



Attorneys at Law

Internet Law Update

December 2003

By Patrick T. O'Regan, Jr. and Cecily Anne Snyder*

VERISIGN AND RSA DO NOT INFRINGE METHOD FOR SECURING INTERNET COMMUNICATIONS

Plaintiff, Leon Stambler, filed an action against VeriSign and RSA for patent infringement of his patents, U.S. Patents 5,793,302 (" '302") and 5,974,148 (" '148") directed to methods for securing communications. At the close of evidence, Stambler moved for a judgment as a matter of law on the issue of inducement of infringement of claim 34 of the '302 patent. Thereafter, the jury found that Stambler had failed to prove that defendants, VeriSign and RSA, had induced infringement of method claim 34 of the '302 patent and claims 1, 16 and 35 of the '148 patent. The court entered a judgment in favor of Stambler on the issue of validity of claim 34 of the '302 patent and claim 27 of the '541 patent; however, in keeping with the jury verdict, the court entered a judgment in favor of VeriSign and RSA on the issue of infringement.

The plaintiff filed post-trial motions requesting judgment as a matter of law with respect to inducement of claim 34 of the '302 patent or for a new trial. The District Court of Delaware denied the motions. *Leon Stambler v. RSA Security and VeriSign, Inc.*, 2003 U.S. Dist. LEXIS 20998 (D. Del. 2003).

Inducement of Infringement

In this case, Stambler needed to show that Secure Sockets Layer version 3.0 ("SSL 3.0), which is the standard method for performing secure communication on the Internet and is used by defendants, infringed

* Patrick T. O'Regan, Jr., is a principal of O'Regan & O'Regan in Falmouth MA. He works with local Cape Cod businesses handling a wide variety of both litigation and transactional matters. He can be reached at patrick@oreganlaw.com. Cecily Anne Snyder is the Vice President of Legal Affairs at Imaging Therapeutics, Inc., Lexington MA. She handles a wide range of intellectual property matters, including developing market focused patent strategies. She can be reached at cecily@imatx.com. © 2003 Patrick T. O'Regan, Jr. and Cecily Anne Snyder.



Attorneys at Law

claim 34 of the patent. SSL 3.0 provides a mechanism for parties communicating over the Internet to identify each other.

SSL 3.0 follows several steps. First, a computer user connects to a website. At that time a number is randomly generated by the user's computer and sent to the website. In response, the website sends a second randomly generated number along with a digital certificate created by a certificate authority. The user's computer applies the certificate authority's public key, embedded in the user's browser, to decrypt the digital signature. The decrypted digital signature is then verified for authenticity. Once the authenticity is verified, the user sends the website a third randomly generated number which has been encrypted with the public key received from the website. The website receives the random number and generates a session key for the user. The website then sends the user a message which is encrypted using the message keys.

Claim 34 depends from claim 33 and therefore includes all the limitations of claim 33. Claim 33 provides: "A method for authenticating a first party by using information stored in a credential, the credential being previously issued to the first party by a second party, wherein information previously stored in the credential comprises at least a non-secret variable authentication number (VAN) and other non-secret credential information, the method comprising: previously generating a first error detection code (EDC1) by using at least a portion the other non-secret credential information; previously coding the first error detection code (EDC1) with first information associated with the second party to derive a variable authentication number (VAN); previously storing the VAN and the other non-secret credential information in the credential; retrieving the VAN and the other non-secret credential information stored in the credential; deriving a second error detection code (EDC2) by using at least a portion of the retrieved other non-secret credential information; retrieving second information associated with the second party previously stored in a storage means associated with at least one of the parties; uncoding the VAN using the second information associated with the second party to derive a third error detection code (EDC3); and



Attorneys at Law

authenticating the first party and at least a portion of the non-secret information stored in the credential if the second error detection code (EDC2) corresponds to the third error detection code (EDC3)." Claim 34 adds the additional limitation that "the first information associated with the second party comprises a public key, and the second information associated with the second party comprises a non-secret key."

In this case there are only three claim limitations in dispute. The terms are: credential, retrieving second information associated with the second party stored in a storage means associated with at least one of the parties, and authenticating the first party and at least a portion of the non-secret information stored in the credential if the second error detection code corresponds to the third error detection code.

The Delaware District Court construed "credential" to mean "a document or information obtained from a trusted source that is transferred or presented to establish the identity of a party." Stambler argues that the digital certificate used by SSL 3.0 is a credential within the meaning of claim 34. The defendants argue that the digital certificate is not a credential because the certificate does not authenticate the identity of the sender. Rather, the certificate establishes the authenticity of the certificate. Where a term, in this case "to establish," is not defined in the patent or in the court's claim construction, the trier of fact applies an ordinary definition. (See *Hewlett-Packard Co. v. Mustek Systems, Inc.*, 340 F.3d 1314, 1321 (Fed. Cir. 2003)). The court then relied on the dictionary definition of "establish" and concluded that "a reasonable jury could have concluded that the digital certificate is not a credential within the meaning of claim 34, because they could reasonably conclude that the identity of the website is not established in the SSL 3.0 at the time the credential is presented or transferred." [*15]

Next, the court defined "storage means" as a "place for storing information, which can be a computer file." The issue revolves around whether the file on the user's computer where the public key is stored is a storage means associated with the certificate authority. The court again



Attorneys at Law

concluded that the jury could have concluded that for a storage means to be associated with one of the parties there must be a connection between one of the parties and the storage means which is more than the presence of a public key, as presented by defendants.

Finally, the court construed the limitation "authenticating the first party and at least a portion of the non-secret information stored in the credential if the second error detection code (EDC2) corresponds to the third error detection code (EDC3)" to mean "verifying the identity of the first party and at least a portion of the non-secret information stored in the credential if EDC2 and EDC3 correspond." The defendants had argued that this limitation was not met in SSL 3.0 and the jury heard substantial evidence that authentication occurs when the finished message is sent by the website using the session keys. Therefore, the court concluded that a reasonable jury could have concluded that correspondence between EDC2 and EDC3 does not authenticate the identity of the website.

Request for New Trial

Plaintiff requested a new trial on two bases: first, the weight of the evidence favors plaintiff; second, defense counsel's improper influence of the jury.

The court dispatches plaintiff's first basis in view of its lengthy discussion that a reasonable jury could have found that defendants did not infringe the contested claim limitations.

With respect to the misconduct of defendants' attorneys, the court notes that "a motion for a new trial on the basis of attorney misconduct may only be granted if the movant demonstrates that such 'conduct constitutes misconduct, and not merely aggressive advocacy, and that the misconduct is prejudicial in the sense of affecting a substantial right in the context of the entire trial record.'" (Citing *Lucent Techs, Inc. v. Newbridge Networks Corp.*, 168 F.Supp.2d 181 260-261 (D. Del. 2000)). The plaintiff bases its misconduct argument on the fact that defendants' counsel raised issues of patent validity, violating an order of the court, and



Attorneys at Law

misstatements of law and claim construction provided by the court. The court concluded that there "was not prejudice to the plaintiff of the quality and quantity that would demand a jury's verdict to be set aside."