IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

LEON STAMBLER,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Civil Action No. 01-065-SLR
	)	
RSA SECURITY, INC.,	)	
VERISIGN, INC.,	)	
OMNISKY CORPORATION,	)	
	)	
Defendants.	)	

MEMORANDUM ORDER

At Wilmington this 29th day of January, 2003, having heard oral argument and having reviewed papers submitted in connection therewith;

IT IS ORDERED that the disputed claim language in United States Patent Nos. 5,793,302; 5,936,541 and 5,974,148 as identified by the above referenced parties, shall be construed as follows, consistent with the tenets of claim construction set forth by the United States Court of Appeals for the Federal Circuit:

A. "Variable Authentication Number (VAN)"

Defendants argue that the VAN must be limited to a number created by applying a symmetric key algorithm. Neither the claims, specification, nor prosecution history impose such a limitation. While nearly all of the embodiments apply symmetric key algorithms to create the VAN, the patent does contemplate creating the VAN using asymmetric algorithms. ('148 patent, col. 5, ll. 34-44) In addition, the patent provides examples of VAN's created using asymmetric algorithms, such as the RVAN. ('148 patent, col. 7, ll. 33-38) Thus, "variable authentication number (VAN)" shall be construed to mean "a variable number that can be used in verifying the identity of a party or the integrity of information or both."

B. "Secret Key of the First Party"

The court shall apply the ordinary definition of the word "secret" - "kept from the knowledge of any but the initiated or privileged."[1] The disputed phrase contemplates the initiated being the first party. Thus, the term "secret key of the first party" shall be construed to mean "a key that is known only to the first party and those intended to know it and that exists beyond the duration of a particular transaction."

---

[1]The Random House College Dictionary, 1189 (revised ed. 1980)

C. "Instrument" or "Payment Instrument"

The claims in the '148 patent state that an instrument is "for transferring funds." ('148 patent, col. 24, ll. 43-44; col. 28, ll. 37-38) Similarly, a payment instrument is "to make a payment." ('148 patent, col. 26, ll. 12-13) Accordingly, the term "instrument" or "payment instrument" shall be construed to mean "a document used to transfer funds to a recipient party."

D. "Secret Key of the Payor"

The court shall apply the ordinary definition of the word "secret" - "kept from the knowledge of any but the initiated or privileged."[2] The phrase contemplates the initiated being the payor. Thus, the term "secret key of the payor" shall be construed to mean "a key that is known only to the payor and those intended to know it and that exists beyond the duration of a particular transaction."

E. "Creating an Error Detection Code (EDC1) by Coding"

The patent defines error detection coding as coding "in such a manner as to permit detection of changes." ('148 patent, col. 5, ll. 41-43) Thus, the term "creating an error detection code (EDC1) by coding" shall be construed to mean "creating an error detection code (EDC1) by applying an algorithm to information in

---

[2]The Random House College Dictionary, 1189 (revised ed. 1980)

such a manner as to permit detection of changes but without complete recovery of the original information."

F. "Secret Key of the Originator"

The court shall apply the ordinary definition of the word "secret" - "kept from the knowledge of any but the initiated or privileged."[3] The phrase contemplates the initiated being the originator. Thus, the term "secret key of the originator" shall be construed to mean "a key that is known only to the originator and those intended to know it and that exists beyond the duration of a particular transaction."

G. "Coding"

Both parties request unsupportable constructions of this term. Plaintiff's construction is exceedingly broad. Defendants' construction imports limitations not found in the claims. The patent specification does not define the term "code," however, the specification does state that a "coder . . . may be any form of such device utilizing a known algorithm[.]" ('148 patent, col. 3, ll. 37-39) Thus, the term "coding" shall be construed to mean "transforming information by applying a known algorithm."

---

[3]The Random House College Dictionary, 1189 (revised ed. 1980)

H. "Wherein a Credential is Previously Issued"

The court shall apply the ordinary definition this term. Thus, the term "previously issued" shall be construed to mean "existing or occurring prior to something else in time or order."[4] The preamble of claim 20 (from which claim 27 depends) of the '541 patent states that "a credential is previously issued to at least one of the parties." Thus, the credential must be issued prior to the steps of the claim.[5] The term "wherein a credential is previously issued" shall be construed to mean "the credential referenced in the claim must already be issued before the execution of the steps recited in the claim."

I. "Credential"

Defendants attempt to import limitations from examples in the specification. Defendants' construction would require a physical credential and thus, the physical presence of the parties. The specification, however, recites that "until the present invention, it has not been possible to verify the

---

[4]The American Heritage Dictionary 982, (2d ed. 1982).

[5]Plaintiff argues that the credential cannot be issued before step one of claim 20 because step one creates the VAN which is included on the credential. Step one of the claim does not state, however, that this is the first time the VAN is created. The patent specifically discusses re-creating the VAN to compare with the VAN from the credential to authenticate the credential. ('541 patent, col. 13, ll. 24-28) This is consistent with the claim language describing a method for securing information.

identity and to secure the interests of . . . absent parties to a transaction." ('148 patent, col. 2, ll. 2-5) Importing defendants' limitation would be improper. Thus, the term "credential" shall be construed to mean "a document or information obtained from a trusted source that is transferred or presented to establish the identity of a party."

J. "Secret Key of the Credential Issuing Entity"

The court shall apply the ordinary definition of the word "secret" - "kept from the knowledge of any but the initiated or privileged."[6] The phrase contemplates the initiated being the credential issuing entity. Thus, the term "secret key of the credential issuing entity" shall be construed to mean "a key that is known only to the credential issuing entity and those intended to know it and that exists beyond the duration of a particular transaction."

K. "Authenticating At Least One of the Parties by Using the VAN"

These terms shall be construed with their ordinary meaning; no further construction is necessary.

---

[6]The Random House College Dictionary, 1189 (revised ed. 1980).

L. "Information Associated with the At Least Two Parties"

These terms shall be construed with their ordinary meaning; no further construction is necessary.

M. "The First Party Has a First Personal Identification Number (PIN1)"

This term was defined by the patentee in both the specification and the prosecution history. Accordingly, the term "the first party has a first personal identification number (PIN1)" shall be construed to mean "at the time the method steps are executed, the first party has a number for identification that is secret, is selected by the first party at the time of enrollment, cannot exist in uncoded form, and cannot be recovered from other information anywhere in the system." ('148 patent, col. 2, ll. 31-36; D.I. 293 at 383)

N. "First Storage Means" and "Second Storage Means"

The claims do not support defendants' limitation that the storage means may only be computer files. Plaintiff's construction, however, would appear to eliminate the first/second limitation. The court finds that the term "first storage means" and "second storage means" shall be construed to mean "a first place for storing information, which can include a computer file," and "a second place for storing information, which can be a computer file."

O. "Being Accessible Only to a Party With Knowledge of the First PIN1"

These terms shall be construed with their ordinary meaning; no further construction is necessary.

P. "Information Associated with the First Party"

These terms shall be construed with their ordinary meaning; no further construction is necessary.

Q. "Information Associated with the Second Party"

These terms shall be construed with their ordinary meaning; no further construction is necessary.

R. "Storing in Escrow and in Trust"

"In Escrow" is defined as "in the keeping of a third person for delivery to a given party upon the fulfillment of some condition."[7] The definition is inherently temporary. Thus, the term "storing in escrow and in trust" shall be further construed to mean "temporarily storing information securely."

S. "Subsequently Granting the First Party Access to the First Storage Means by Using the PIN1 or the Credential"

Claim 12 of the '302 patent recites steps for "a method of enrollment and issuing a credential to a first party by a second party, and subsequently granting access to a first storage

---

[7]The Random House College Dictionary, 450 (revised ed. 1980).

means[.]" ('302 patent, col. 26, ll. 10-12) The final claim element recites "subsequently granting the first party access to the first storage means by using the PIN1 or the credential." ('302 patent, col. 26, ll. 10-29) Defendants argue that the grant of access must occur subsequent to the issuance of the credential. The court agrees. If the first party is to obtain access to the first storage means using the credential, the credential must have been previously issued. Plaintiff does not explain how access could be granted using the credential if the credential has not yet been issued.

Thus, the term "subsequently granting the first party access to the first storage means by using the PIN1 or the credential" shall be construed to mean "the step of subsequently granting the first party access to the first storage means by using the PIN1 or the credential must occur after the previous steps of the method have been performed, including the step of issuing the credential to the first party."

T. "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)"

Defendants' construction adds limitations not supported by the claims. The term "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)" shall be construed to mean "verifying the identity of the first party and the integrity of at least a portion of the non-secret information if EDC2 and EDC3 correspond."

United States District Judge