UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/016,022	08/30/2013	Francisco Corella	A24	1057

85547 7590 01/25/2019

Francisco Corella
Francisco Corella
5120 Marconi Avenue #26
Carmichael, CA 95608

EXAMINER
KING, JOHN B

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
01/25/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

francisco_corella@yahoo.com
fcorella@pomcor.com
fcorella@pomcor.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte FRANCISCO CORELLA and KAREN POMIAN LEWISON

Appeal 2018-000695
Application 14/016,022[1]
Technology Center 2400

Before ELENI MANTIS MERCADER, CARL L. SILVERMAN, and JASON M. REPKO, *Administrative Patent Judges*.

SILVERMAN, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1–5, 7–13 and 15–18. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

---

[1] The real party in interest is identified as Pomian & Corella, LLC. App. Br. 3.

STATEMENT OF THE CASE

The invention relates to protecting confidential data stored in a computing device. Abstract; Fig. 1. Claim 1 is exemplary of the subject matter on appeal (emphasis added):

> 1. A method of protecting confidential data stored in a computing device, comprising:
>
> storing the confidential data in encrypted form;
>
> regenerating a credential from a protocredential stored in the device and one or more secrets not stored in the device, the credential comprising a public key and a private key, the credential not being stored in the computing device prior to being regenerated;
>
> *requesting* an externally stored content-encryption key from a key storage service, the credential being used to authenticate the request cryptographically to the key storage service, *the cryptographically authenticated request comprising a signature* computed with the private key, *the cryptographically authenticated request being transmitted with confidentiality protection after the key storage service has authenticated to the computing device*, the key storage service using the public key to verify the signature, the key storage service using a consecutive failure counter to disable a record containing the externally stored content-encryption key after a configured number of consecutive authentication failures; and
>
> using the content-encryption key to decrypt the confidential data.

App. Br. 25 (Claims Appendix).

THE REJECTIONS

Claims 1, 2, 7, 8, 10, 15, and 18 are rejected under 35 U.S.C. § 103 as being unpatentable over Allen et al. (US 7,711,122 B2; iss. May 4, 2010) ("Allen "), Hird (US 7,328,350 B2; iss. Feb. 5, 2008) ("Hird"), and Misra et al. (US 5,757,920; iss. May 26, 1998) ("Misra"). Final Act. 9–19.

Claims 3 and 11 are rejected under 35 U.S.C. § 103 as being unpatentable over Allen, Hird, Misra, and Chaum (US 2010/0061553 A1;

Mar. 11, 2010) ("Chaum"). Final Act. 20–21.

Claims 4 and 12 are rejected under 35 U.S.C. §103 as being unpatentable over Allen, Hird, Misra, and Rajasekaran et al. (US 2002/0083327 A1; pub. June 27, 2002) ("Rajasekaran"). Final Act. 21–22.

Claims 5 and 13 are rejected under 35 U.S.C. § 103 as being unpatentable over Allen, Hird, Misra, and Prakash et al. (US 2010/0023782 A1; pub. Jan. 28, 2010) "Prakash". Final Act. 22–23.

Claims 9, 16 and 17 are rejected under 35 U.S.C. § 103 as being unpatentable over Allen, Hird, Misra, and Boubion et al. (US 2007/0223685 A1; Sept. 27, 2007) ("Boubion"). Final Act. 23–25.

ANALYSIS

Appellants argue the Examiner errs in finding the combination of Allan, Hird, and Misra teaches the claim 1 limitation, "*the cryptographically authenticated request being transmitted with confidentiality protection after the key storage service has authenticated to the computing device.*" App. Br. 21–22. In particular, Appellants argue that the Examiner errs in finding "Misra discloses the request being transmitted with confidentiality protection, the request being transmitted after the key storage service has authenticated to the computing device." App. Br. 21–22 (citing Misra 2:10–24). According to Appellants, the Examiner errs in finding Misra teaches "encrypting a digital signature with a session key before storing/transmitting the signature" because, although the cited Misra paragraph mentions a signature being encrypted with a session key, it "says nothing about 'transmitting the signature.'" *Id.* at 21. Appellants additionally argue the cited paragraph does not mention any request, let

alone a request being transmitted with confidentiality protection to a key storage service after the key storage service has authenticated to a computing device. *Id.* at 22. According to Appellants, the Examiner has constructed a "fanciful combination" of Allen and Misra and applied hindsight. *Id.*

Appellants additionally argue the concept of a signature encrypted under a session key is mentioned in the summary of the Misra patent, and hinted at in claim 1 of the Misra patent, but does not appear in the detailed description or the drawings. *Id.* Appellants then argue:

> A person skilled in the art trying to make sense of the Misra patent and confronted with this inconsistency between the summary and the detailed description that it purports to summarize would assume that the summary and the claims had been added to the detailed description by an attorney who had failed to understand the technical details of invention, and would not view the concept of a signature encrypted under a session key as a teaching of Misra worthy of consideration.

Id.

In the Answer, the Examiner notes that "All of the disclosures in a reference must be evaluated for what they fairly teach one of ordinary skill in the art." Ans. 4 (citing *In re Lemelson*, 397 F.2d 1006, 1009 (CCPA 1968)); *see also* Ans. 5 (citing additional court decisions). The Examiner points out that the claim does not require the signature or request to be encrypted as "[t]he claim merely requires that the request is transmitted with 'confidentiality protection' and that the request includes a signature." *Id.* The Examiner finds that the well-known concept of digital signatures using public and private keys with the signatures to process data is described by Allen. *Id.* at 4–5 (citing Allen 2:5–28, 5:13–32, 6:29–36). The Examiner

finds Allen teaches "transmitting a request to a key server where the request is signed with a private key to be verified at the key server" and, because "the request is signed with a digital signature and verified at the key server, it is considered as 'confidentiality protection' due to the fact that utilization of the keys in the opposite order as public-key encryption and public-key decryption provides confidentiality." *Id.* The Examiner alternatively finds Allen "teaches encrypting the request during transmission using the SSL or TLS protocols, which adds an additional layer of 'confidentiality protection' to protect the request/message from being intercepted during transmission to the key server." *Id.* at 5 (citing Allen 7:6–21). The Examiner finds, because the request is sent to the key server using the SSL or TLS connections, it is also sent after "the key storage service has authenticated to the computing device." *Id.* at 7. According to the Examiner:

> In the SSL and TLS connections a handshake protocol is used to authenticate the server (key server in Allen) to the user device and to also negotiate a shared secret that will be used to generate a shared symmetric encryption key. Therefore, in order for the invention of Allen to transmit the request to the key server in encrypted form using SSL or TLS, the key server must first have authenticated itself to the user device to generate the encryption key to perform the SSL or TLS encryption.

Id.

The Examiner additionally finds Misra teaches sending the digital signature in an encrypted and confidential form. *Id.* at 8 (citing Misra 2:10–24). Misra describes:

> A digital signature is attached to the encrypted credentials information at the home domain for the user. The digital signature is created using a private key for the home domain. A session key is

> received from the user and is used to encrypt the digital signature and the block of encrypted credentials information to produce a secure package. The secure package is provided to the user to enable the user to logon to the distributed system in a domain other than the home domain.

Id. at 8.

The Examiner concludes it would have been obvious to add the teachings of Misra to Allen for the purpose of encrypting the digital signature during transmission to prevent it from being intercepted by an attacker. *Id.*

In the Reply Brief, Appellants argue the Examiner errs in finding Allen provides confidentiality because "signing a message with a private key provides no confidentiality protection." Reply Br. 3–5. According to Appellants, Allen's request for the control key is not sent over as SSL or TLS connection and Allen does not teach "encrypting the request during transmission using the SSL or TLS protocols." *Id.* at 6. Appellants argue the Examiner's proposed combination is incorrect because neither Allen nor Misra describe a TLS or SSL connection and a session key generated during a TLS or SSL handshake. *Id.* at 7.

We note much of Appellants' argument is unsupported by factual evidence. Mere attorney arguments and conclusory statements that are unsupported by factual evidence are entitled to little probative value. *See In re Geisler*, 116 F.3d 1465, 1470 (Fed. Cir. 1997); *In re De Blauwe*, 736 F.2d 699, 705 (Fed. Cir. 1984); and *Ex parte Belinne*, 2009 WL 2477843, at *3–4 (BPAI Aug. 10, 2009) (informative).

As discussed below, we are not persuaded by Appellants' arguments and agree, instead, with the findings, claim interpretations, and conclusions of the Examiner.

Regarding the term "confidentiality protection," we agree that Allen and Misra each describe confidentiality protection as would be understood by one of ordinary skill in the art under a broad, but reasonable interpretation, and, we note the Specification does not provide a definition for this term. A claim in a patent application is given the broadest reasonable interpretation consistent with the specification, as understood by one of ordinary skill in the art. *In re Crish,* 393 F.3d 1253, 1256 (Fed. Cir. 2004). Great care should be taken to avoid reading limitations of the specification into the claims. *E-Pass Techs., Inc. v. 3Com Corp.,* 343 F.3d 1364, 1369 (Fed. Cir. 2003). Allen teaches requesting a content key from a key server wherein the request is signed using an access private key, the key server verifies the signature using the access public key, and the request includes confidentiality protection. Allen 2:5–28, 4:39–47. Allen also teaches using SSL or TLS secure connections to transmit confidential messages. Allen 7:6–21. Misra teaches encrypting a digital signature with a session key. Misra 2:10–24. In the combination of Allen and Misra, in a TLS or SSL connection, the session key is generated during the TLS handshake/authentication protocol, and the TLS handshake/authentication is performed and then afterwards the session key generated during the authentication is used to encrypt the digital signature for storage or, in the case of Allen, transmission as a request for a content key. Thus, we agree with the Examiner's conclusion that one of ordinary skill in the art would have improved upon the teachings of Allen by adding the teachings of Misra

for the purpose of encrypting the digital signature during transmission to prevent it from being intercepted.

Appellants argue the references individually while the rejection is based on the combination of the teachings of the cited references. *In re Keller*, 642 F.2d 413, 426 (CCPA 1981) ("[O]ne cannot show non-obviousness by attacking references individually where, as here, the rejections are based on combinations of references." (citations omitted)); *In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986).

Appellants also argue an unreasonably narrow teaching of the cited references and an overly demanding standard of obviousness.

> The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art.

Keller, 642 F.2d at 425.

Here, the Examiner provides sufficient evidence as required for obviousness. As stated by the Supreme Court, the Examiner's obviousness rejection must be based on:

> [S]ome articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. . . . [H]owever, the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.

KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 418 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

The Examiner's findings are reasonable because the skilled artisan would "be able to fit the teachings of multiple patents together like pieces of a puzzle" since the skilled artisan is "a person of ordinary creativity, not an automaton." *KSR*, 550 U.S. at 420–21.

Based upon the teachings of the references and the fact that each claimed element was well-known in the art, we agree with the Examiner because the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. *Id.* at 415–16. We note Appellants present no persuasive arguments that the results are unpredictable. Moreover, as discussed *supra*, the Examiner additionally provided reasons why one of ordinary skill in the art would combine each of the references in the manner suggested.

In view of the above, we sustain the rejection of claim 1, independent claims 2, 10, and 18 as these claims are argued together with claim 1, and dependent claims 3–5, 7–9, 11–13, and 15–17 as these claims are not argued separately. *See* 37 C.F.R. § 41.37(c)(1)(iv).

DECISION

We affirm the Examiner's decision rejecting claims 1–5, 7–13, and 15–18.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a) (1)(iv).

AFFIRMED