IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent No.: US 8625805 B1

Issue date: January 7, 2014

Patentee: WICKR, INC.

Title: DIGITAL SECURITY BUBBLE

SUBMISSION OF PRIOR ART UNDER 37 CFR 1.501

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

The undersigned herewith submits in the above-identified patent the following prior art (including copies thereof) which is pertinent and applicable to the patent and is believed to have a bearing on the patentability of at least claims 1, 2, 4, 6, 12 – 14, 17, 19 and 20 thereof:

B. Kaliski, PKCS #7: Cryptographic Message Syntax Version 1.5, March 1998. Internet Engineering Task Force Request for Comments (RFC) 2315. Available online at http://tools.ietf.org/html/rfc2315. (Hereinafter, RFC 2315.)

S. Kent, Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management, February 1993. Internet Engineering Task Force Request for Comments (RFC) 1422. Available online at http://tools.ietf.org/html/rfc1422. (Hereinafter, RFC 1422.)

As a preliminary remark, the patent uses the term "Digital Security Bubble" to refer to a data structure that "encapsulates or is otherwise provided around a message" and allows a variety of information to "securely travel with the message." The term is used by itself as the title of the patent, suggesting that the concept is considered by the inventors as a key innovation of the patent. However, the concept is well known in the art under the term "digital envelope," or "enveloped data," as can be seen in Section 10 of RFC 2315. (Although RFC 2315 does not discuss how enveloped data travels, hence does not specify that it travels "securely", it is standard best practice today to protect email messages as they travel, including enveloped data. For example, messages sent using the Simple Mail Transport Protocol (SMTP) are often protected by running the SMTP protocol over a Transport Layer Security (TLS) connection.)

Regarding claims 1, 17 and 20, RFC 2315 teaches the following limitations, which are found in all three claims:

"encrypt a message containing one or more components using a symmetric key" (Preamble of Section 10, item 4: "The content is encrypted with the content-encryption key."

RFC 2315 uses the term "content" to refer to a message exchanged between entities. See, for example, Section 7: "The general syntax for content exchanged between entities according to this document associates a content type with content." The content-encryption key is a symmetric key, since Section 6.2 mentions the symmetric encryption algorithm DES as an example of a content-encryption algorithm.)

"encrypt the symmetric key with a public key received in response to the request" (Preamble of Section 10, item 2: "For each recipient, the content-encryption key is encrypted with the recipient's public key".)

"encapsulate the encrypted message, the encrypted symmetric key, and the device identifier in a digital security bubble encapsulation" (Preamble of Section 10, item 3: "For each recipient, the encrypted content-encryption key and other recipient-specific information are collected into a RecipientInfo value, defined in Section 10.2"; and item 5: "The RecipientInfo values for all the recipients are collected together with the encrypted content into a EnvelopedData value, defined in Section 10.1." Thus, when there is only one recipient, the enveloped data, i.e. the digital security bubble of the patent, comprises the encrypted content, i.e. the encrypted message of the patent, the encrypted content-encryption key, i.e. the encrypted symmetric key of the patent, and other recipient-specific information. According to Section 10.2, the other recipient-specific information includes a data item "issuerAndSerialNumber" of type "IssuerAndSerialNumber." According to Sections 10.2 and 6.7, this data item identifies, and thus includes by reference, a certificate of the recipient entity, which includes its distinguished name and public key, the term "distinguished name" being used in the art to refer to an identifier of an entity that may be listed in a X.500 directory. The recipient entity is not necessarily a human user. It may be, for example, a computing device used as a mail server that hosts a mailing list and forwards the messages it receives to the members of the list. Thus, according to RFC 2315, the other recipient-specific information may include by reference a device identifier.)

"request a public key and a device identifier of at least one recipient from a first server" (To assemble the enveloped data, the originator of the message needs the certificate of the recipient. RFC 2315 does not specify in detail how the originator obtains the certificate, but

refers to RFC 1422 as follows: "This document can support a variety of architectures for certificate-based key management, such as the one proposed for Privacy-Enhanced Mail in RFC 1422." RFC 1422 specifies, in Section 2: "Prior to sending an encrypted message (using PEM), an originator must acquire a certificate for each recipient and must validate these certificates." And earlier in the same section: "Once signed, certificates can be stored in directory servers, transmitted via non-secure message exchanges, or distributed via any other means that make certificates easily accessible to message system users, without regard for the security of the transmission medium." This provides two methods by which the originator can obtain the recipient's certificate, which contains the recipient's public key and distinguished name, the distinguished name being a device identifier in the case where the recipient is a device such as a mailing list host. A first method is to request the certificate from a directory server. A second method is to request it from the mail server used by the recipient itself, in a non-secure message exchange. In both methods, if the recipient is a device, the originator requests a public key and a device identifier of the recipient from a server.)

"transmit the digital security bubble encapsulation to a second server" (Preamble of Section 10 of RFC 2315: "The enveloped-data content type consists of encrypted content of any type and encrypted content-encryption keys for one or more recipients." The enveloped data is therefore intended to be transmitted to at least one recipient, and it is customary in the art to use a mail server to receive such transmission.)

Regarding claim 2, RFC 2315, including the above-mentioned material from RFC 1422 referenced by RFC 2315, teaches the limitation "wherein the first and second server are the same". (Indeed, the above-mentioned second method of obtaining a recipient's certificate is to request it from the mail server of the recipient, which is the same server to which the enveloped data, i.e. the digital security bubble of the patent, is customarily transmitted.)

Regarding claim 4, RFC 2315 teaches the limitation "wherein at least one component included in the message is a message parameter." (The patent defines "message parameter" as a constituent part of a message. As explained above, RFC 2315 uses the term "content" to refer to

a message. The preamble of Section 10 asserts that the content can be of any type: "The enveloped-data content type consists of encrypted content of any type and encrypted content-encryption keys for one or more recipients." Hence the content can be composite, including constituent parts, and hence what the patent calls message parameters. RFC 2315 actually defines a variety of composite contents.)

Regarding claim 6, RFC 2315 teaches the limitation "wherein the processor is further configured to generate the symmetric key." (Preamble of Section 10: "A content-encryption key for a particular content-encryption algorithm is generated at random.")

Regarding claim 12, RFC 2315, with the above-mentioned reference to RFC 1422, claims the limitation "wherein the processor is configured to request a plurality of keys and a plurality of device identifiers associated with a plurality of recipients from the server," for the same reasons that it claims the limitation "request a public key and a device identifier of at least one recipient from a first server" of claim 1, since both RFC 2315 and RFC 1422 allow for multiple recipients.

Regarding claim 13, RFC 2315 claims the limitation "wherein the symmetric key is respectively encrypted with each of the received public keys, resulting in a plurality of encrypted symmetric keys." (Preamble of Section 10, item 2: "For each recipient, the content-encryption key is encrypted with the recipient's public key".)

Regarding claim 14, RFC 2315 claims the limitation "wherein each of the plurality of encrypted symmetric keys is included in a single digital security bubble encapsulation." (Preamble of Section 10, item 3: "For each recipient, the encrypted content-encryption key and other recipient-specific information are collected into a RecipientInfo value, defined in Section 10.2"; and item 5: "The RecipientInfo values for all the recipients are collected together with the encrypted content into a EnvelopedData value, defined in Section 10.1.")

Regarding claim 19, RFC 2315 teaches the limitation "generating the symmetric key." (Preamble of Section 10: "A content-encryption key for a particular content-encryption algorithm is generated at random.")

Respectfully submitted,

Date: April 18, 2014 _____

Francisco Corella
Pomian & Corella, LLC
111 N. Market Street
Suite 300
San Jose, CA 95113

CERTIFICATE OF SERVICE

I hereby certify on this eighteenth day of April 2014, that a true and correct copy of the foregoing "Submission of Prior Art" was mailed by first-class mail, postage paid, to:

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO CA 95014

Date: April 18, 2014

Francisco Corella
Pomian & Corella, LLC
111 N. Market Street
Suite 300
San Jose, CA 95113