Ginter under 35 U.S.C. § 102(e).

Apple has not demonstrated, by a preponderance of the evidence, that claims 1-7 and 9-12 are anticipated by Ginter under 35 U.S.C. § 102(e), or that claim 8 is unpatentable over Ginter and Beetcher under 35 U.S.C. § 103(a). Claims 13-16 of the ’403 patent are not subject to the instant *inter partes* review.

In consideration of the foregoing, it is hereby:

ORDERED that claims 1-12 and 17-19 of the ’403 patent have been shown to be unpatentable;

FURTHER ORDERED that Achates’s Motion to Exclude is *denied*;

FURTHER ORDERED that Achates’s Motion to Seal is *denied*;

FURTHER ORDERED that Papers 74, 75, and 79, and Exhibits 1067 and 1068, are unsealed; and

FURTHER ORDERED that the copies of Exhibits 1003 and 1041 filed on December 14, 2012, are expunged from the record of this proceeding.

This is a final 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:

Jeffrey P. Kushan
Joseph A. Micallef
SIDLEY AUSTIN LLP
jkushan@sidley.com
jmicallef@sidley.com

PATENT OWNER:

Brad D. Pedersen
Eric H. Chadwick
PATTERSON THUENTE PEDERSEN, P.A.
prps@ptslaw.com
chadwick@ptslaw.com

Jason Paul DeMont
KAPLAN BREYER SCHWARTZ & OTTESEN
jpdemont@kbsolaw.com

Vincent McGeary
GIBBONS, P.C.
vmcgeary@gibbonslaw.com