

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEEPER SECURITY, INC.,
Petitioner,

v.

CUMBERLAND SYSTEMS LLC,
Patent Owner.

Case CBM2017-00057
Patent 8,023,647 B2

Before JAMESON LEE, MICHAEL R. ZECHER, and
KEVIN W. CHERRY, *Administrative Patent Judges*.

CHERRY, *Administrative Patent Judge*.

DECISION

Denying Institution of Covered Business Method Patent Review
35 U.S.C. § 324(a) and 37 C.F.R. § 42.208

I. INTRODUCTION

Keeper Security, Inc. (“Petitioner”) filed a Petition (Paper 2, “Pet.”) seeking a covered business method patent review of claims 1–19 of U.S. Patent No. 8,023,647 B2 (Ex. 1001, “the ’647 patent” or the “challenged patent”) under section 18 of the Leahy-Smith America Invents Act, Pub. L. No. 112–29, 125 Stat. 284, 331 (2011) (“AIA”). Patent Owner, Cumberland Systems LLC, filed a Preliminary Response (Paper 9, “Prelim. Resp.”). Under 35 U.S.C. § 324(a),¹ a covered business method patent review may not be instituted “unless . . . the information presented in the petition . . . , if such information is not rebutted, would demonstrate that it is more likely than not that at least 1 of the claims challenged in the petition is unpatentable.” 35 U.S.C. § 324(a); see 37 C.F.R. § 42.208.

For reasons that follow, we determine that Petitioner has failed to show that the challenged patent qualifies as a covered business method patent. Accordingly, we deny the Petition and decline to institute a covered business method patent review of the challenged claims.

A. Related Matters

Petitioner and Patent Owner represent that the challenged patent is, and has been, at issue in a number of district court cases. See Pet. 3–4; Paper 8, 2–3.

¹ See 37 C.F.R. § 42.300(a).

B. The Challenged Patent

The '647 patent, titled “Password Self Encryption Method and System and Encryption by Keys Generated from Personal Secret Information,” describes a public key cryptographic system for passwords or other predefined personal secret information that defeats key factoring and spoofing attacks. Ex. 1001, [54], Abstract. The '647 patent states that “[a] password in clear text is vulnerable to interception and eavesdropping on the Internet, which may result in significant information and financial loss to its owner. Public key encryption algorithms that are in use today provide computationally unbreakable encryption to passwords. . . .” *Id.* at 1:28–32. The '647 patent explains that, “[t]hough [prior-art public key encryption] algorithms are perceived to be unbreakable with today’s possible computational speeds, there lies no guarantee that the same situation will continue in [the] future.” *Id.* at 1:33–36. The '647 patent purports to offer an improvement on these prior art encryption algorithms. *Id.* at 2:17–30. An embodiment of the cryptographic process of the '647 patent is shown in Figure 2, which is reproduced below.

Fig. 2

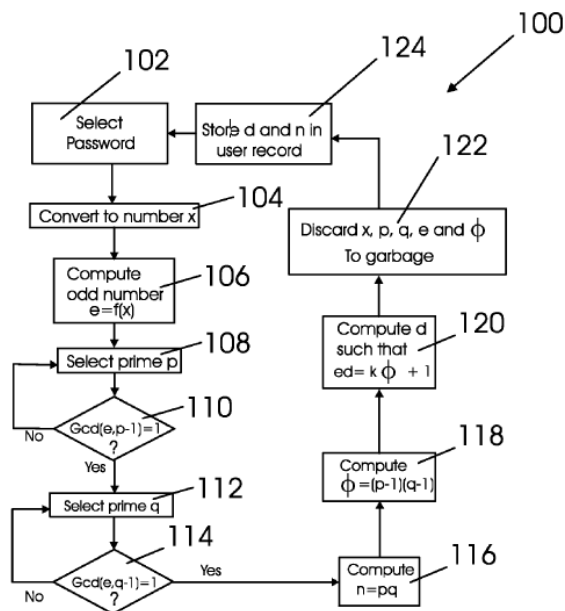


Figure 2 shows a block diagram of a cryptographic process in accordance with an embodiment described in the '647 patent. *Id.* at 3:45–46.

According to the '647 patent, the process shown in Figure 2 can be executed by a computer program running on a server computer that is connected via a communications link to a client computer. *Id.* at 3:57–66. The process of diagram 100, shown in Figure 2, begins at step 102, at which the server computer selects a defined password of a user from a web application's user table, which is located in database or flat file of the server computer. *Id.* at 3:66–4:3. At step 104, the server computer next converts the password into an integer number x . *Id.* at 4:3–4. The conversion of a password to a number may be done in various ways by the server computer. *Id.* at 4:4–6. “For example, the server computer 2 may use a conversion

scheme like 01 for a, 02 for b, . . . 26 for z, 27 for A, . . . 52 for Z, 53 for the number 1, 54 for number 2, . . . and so on.” *Id.* at 4:6–9.

At step 106, the server computer next computes an odd public key exponent $e=f(x)$ where $f(x)$ is any function of x that results in an odd integer for e . *Id.* at 4:22–24. At step 108, the server computer next selects a prime number p . *Id.* at 4:24–25. At step 110, it is determined if the greatest common divisor between e and $p-1$ is 1 to ensure that e and $p-1$ are relative primes. *Id.* at 4:25–27. If not, then a different prime number is selected for p , steps 108 and 110 are then repeated. *Id.* at 4:27–29. This continues until the greatest common divisor of e and $p-1$ is equal to 1. *Id.* at 4:29–30.

At step 112, the server computer selects a prime number q . *Id.* at 4:31–32. At step 114, it is determined if the greatest common divisor between e and $q-1$ is equal to 1. *Id.* at 4:32–33. If the answer is no, then another prime number q is selected and step 114 is repeated. *Id.* at 4:33–34. If the answer is yes, then the key modulus $n=pq$, i.e., p times q , is determined by the server computer. *Id.* at 4:35–36. At step 118, the server computer computes the Euler Totient Function $\phi=(p-1)(q-1)$. *Id.* at 4:36–38. At step 120, the server computer determines the private key exponent d such that $ed=k\phi+1$ using Euclid’s algorithm. *Id.* at 4:38–39.

At step 122, x , p , q , e and ϕ are discarded by the server computer, leaving no record thereof. *Id.* at 4:40–41. At step 124, d and n are stored in a user table record in database of server computer with a specific d and n for a specific password. *Id.* at 4:41–44.

Some uses of this encryption algorithm described in the specification include email (*id.* at 4:61–14), e-commerce transactions (*id.* at 6:25–31), and other web applications (*id.* at 8:18–20).

D. Illustrative Claim

Petitioner challenges all nineteen claims of the challenged patent. Claim 1 is the sole independent claim and is illustrative of the claimed subject matter:

1. A method comprising:

submitting a user identification for a user from a user computer to a server computer;

receiving a set of information at the user computer from the server computer, in response to the submission of the user identification for the user;

wherein the set of information includes a parameter of a key; and further comprising

using the user computer to convert user confidential information to a number x , wherein the number x is dependent on the user confidential information;

using the user computer to compute a number e which is a function of x and which is a function of the user confidential information;

using the user computer to pad the number x to convert x to X_p ;

using the user computer to encrypt x_p by using the parameter of the key and the number e to form a cipher C , wherein C is a function of the user confidential information; and

submitting the cipher C from the user computer to the
server computer.

Ex. 1001, 8:45–67.

II. DISCUSSION

The AIA defines a “covered business method patent” as “a patent that claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service” AIA § 18(d)(1); *see* 37 C.F.R.

§ 42.301(a). To determine whether a patent is eligible for a covered business method patent review, the focus is on the claims. *Secure Axxess, LLC v. PNC Bank N.A.*, 848 F.3d 1370, 1379 (Fed. Cir. 2017) (“It is the claims, in the traditional patent law sense, properly understood in light of the written description, that identifies a CBM [covered business method] patent.”). One claim directed to a covered business method is sufficient to render the patent eligible for CBM patent review. *See id.* at 1381.

With respect to the financial prong of covered business method patent eligibility, the U.S. Court of Appeals for the Federal Circuit has clarified that merely determining whether the claims involve activities “incidental to,” or “complementary to,” a financial activity is insufficient. *Unwired Planet, LLC v. Google Inc.*, 841 F.3d 1376, 1379–82 (Fed. Cir. 2016). Instead, “the statutory definition of a CBM patent requires that the patent have a claim that contains, however phrased, a financial activity element.” *Secure Axxess*, 848 F.3d at 1381.

Petitioner contends the challenged patent meets the financial product or service requirement because the patent claims “are directed to data processing that is used in the practice, administration, and management of financial products and services.” Pet. 10. Petitioner asserts that “the claims are directed to a method of encryption which can be implemented in web browsers such as Internet Explorer and Netscape Navigator to secure e-commerce transactions.” *Id.* (citing Ex. 1001, 8:18–20). Petitioner argues that “[t]he encryption techniques purport to improve upon existing password technology, ‘which may result in significant information and financial loss to its owner.’” *Id.* (quoting Ex. 1001, 1:28–30, 1:53–56). Petitioner further asserts “the specification explains that, allegedly, the claimed method ‘will keep web based authentication and online e-commerce transactions safe . . .’” *Id.* (quoting Ex. 1001, 6:25–29).

Patent Owner submits that Petitioner failed to show that the claims of the ’647 patent claim a financial product or service. Prelim. Resp. 9–12. Patent Owner asserts that, “[a]t best, Petitioner argues that the ’647 patent *could* be used in [the practice, administration, or management of a financial product or service, as required by 37 C.F.R. § 42.301].” *Id.* at 9. Patent Owner contends that is not enough under *Unwired Planet* and *Secure Axxess*. *Id.* at 9–10. Indeed, Patent Owner argues that the ’647 patent is “analogous to the disputed patent in *Secure Axxess*.” *Id.* at 11. Patent Owner asserts that, “[l]ike the *Secure Axxess* patent, the ’647 patent involves computer security and contains references in its written description about how its security features can benefit e-commerce . . . [but] these references

are made in an exemplary context, to show the benefits of the application's protection." *Id.* (citations omitted).

We agree with Patent Owner that Petitioner has failed to show adequately that the '647 patent "claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service," to qualify as a covered business method patent. As we explained above, *Secure Access* requires a challenged patent to "have a claim that contains . . . a financial activity element." *Secure Access*, 848 F.3d at 1381 (emphasis added). Petitioner fails to point to any element of claims of the '647 patent that it contends meets the "financial activity element" required by *Secure Access*. Instead, it merely points to statements in the specification regarding potential applications for the claimed cryptographic algorithm. At best, Petitioner argues that the claimed encryption method *can be* for financial matters, such as securing e-commerce transactions, but this is not sufficient after the Federal Circuit's guidance in both *Unwired Planet* and *Secure Access*. See *id.* Petitioner has simply failed to identify anything in the claims that are financial in nature.

Indeed, the claimed method of encryption of the '647 patent is most similar to the claimed method of authenticating a web page, which the Federal Circuit in *Secure Access* found was not qualified for CBM review. *Id.* at 1382. As the Federal Circuit explained, "just because an invention could be used by various institutions that include a financial institution, among others, does not mean a patent on the invention qualifies under the

proper definition of a CBM patent.” *Id.* This is the case here. The claimed encryption method has a variety of uses including web pages, email, and e-commerce transactions, and the specification does not limit the claimed invention’s application to financial uses. Thus, we agree with Patent Owner that Petitioner has failed to show that any ’647 patent claim is “directed to data processing that is used in the practice, administration, and management of financial products and services,” and has failed to show the challenged patent is eligible for a covered business method patent review.

III. CONCLUSION

We have reviewed the information in the Petition, as well as Patent Owner’s Preliminary Response. On this record, we have determined that Petitioner has failed to demonstrate that the ’647 patent is a covered business method patent. Thus, we deny the petition.

IV. ORDER

For the foregoing reasons, it is ORDERED that the Petition is *denied* and no covered business method patent review is instituted.

CBM2017-00057
Patent 8,023,647 B2

For PETITIONER:

Oliver D. Yang
Dean D. Niro
VITALE, VICKREY, NIRO & GASEY, LLP
oyang@vvnlaw.com
dniro@vvnlaw.com

For PATENT OWNER:

Bradley D. Liddle
bdliddle@gmail.com

Richard A. Baker
NEW ENGLAND INTELLECTUAL PROPERTY, LLC
rbaker@newenglandip.com