

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

LEON STAMBLER,)	
)	
Plaintiff,)	
)	
v.)	Civil Action No. 01-65 SLR
)	
RSA SECURITY INC. ,)	
VERISIGN INC.,)	
FIRST DATA CORPORATION, and)	
OMNISKY CORPORATION,)	
)	

**PLAINTIFF'S OPENING BRIEF ON
ISSUES OF CLAIM CONSTRUCTION**

MORRIS, NICHOLS, ARSHT & TUNNELL
Douglas E. Whitney (#461)
Maryellen Noreika (#3208)
John D. Pirnot (#3767)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899-1347
(302) 658-9200

Attorneys for Plaintiff Leon Stambler

OF COUNSEL:
David S. Shrager, Esquire
Shrager Spivey & Sachs
Two Commerce Square, 32nd Floor
2001 Market Street
Philadelphia, PA 19103

October 15, 2002

TABLE OF CONTENTS

	<u>Page</u>
TABLE OF CITATIONS	iv
I. INTRODUCTION AND NATURE AND STAGE OF THE PROCEEDING	1
II. SUMMARY OF ARGUMENT	2
III. THE TECHNOLOGY	2
A. The Problem: Conducting Electronic Transactions Securely Over An Open Communication Channel.	2
B. The Requirements Of Electronic Transaction Security.	4
C. The Challenge: Designing Workable Security Protocols.	9
D. The Stambler Inventions: Methods For Securing The Interests Of All Parties To A Transaction.	11
IV. THE CORRECT LEGAL CONSTRUCTION OF DISPUTED CLAIM TERMS.	14
A. Law Of Claim Construction.	14
B. “Coding” Has Its Ordinary And Accustomed Meaning.	15
C. “Credential” Has Its Ordinary And Accustomed Meaning.	19
D. “Secret Key” Has Its Ordinary And Accustomed Meaning.	20
E. “PIN” Has Its Ordinary And Accustomed Meaning.	21
F. The Phrase “Variable Authentication Number” Has The Ordinary And Accustomed Meaning Given By Each Of Its Constituent Words.	22
G. “Using The VAN” Has Its Ordinary And Accustomed Meaning.	22
H. Information “Associated With” A Party Has Its	

TABLE OF CONTENTS (continued)

	<u>Page</u>
Ordinary And Accustomed Meaning.	23
I. “Instrument” Or “Payment Instrument” Has Its Ordinary And Accustomed Meaning.	23
J. “Storage Means” Has Its Ordinary And Accustomed Meaning.	23
K. “Storing In Escrow and In Trust” Has Its Ordinary And Accustomed Meaning.	24
L. “Previously Issued” Is Used In Its Ordinary And Accustomed Sense To Mean Issued “Prior To The Transaction.”	24
M. “Subsequently Granting” Describes A Step That Is Part Of A Method Of Enrolling And Issuing A Credential.	25
V. DEFENDANTS’ ARTIFICIALLY LIMITED CLAIM CONSTRUCTIONS ARE CONTRARY TO LAW.	25
A. Defendant’s Standard For Claim Construction.	25
B. “Coding” Is Not Limited Only To Coding By “Applying A Reversible, Symmetric Encryption Algorithm.”	27
C. “Credential” Is Not Limited Only To “Physical” Credentials That “Can Only Be Authenticated By The Issuing Entity.”	31
D. The “Secret Key” Of A Party Is Not Limited Only To Secret Keys Known Only To The Party, Or To Keys Associated With The Party Beyond The Duration Of A Particular Transaction.	33
E. “PIN” Is Not Limited Only To A PIN “Selected By” A Party, “Known Only To” That Party, Which “Cannot Exist In Uncoded Form,” Or Which “Cannot Be Recoverd From Other Information.”	34
F. “Variable Authentication Number” Is Not Limited Only To An Authentication Number “Created By Applying A Symmetric-Key Algorithm To At Least	

TABLE OF CONTENTS (continued)

	<u>Page</u>
Some Information In Such A Way That That Information Can Be Recovered.”	34
G. “Using A VAN” To Authenticate A Party Is Not Limited Only To “Verifying That Party’s Ability To Regenerate The Key That Was Used To Originally Generate The VAN.”	36
H. Information “Associated With” A Party Is Not Limited Only To Information “Tied To The Identity” Of The Party “Beyond The Duration Of A Particular Transaction.”	36
I. “Instrument” And “Payment Instrument” Are Not Limited Only To “Documents.”	37
J. “Storage Means” Is Not Limited Only To Discrete Computer “Files.”	37
K. “Storing In Escrow and In Trust” Is Not Limited Only To Storing “Until The Credential Is Issued.”	38
L. A “Previously Issued” Credential Cannot Mean A Credential Issued Before A Claim Step Needed For Creation Of The Credential Has Been Performed.	38
M. The Step Of “Subsequently Granting” Cannot Occur After The Entire Claimed Method Has Been Carried Out.	39
VI. CONCLUSION	39

TABLE OF CITATIONS

Page(s)

Cases

<i>Beckson Marine, Inc. v. NFM, Inc.</i> , 292 F.3d 718 (Fed. Cir. 2002)	14
<i>Electro Med. Sys., S.A. v. Cooper Life Sci., Inc.</i> , 34 F.3d 1048 (Fed. Cir. 1994)	15
<i>Johnson Worldwide Assocs., Inc. v. Zebco Corp.</i> , 175 F.3d 985 (Fed. Cir. 1999)	14
<i>K-2 Corp. v. Soloman S.A.</i> , 191 F.3d 1356 (Fed. Cir. 1999)	14
<i>Laitram Corp. v. NEC Corp.</i> , 163 F.3d 1342 (Fed. Cir. 1998)	15
<i>Renishaw PLC v. Marposs Soc. Per Azioni</i> , 158 F.3d 1243 (Fed. Cir. 1998)	15
<i>Teleflex, Inc. v. Ficosa N. Am. Corp.</i> , 299 F.3d 1313, 1327 (Fed. Cir. 2002)	14
<i>Wesley Jessen Corp. v. Bausch & Lomb, Inc.</i> , 209 F. Supp. 2d. 348 (D. Del. 2002)	15
<i>York Prods., Inc. v. Central Tractor Farm & Family Cent.</i> , 99 F.3d 1568 (Fed. Cir. 1996)	14

I. INTRODUCTION AND NATURE AND STAGE OF THE PROCEEDING

In this contentious case, the parties cannot agree on the meaning of “ordinary ... meaning,” the pivotal aspect of claim construction. As a result, this Court must now address numerous claim terms formed by plain and simple words found in general and technical dictionaries. But defendants say that the “ordinary meaning” is not found in any dictionary or common usage (by themselves or their experts in different, but revealing, contexts) (*see pp. 25-26, infra*), but only after the Stambler patents and file histories are studied by their claim construction “experts” and vetted in a room of defense counsel during the crafting of their “expert” reports.

The Court will be told by the defendants that it and most other courts in *Markman* rulings have been approaching the task of claim construction from the wrong direction. The Court may be surprised to hear that it is wrong to start with the words of the claim and their ordinary meanings, but instead the Court must first read all of the intrinsic evidence and only then determine the meaning of a limitation. By this approach, simple words like “coding,” “authentication,” “number,” and “credential” can be found to have been severely qualified to mean (*see pp. 27-39, infra*):

coding: “applying a reversible, symmetric encryption algorithm”

authentication: “verifying identity only by an issuing authority”

number: “a quantity created only by reversible, symmetric encryption”

credential: “a physical item that vouches for the holder’s identity and that
can only be authenticated by the issuing entity”

Apparently, the ordinary meaning of even the simplest words, “a,” “the,” and “or,” cannot be determined without first reading the entire intrinsic evidence (*pp. 26-27, infra*).

Indeed, one claim construction “expert” for the defense (who presumably had studied the intrinsic evidence himself) refused to answer questions asking for the ordinary meaning of words in a claim some 15 times (A77.1-79.2, 82, 90, 91.1, 98.1-98.2, 103-106.1).

The good news is that this case presents numerous blatant instances of improper claim construction, and thus the opportunity to make abundantly clear that it is still wrong to read extraneous limitations into the words of a claim, even under the pretense of “searching for the ordinary meaning.”

II. SUMMARY OF ARGUMENT

The asserted claims are composed of ordinary words to describe terms recognized in the field of computer science. No specialized definitions are given in the patents or other intrinsic evidence, and no express disavowal of the ordinary meanings of these terms can be found. The disputed claim terms are used in the patents consistently with their ordinary and accustomed meanings.

Nevertheless, according to the defendants, no fewer than thirteen claim terms of the patents-in-suit have highly specialized meanings, or in some cases no meanings. Defendants’ proposed constructions would read into the plain words of the claims unstated and unintended limitations of defendants’ choosing from specific embodiments described in the patents.

III. THE TECHNOLOGY

A. The Problem: Conducting Electronic Transactions Securely Over An Open Communication Channel.

The Stambler patents involve *transaction security*, that is, systems that allow parties to carry out transactions without unintended disclosure or compromise of

the transaction information. In particular, the patents claim a number of methods for securing information exchanged electronically between remote parties carrying out their transactions on computers. The patents share a common specification that describes many applications that require transaction security in computer systems, including electronic banking and commerce, electronic payment of bills, and electronic identification for remote access to computer resources. Three of the patents are asserted in this case, namely, U.S. Patent Nos. 5,793,302 (“the ‘302 patent”), 5,936,541 (“the ‘541 patent”), and 5,974,148 (“the ‘148 patent”).

In a typical computer transaction, information about the transaction is sent from an originating or requesting party (“originator”) to a receiving or responding party (“recipient”). A transaction may involve other parties as well, such as a person or organization that authorizes the transaction, or a beneficiary of the transaction. By way of example, an electronic banking transaction might involve a bank customer wanting to transfer an amount of funds from one account to another, perhaps even to the account of some other person. Depending upon how the transaction system is designed, the customer might first send a message to the bank requesting a transaction. Upon confirmation of the customer’s identity, the bank may respond with its own message that it is prepared to receive the transaction data. The customer would then send a message containing instructions for carrying out the transaction. Finally, the bank may respond with an acknowledgement that the transaction was carried out as instructed.¹

¹ In the context of electronic transactions, a “party” may not only be a person who sits at a computer entering information, but may also be a program operating within the computer itself. Thus, in the electronic banking example above, if the customer’s transaction instructions are received and processed by an automated
(continued . . .)

The ability to conduct transactions electronically by computer has already revolutionized commerce on a worldwide scale, a phenomenon nowhere more apparent than in the explosive growth of the Internet. With the added speed and convenience made possible by electronic transactions, however, come security concerns not present in face-to-face transactions. In an electronic transaction, for example, it is considerably more difficult for one party to ensure that a remote party is who they say they are, or that a received message has precisely the same content that the other party originally sent. A degree of security may be obtained by restricting access to transaction systems to a known group of authorized users, or by conducting the transactions over closed communication channels. Thus, in the example of an electronic banking system, security might be enhanced somewhat by ensuring that only registered banking customers were able to send messages, or that messages were sent over private, dedicated transmission lines. Over open communications channels, however, like those that carry messages over the Internet, any message that is sent may be intercepted, read, and possibly altered before it is received.

B. The Requirements Of Electronic Transaction Security.

As viewed today, the security of electronic communications requires three essential factors: (1) *Privacy*, which ensures that the content of a communication is known only by the intended parties, (2) *Integrity*, which ensures that the content of a

(. . . continued)

program running on the bank's computer, rather than an actual person, the bank is nonetheless deemed a "party" to the transaction.

communication has not been altered after it was sent, and (3) *Authentication*, which allows the parties to know with whom they are communicating (Finkel Decl. ¶¶ 4, 5).²

1. Coding Messages For Privacy.

The privacy of a message sent over an open communication channel can be protected by transforming the message to a form that is unrecognizable except to those intended to know its content. The science of using codes to transform information to preserve its privacy is known as *cryptography*.

Encryption is the process of converting information, typically referred to as “plaintext” or “cleartext,” into a form that cannot be understood by looking at the encrypted message. *Decryption* is the process of converting encrypted information back to its original form so that it can be understood. A method for encrypting or decrypting information is called a *cipher*. Thus, an encrypted message is sometimes referred to as “ciphertext.” As an elementary example, a message could be coded by substituting for each letter of the message the next letter of the alphabet; in that example, the plaintext “this message is secret” would result in the ciphertext “uijt nftbhf jt tfdsfu.” In the context of computer communications, where all information is represented as strings of binary numbers, ciphers are typically mathematical functions or “algorithms” that transform one number into another (see Finkel Decl. ¶ 7).

² Refers to Declaration of David Finkel, Ph.D., filed contemporaneously herewith. As Professor Finkel notes in ¶ 5, some refer to a fourth attribute of information security known as “non-repudiation,” which ensures that a party cannot deny having sent a particular message. Non-repudiation can also be viewed as the result of combining features of message integrity and authentication.

A cryptographic system (or “cryptosystem”) consists of an encryption cipher and a decryption cipher, which may or may not be the same algorithm. Encryption and decryption ciphers typically make use of variables called *keys*, which are numerical inputs to the algorithm. Ciphers are designed so that it is easy for someone who knows the decryption key to turn ciphertext back into plaintext, but virtually impossible to decrypt ciphertext without knowing the key. A typical cipher key is an extremely large number (hundreds or even thousands of digits long), so that an adversary cannot break the code merely by guessing the key, or by trying all possible keys in any feasible time using even the fastest computers. Thus, by restricting knowledge of keys of a cryptographic system, parties can keep their communications private even if the ciphertext messages are intercepted by an eavesdropper (*see* Finkel Decl. ¶ 8).

Cryptosystems may be classified as either “symmetric” or “asymmetric.” Symmetric cryptosystems utilize the same key for both encryption and decryption. Parties using a symmetric cryptosystem must agree on a key beforehand, and must keep it secret from others if the communication is to be secure. One of the best known symmetric encryption algorithms is the Data Encryption Standard (DES), which was originally developed in the 1970s and is widely used in various derivative forms today. In asymmetric cryptosystems, different keys are used for encryption and decryption. Asymmetric cryptography works with key pairs, such that data encrypted with one key of a pair may only be decrypted with the other key of the pair. In asymmetric cryptosystems, one of the keys can be made available to the public (the “public” or “non-secret” key), while the other key is kept secret by one party (the “private” or “secret” key). An example of a so-called “public-key” asymmetric cryptosystem is the widely

used “RSA” algorithm, also introduced in the 1970s. While symmetric and asymmetric algorithms differ mathematically, they are both used for the same purpose: to encrypt and decrypt information (*see* Finkel Decl. ¶¶ 9, 10).³

2. Coding Messages To Detect Errors Or Alterations.

Ensuring the integrity of an electronic message is in some respects more challenging than for other types of messages. If a portion of a paper document is altered, physical evidence of the alteration may typically be found. Banking institutions have become adept, for example, at detecting alterations made to checks. By comparison, information in an electronic document may be changed, added, or deleted at will, while leaving no sign that an alteration ever occurred. Thus, in a non-secure electronic banking transaction, there would be nothing to prevent an eavesdropper from altering a customer’s funds transfer instructions to change the amount of the transfer, or even the destination of the transfer to the eavesdropper’s own account, with the bank being none the wiser.

One way of testing the integrity of an electronic message is to employ *error detection coding*, where the originator of a message creates a number or symbol that corresponds in some unique way to the message. An early type of error detection code used for computer messages was the “checksum,” which was the mathematical combination of all the binary numbers (“ones and zeros”) that represent the information.

³ Prior to the 1970s, the science of cryptography in this country was essentially the sole province of the U.S. Government, classified at the highest levels by the National Security Agency. Even today, with a variety of cryptosystems in widespread public use, cryptographic algorithms developed and used by the NSA remain a closely guarded secret (*see, e.g.*, A114-15).

A more sophisticated type of error detection code can be constructed using a cryptographic algorithm known as a *hash* function. A hash function transforms a message of an arbitrary length and encodes it into a fixed-length number called the hash value, from which it is virtually impossible to recreate the original message. As the name implies, the hash is a “scrambled” version of the message. Error detection codes formed using hash functions are sometimes referred to as “message digests,” “message integrity checks,” or “message authentication codes” (*see* Finkel Decl. ¶¶ 11, 12).

Because hash functions cannot be applied in reverse to recreate the original information from a hash value, hash functions are often referred to as *irreversible* algorithms. An example of using an irreversible cryptographic algorithm for message integrity is the Data Authentication Algorithm described in 1985, which applies the DES algorithm (*see* p. 6, *supra*) irreversibly to successive blocks of a message.

3. Establishing The Identity Of The Parties.

Ensuring the identity of parties in electronic transactions also presents a greater challenge than in face-to-face transactions. With no face or voice to associate with a transaction, it is a relatively easy matter for someone to originate a computer message under the guise of another person’s identity.

One way for parties to authenticate themselves in an electronic transaction is by proving knowledge of a secret. For example, a bank customer might identify himself or herself in an electronic banking transaction by furnishing a secret user name and password that the bank associates with that customer. For this to work, however, the customer must first have established his or her identity with the bank, usually in person, and agreed upon the password or other secret to be used for identification in future

transactions. Although this approach is feasible for small organizations with closed networks, a password management system quickly becomes impracticable in any network environment with a substantial number of public users.

When parties to a transaction are not previously known to each other, identification may be accomplished through the use of *credentials*. For example, a bank might require someone who is not a known customer of the bank to present a driver's license or some other credential before redeeming a check; if the credential appears to be issued by a valid authority, and if the information on the credential corresponds to the person who presents it, the bank may accept the credential as proof of that person's identity. In the world of computer communications, electronic versions of credentials have been devised known as *digital certificates*. A digital certificate is an electronic document that is created by some recognized authority, and that contains identifying information about a person or organization. As it is commonly described in the field of information security, a digital certificate is "the electronic equivalent to a passport or business license" (A415).⁴

C. The Challenge: Designing Workable Security Protocols.

While cryptographic algorithms have been devised having potential application to problems of privacy, integrity, and authentication, the algorithms themselves are of little use in isolation. For example, there is no point in establishing a communication channel that is completely private if the identities of the communicating

⁴ "A_____" refers to Appendix To Plaintiff's Opening Brief On Issues Of Claim Construction, filed contemporaneously herewith.

parties cannot be authenticated. Similarly, using cryptography for message privacy is not enough to ensure message integrity. Real end-to-end security in electronic communications requires using cryptographic algorithms as components, in combination with other procedures and techniques, to define a workable system that accomplishes the more complicated task of ensuring overall message security.

A *protocol* is a series of steps, involving two or more parties, designed to accomplish a task. Cryptographic algorithms all have strengths and weaknesses, and well-designed protocols take advantage of the strengths and account for the weaknesses. For example, a skilled designer of cryptographic systems will structure a protocol so as to use faster algorithms where they can be used safely, while at the same time avoiding an algorithm's exposure to known cryptographic attacks.

Examples abound of the difficulties in designing a computer security protocol that can withstand security attacks. "Pretty Good Privacy" (PGP) was an encryption system developed in the early 1990s for sending secure e-mail based upon both symmetric and asymmetric cryptographic techniques. PGP was one of the first cryptographic protocols ever to be made available to the general public, and its designer was hailed as a pioneer in the field. A serious flaw was subsequently discovered in the PGP protocol, however, that allows an attacker to determine the contents of an encrypted message without having an appropriate decryption key (A392-403).

Comparable weaknesses have been revealed in other prior art protocols once considered secure. For example, the "X9.9" standard for Financial Institution Message Authentication was approved in 1986 for transactions between members of the wholesale banking industry. X9.9 was based upon irreversible cryptographic techniques

for message authentication, using shared keys furnished by a central key distribution manager. The X9.9 message authentication code was ultimately determined to be insecure, and has been formally withdrawn (A274-297). Similarly, the Microsoft “MS-CHAP” protocol, also based upon hashing algorithms, was thought to provide a reliable means of authentication for computer communications. Yet, despite Microsoft’s considerable resources, and the importance of MS-CHAP to its software business, the MS-CHAP protocol has been shown to be vulnerable to a relatively straightforward cryptographic attack (A404-13).

As for the Internet, security simply had not been addressed by the early 1990s. In those emerging days of the Internet, the focus was upon designing the basic protocols that would be needed even to be able to send messages and information between different computer systems. *See, e.g.,* Tanenbaum, “Computer Networks” (observing that, prior to 1994, “[S]ecurity was not an issue . . . making the Internet work at all was the issue”) (A130-32). Internet advisory bodies began to take up the issue of security in the mid-1990s, and a protocol called the Secure Sockets Layer “(SSL)” was developed for securing Internet message traffic. The third version of SSL, which remedies a number of weaknesses discovered in earlier versions, is central to this patent dispute.

D. The Stambler Inventions: Methods For Securing
 The Interests Of All Parties To A Transaction.

The Stambler patents variously address the need to secure transactions and to authenticate the documents, records or objects as well as the parties involved in the

transactions (JA18 col. 1 ln. 16-20).⁵ As their common specification explains, while the introduction of computers and computer communications into business transactions resulted in a certain degree of security, verification of the identity of the parties and the accuracy of the information involved became more difficult (*id.* ln. 43-54). To address this problem, the Stambler patents are directed to systems for performing secure transactions while identifying and securing the interests of *all* parties:

[U]ntil the present invention, it has not been possible to verify the identity and secure the interests of all parties to multi-party transactions and, in particular, absent parties to a transaction (*id.* col. 2 ln. 1-4).

The patents claim a number of methods directed to the various problems of transaction security, including securing transaction information, issuing credentials, and authenticating parties. Certain methods require a step of “coding” various types of information, and certain claims specify that the coding is to be performed using particular cryptographic keys. The patents give no restricted meaning to the term “coding,” but state that a coder may be “any form of such device utilizing a known algorithm, such as the Data Encryption Standard (DES)”⁶ (JA19 col. 3, l. 38-39). The patent describes examples of coding and decoding using the same key, which is characteristic of symmetric cryptosystems, and using key pairs (*e.g.*, JA19 col. 3, l. 41-44), which is

⁵ “JA _____” refers to Joint Appendix To Plaintiff And Defendants’ Opening Briefs On Claim Construction And Summary Judgment, filed contemporaneously herewith.

⁶ The defendants would have the Court read this intentionally broad statement as a “clear and deliberate statement of intent” to limit the term “coding” to the specific type of encryption system exemplified. To do so, however, requires one not only to disregard the plain words of the statement, but also to apply distorted logic to artificial distinctions (such as the difference between “coding” and “coding with”) in order to avoid the disclosure of *other* exemplified coding systems in the patent (*see pp. 27-30, infra*).

characteristic of asymmetric cryptosystems. The patents also state that in certain cases information might be coded for error detection only, without recovering the original information, and provide many examples of methods that use such “irreversible” coding (JA20 col. 5, ll. 39-44). Plainly, the term “coding” is used in the patents as a generic word to include a variety of coding methods.

Many of the Stambler protocols involve the use of other familiar security tools, including “credentials,” “error detection codes,” “secret” or “non-secret” keys, or “personal identification numbers” (PINs). Examples of how these may be employed are provided in preferred embodiments. The patents do not, however, set forth specialized definitions of any of these terms.

One important element required by certain claims of the Stambler patents is a *variable authentication number* (abbreviated “VAN”). As the name implies, and the specification states, a VAN is number that can be used for authentication, including authentication of transaction information, parties, or credentials. The specification describes examples of creating and using a VAN for authentication of transaction information and parties involved in a financial transaction (*e.g.*, JA 4, Figure 7; JA5, Figure 8B), and of creating and using a VAN for authentication of a credential (*e.g.*, JA15-16, Figures 15B and C).

The claims of the Stambler patents asserted in this litigation are claim 27 of the ‘541 patent; claims 1, 16, 28, and 35 of the ‘148 patent; and claims 12 and 34 of the ‘302 patent. The asserted claims are set forth in Exhibit 1, attached hereto, with the terms that require construction by the Court highlighted.

IV. THE CORRECT LEGAL CONSTRUCTION OF
DISPUTED CLAIM TERMS.

A. Law Of Claim Construction.

“Claim language defines claim scope.” *Beckson Marine, Inc. v. NFM, Inc.*, 292 F.3d 718, 723 (Fed. Cir. 2002). “As a general rule, claim language carries the ordinary meaning of the words in their normal usage in the field of the invention.” *Id.* “[A] court must presume that the terms in the claim mean what they say, and, unless otherwise compelled, give full effect to the ordinary and accustomed meaning of claim terms.” *Johnson Worldwide Assocs., Inc. v. Zebco Corp.*, 175 F.3d 985, 989 (Fed. Cir. 1999).

The circumstances warranting departure from the ordinary meaning of a claim term are exceptional:

[C]laim terms take on their ordinary and accustomed meanings unless the patentee demonstrated an intent to deviate from the ordinary and accustomed meaning of a claim term by redefining the term or by characterizing the invention in the intrinsic record using words or expressions of manifest exclusion or restriction, representing a clear disavowal of claim scope.

Teleflex, Inc. v. Ficosa N. Am. Corp., 299 F.3d 1313, 1327 (Fed. Cir. 2002) (emphasis added). Consequently, there is a “heavy presumption” in favor of the ordinary meaning, that can only be overcome if the patentee’s intent to deviate from the plain and ordinary meaning of a claim term is “clearly and deliberately set forth in the intrinsic evidence.” See *K-2 Corp. v. Soloman S.A.*, 191 F.3d 1356, 1363 (Fed. Cir. 1999); *Johnson Worldwide*, 175 F.3d at 989. The intent to deviate from the ordinary meaning of the words chosen must be “an express intent to impart a novel meaning,” *York Prods., Inc. v. Central Tractor Farm & Family Cent.*, 99 F.3d 1568, 1572 (Fed. Cir. 1996), or a “special

and particular definition created by the patent applicant.” *Renishaw PLC v. Marposs Soc. Per Azioni*, 158 F.3d 1243, 1249 (Fed. Cir. 1998). Absent a deliberate alteration of the meaning of a claim term by the patentee, the ordinary meaning of the term will not be disturbed. *Teleflex*, 299 F.3d at 1325.

The meaning of a claim term may *not* be limited by references to particular embodiments described in the patent specification. *Laitram Corp. v. NEC Corp.*, 163 F.3d 1342, 1347 (Fed. Cir. 1998) (“[A] court may not import limitations from the written description into the claims”); *Electro Med. Sys., S.A. v. Cooper Life Sci., Inc.*, 34 F.3d 1048, 1054 (Fed. Cir. 1994) (“Particular embodiments appearing in a specification will not be read into the claims when the claim language is broader than such embodiments”). “The fact that the specification provides a wealth of teaching about the preferred embodiments does not mean that the claims are limited to those preferred embodiments.” *Wesley Jessen Corp. v. Bausch & Lomb, Inc.*, 209 F. Supp. 2d 348, 381 (D. Del. 2002). “[A]n accused infringer cannot overcome the ‘heavy presumption’ that a claim term takes on its ordinary meaning simply by pointing to the preferred embodiment or other structures or steps disclosed in the specification or prosecution history.” *Teleflex*, 299 F.3d at 1327.

Hence, unless the intrinsic evidence contains a *redefinition* of a disputed claim term, or a *clear and deliberate disavowal* of its scope, apart from descriptions in particular embodiments, the term must be given its ordinary and accustomed meaning.

B. “Coding” Has Its Ordinary And Accustomed
Meaning.

The term “coding,” as used in claim 27 of the ‘541 patent, claim 34 of the ‘302 patent and claim 35 of the ‘148 patent, has its ordinary and accustomed meaning,

which is “transforming information from one form to another.” The ordinary meaning of “coding” includes “encoding,” which is a synonym for “encrypting.” *See, e.g.*, A5 (definition of “code” synonymous with “encode”), A7 (definition of “encode”), A16 (definition of “code”). In the field of computer security, the term “coding” is commonly understood to refer to transforming information by cryptographic processes, which may include encryption using either symmetric or asymmetric algorithms (*e.g.*, A122-23), as well as irreversible coding such as hashing (*e.g.*, A121). The patents express no restriction, exclusion, or disavowal of the scope of the term “coding,” and no statements excluding any particular types of “coding” from the scope of the invention appear anywhere in the prosecution histories of the patents. *See* Finkel Decl. ¶¶ 14-17.

The term “coding” is used generically in the patent specification consistent with the full scope of its ordinary meaning. According to the specification, one of the fundamental building blocks of the invention is a “coder,” which “may be any form of such device utilizing a known algorithm” (JA19 col. 3, ll. 30-39). At the time the patents were filed, “known algorithms” included a profusion of both symmetric and asymmetric encryption and decryption algorithms. To cite but two examples, the symmetric DES algorithm and the asymmetric RSA algorithm had each been well known in the field for more than a decade (A063 at 26; A128). Detailed examples of coding operations are described in abundance in the preferred embodiments, including operations that may be performed by either symmetric or asymmetric encryption algorithms (*e.g.*, JA4-5 Figures 7 and 8B (symmetric or asymmetric coding of “VAN,” asymmetric coding of “RVAN”)).

“Known algorithms” at the time of the invention also included irreversible or “hashing” algorithms (*see* Finkel Decl. ¶ 11). Several figures in the patents, along

with the text discussing those figures, refer specifically to an “irreversible coder” (*e.g.*, JA3-17 Figs. 6, 7, 8A, 9, 10A, 11, 12A, 13A, 15A, 15C, 16). The specification states that in one embodiment, that an irreversible “[c]oder ... may be any type of conventional coding device which can process the PIN so that the coding is irreversible (*i.e.*, the PIN cannot be recovered from the CPN)” (JA19 col. 4, ll. 21-24). In a similar context, the specification further states that all information “would not necessarily be coded in the same manner” and that some information might be coded “so as to be recoverable completely,” *i.e.*, reversibly, but that other information might be coded “without complete recovery of the original information,” *i.e.*, irreversibly (JA 20 col. 5, ll. 34-44). Similarly, certain claims refer specifically to irreversible coding of information (*e.g.*, JA32-38 claims 28, 74, 75, 78, 86).

The ordinary meaning of the term “coding” is also consistent with its use during prosecution of the patents, and particularly its use in the prior art references cited to and considered by the Patent Office in the context of the inventions. In those prior art references, the terms “coder,” “coding,” and “encoding” are used in exactly the same way they are used in the Stambler patents as including either symmetric or asymmetric cryptographic operations. MIT’s U.S. Patent No. 4,405,829 (A186-205), for example, which is widely regarded as a pioneering description of the first practical asymmetric cryptosystem, refers repeatedly to elements that carry out the RSA asymmetric algorithms as “encoding and decoding” devices (*e.g.* A191 col. 4 ll., 56-65; A196 col. 14, ll. 42-64). Another, Patent No. 5,224,162 (A211-33), describes using the RSA asymmetric algorithm in a system in which information is “encoded by an RSA encoder” (A226 col. 7, ll. 36-38). The ordinary meaning of the terms “coding” and “coder” could

not be more clear from their use in an AT&T Bell Labs Patent No. 4,590,470 (A206-10), which describes an authentication system having “coders” that “encrypt” and “decrypt” information and which, like the Stambler patents, includes claims that specify “*coding* [information] to develop encrypted signals” (emphasis added) using an asymmetric algorithm (A209 col. 4, ll. 31-42; A 210 col. 6, ll. 39-41).

An unmodified construction of the term “coding” is also fully consistent with its usage in the field of communications security by the defendants themselves and their experts. Defendants’ expert Professor Konheim agrees that Mr. Stambler’s proposed construction of the term “coding” is “perfectly reasonable” (A069 at 29):

Coding used in cryptology means the way of changing the [f]orm of information. For example, at the very beginning of my expert report I was [informed] by the attorneys for Heller Ehrman that the claim term “coding” by Mr. Stambler’s definition was transforming information from one form to another. I accept that. That is a perfectly reasonable definition.

Another of defendants’ experts, Dr. Birch, described in his own patent the “encoding” of information as including encryption with either a symmetric (*e.g.*, DES) or an asymmetric (*e.g.*, RSA) cryptographic algorithm (A234-50 Col. 10, 1.57-Col. 11, 1.6, emphasis added):

In the preferred embodiment of applications’ fraud prevention process and apparatus as shown in FIG. 5, the user authorization data for each respective cellular network N_j of FIG. 2 would be encoded by network N_j before it is sent to the fraud prevention central memory The process or method of encryption may be any of a number of processes or combination of processes well known in the arts for data protection, for example the Data Encryption Standard and RSA public key algorithm, including use of various keys or codes and their associated key management schemes

C. “Credential” Has Its Ordinary And Accustomed Meaning.

The term “credential,” as used in claim 27 of the ‘541 patent, and claims 12 and 34 of the ‘302 patent, has its ordinary and accustomed meaning, which is “a document or information obtained from a trusted source that is transferred or presented to establish the identity of a party.” *See, e.g.*, A023 (definition of “credentials”); Finkel Decl. ¶ 18. The patents do not restrict the term “credential,” and do not exclude any types of credentials from the scope of the invention (Finkel Decl. ¶ 18-19).

As used in the field of information security, the term “credential” is commonly understood to include electronic versions of credentials known as “digital certificates.” According to VeriSign, for example, “[i]n the digital world, the most robust form of credential is the digital certificate” (A342). *See also* A386 (“Present your credentials via a VeriSign Server ID”); A389 (“Digital certificates therefore can serve as a kind of digital passport or credential”); A415 (“A Digital ID, also known as a digital certificate, is the electronic equivalent to a passport or business license. It is a credential, issued by a trusted authority, that individuals or organizations can present electronically to prove their identity or their right to access information”). Indeed, defendants own opinion counsel concluded that a digital certificates was a type of “credential” within the meaning of the Stambler patents (*see* A378; A333). VeriSign’s Director of Engineering, as well as defendants’ expert Professor Konheim, both confirmed that digital certificates are credentials (A046-47 at 279, 283-84; A65 at 19-20).

The credentials described in the patents are not limited to particular types of credentials, and include paper as well as electronic credentials. For example, the specification provides that “[i]t is contemplated that this system would be useful for all

types of credentials and records; for example, motor vehicle registrations, social security cards, passports, birth certificates and all types of identification cards or personal storage media” (JA26 col. 8, ll. 54-58). Similarly, claim 19 of the ‘302 patent specifies that the entity to which a credential is issued may be a “computer program,” necessitating that the credential be a digital document (JA31). So too, the prosecution history refers to electronic and other forms of credentials. For example, a preliminary amendment filed during the prosecution of the ‘541 patent, Mr. Stambler stated: “A credential may be a check, document, record, electronic storage medium, or the like” (JA771).

D. “Secret Key” Has Its Ordinary And Accustomed Meaning.

The term “secret key” is used in claim 27 of the ‘541 patent, claim 34 of the ‘302 patent, and claims 1, 16, 28, and 35 of the ‘148 patent. “Secret key” has an ordinary and accustomed meaning in the field of information security, which is “a key that is secret, *i.e.*, unknown to parties who are not intended to know it” (Finkel Decl. ¶ 25). This ordinary meaning of “secret key” may refer to either a shared secret key of a symmetric cryptosystem, or the private key of an asymmetric cryptosystem. *Id.*; *see also* A12 (“private key” a type of “secret key”). Neither the specification nor the prosecution history states any specialized definition of the term “secret key” or excludes any type of secret key from the scope of the invention (A097 at 169-70).

The patent specification uses the term “secret key” to refer to both shared secret encryption keys known to multiple parties and encryption keys known only to one party. In Figure 9, for example, the secret key “PKO” (used at block 106) is the “personal key” of an official, *i.e.*, a key known only to the official (*see* JA22 col. 9, ll. 2-6; *see also* (A052 at 131-32). By comparison, in Figures 15A, 15B, and 15C, the key

“PKU” is a secret key that may be known to both a user and an official (*see* A053 at 133-34).

Use of the term “secret key” in the patents is consistent with the defendants’ own use of that term. Defendants’ expert Professor Tygar confirmed that a “secret key” may commonly refer to either a shared key of a symmetric cryptosystem or the private secret key of an asymmetric cryptosystem (A079 at 53-54, A081 at 69-70). Similarly, RSA’s Dr. Adams and VeriSign’s Dr. Ford testified regarding shared secret keys as well as private secret keys (A025-34 at 73, 156, 161-62, 182, 240; A058-60 at 109-110; A124.5).

E. “PIN” Has Its Ordinary And Accustomed Meaning.

The term “PIN,” an acronym for “personal identification number,” is used in claim 12 of the ‘302 patent. “PIN” is used in the art to refer to a secret code number used by an authorized user. *E.g.*, A024 (definition of “PIN”); *see also* A384 (“VeriSign may send the Subscriber a PIN, which the Subscriber enters into an enrollment web page to obtain the Certificate”); (A124.1-24.5 at 121). No intent to deviate from the ordinary meaning of the term “PIN” appears “clearly and deliberately” in the specification or prosecution histories of the patent. While the specification gives many examples of how PINs may be used in various embodiments, and describes properties that certain PINs might have, no express restriction, exclusion, or disavowal can be found of the term “PIN” itself with respect to the scope of the invention as a whole.

F. The Phrase “Variable Authentication Number” Has
The Ordinary And Accustomed Meaning Given By
Each Of Its Constituent Words.

The term “VAN” is used in claim 27 of the ‘541 patent, claim 34 of the ‘302 patent, and claims 1, 16, 28, and 35 of the ‘148 patent. “VAN” is an acronym for “variable authentication number” (col. 2, l. 17), and is, as its name implies, a variable number that can be used in verifying the identity of a party or the integrity of information or both.

Nothing in the specification or prosecution history limits the generic VAN by how it is created. The specification gives examples of VANs formed using symmetric encryption, asymmetric encryption (*e.g.*, JA5 Fig. 8B (“RVAN”)), and hashing (*e.g.*, JA17 Fig. 16 (“ADVAN”)). In particular, the specification expressly contemplates that a VAN may be formed using irreversible coding when it states that certain information could be “coded into the VAN in such a manner as to permit detection of changes (*e.g.*, error detection coding), but without complete recovery of the original information” (*e.g.*, JA20 col. 5, ll. 40-44).

G. “Using The VAN” Has Its Ordinary And
Accustomed Meaning.

The words “authenticating at least one of the parties by using the VAN” are used in claim 27 of the ‘541 patent. These words have their ordinary meaning, *i.e.*, that the VAN is used in the process of establishing the identity of at least one of the parties (Finkel Decl. ¶ 31). The patents provide examples of using a VAN in the process of establishing a party’s identity (*e.g.*, JA18 col. 2, ll. 20-30; JA 8 Figures 12A, 12B). Nothing in the specification or the prosecution history defines these words differently or suggests that the authentication must be performed in any particular way.

H. Information “Associated With” A Party Has Its Ordinary And Accustomed Meaning.

The words “information associated with” a “party” or “parties” are used in claim 27 of the ‘541 patent and claim 34 of the ‘302 patent. The ordinary meanings of these words refer to information that is in some way associated with a party. *See* A15 (definition of “associate”). The specification and the prosecution histories of the patents contain no special definition of the words or instance of use that contradicts their ordinary meaning (Finkel Decl. ¶ 20).

I. “Instrument” Or “Payment Instrument” Has Its Ordinary And Accustomed Meaning.

The term “instrument” as used in claims 1, 16, 28 and 35 of the ‘148 patent has its ordinary and accustomed meaning, which is a document or communication containing instructions for a transaction (Finkel Decl. ¶ 22). Neither the specification nor the prosecution histories limit the type of instrument, the method by which it is created, the entity who creates it, or the information it must contain. The specification refers specifically to payment methods and funds transfer methods, which utilize both paper and electronic instructions in carrying the transaction (JA20 col. 5, ll. 19-34; JA25 col. 16, ll. 60-67). Additionally, claims 16 and 20 of the ‘148 patent refer specifically to electronic instruments (JA909).

J. “Storage Means” Has Its Ordinary And Accustomed Meaning.

The term “storage means” is used in claims 12 and 34 of the ‘302 patent. By its ordinary meaning, the term “storage means” refers to a place for storing information (Finkel Decl. ¶ 32). Neither the specification nor the prosecution histories of

the patents limits the type or structure of storage means. The specification describes storing information in a variety of forms in the context of computer communications, including examples of information stored in computer files (*e.g.*, JA6-16 Figs. 10A, 11, 12B, 15A, 15B, 15C).

K. “Storing In Escrow and In Trust” Has Its Ordinary And Accustomed Meaning.

The words “storing in escrow and in trust” are used in claim 12 in accordance with their ordinary meaning, *i.e.*, storing information securely (Finkel Decl. ¶ 33). The defendants agree that “storing in escrow and trust” means storing information securely, but insist that the term refers to storing information only “until the credential is issued” (D.I. 262). While the specification gives one example of storing information “in escrow or in trust” until a credential is issued, neither the specification nor the prosecution history restricts the meaning of “storing in escrow and trust” to the scope of that example.

L. “Previously Issued” Is Used In Its Ordinary And Accustomed Sense To Mean Issued “Prior To The Transaction.”

The term “previously issued” is used in claim 27 of the ‘541 patent to describe the “credential.” In the context of that claim, the words “previously issued” mean that the credential is issued prior to the transaction. This interpretation follows from a reading of the plain language of the claim.

The preamble of claim 27 states that “the credential includ[es] a variable authentication number (VAN)” (JA505 col. 27 l. 9-10). The first step of the claim indicates how that VAN is created, namely, by “coding credential information with a

secret key of the credential issuing entity.” Logically, then, it is only after the VAN is created, and then included on the credential, that the credential can be issued

The credential must be issued prior to the second step of the claim, however, which requires “authenticating at least one of the parties using the VAN” on the credential. The second step of the claim is the first step of the “transaction”; thus, the credential must be issued prior to the transaction.

M. “Subsequently Granting” Describes A Step That Is Part Of A Method Of Enrolling And Issuing A Credential.

Claim 12 of the ‘302 patent claims a “method of enrollment and issuing a credential comprising” four steps. The last of the four steps recited that comprise the method is “subsequently granting the first party access to the first storage means by using the PIN1 or the credential.” Thus, by the plain language of the claim, the step of “subsequently granting” access is part of the method of enrollment and issuing a credential, and would therefore occur before the issuance of the credential is complete.

V. DEFENDANTS’ ARTIFICIALLY LIMITED CLAIM CONSTRUCTIONS ARE CONTRARY TO LAW.

A. Defendant’s Standard For Claim Construction.

Defendants’ claim construction “expert,” Professor Tygar, recited the methodology he used to construe claim terms in this case (A076-77 at 28-29 and A183-85):

I understand that claims are interpreted based on an objective inquiry into how one of ordinary skill in the relevant art at the time of the invention would understand the disputed word or phrase in view of the patent claims themselves, patent specification, and prosecution history. I

also understand that “extrinsic evidence” (evidence other than from the three sources just noted) may be considered to determine the ordinary meaning of the claim limitation. However, such extrinsic evidence cannot be used to vary, contradict, expand, or limit the claim language from how it is defined in the specification or prosecution history.

That proposed claim construction methodology has no connection to the ordinary and accustomed meanings of the disputed terms, which were not even understood by defendants’ claim construction “experts.” Their opinions did not begin, as the law requires, with the ordinary meanings of the words themselves, but rather with a reading of the intrinsic evidence giving the claim construction contentions provided by the defense counsel. (A075-76, A037-40). With those contentions in mind, and guided by the lawyers, the experts reviewed selected portions of the specification and prosecution histories of the patents for particular embodiments containing limitations that fell within defendants’ narrow constructions. (*id.*, A087 at 93). The result is a series of contrived definitions, crafted in every instance out of limitations found in examples and preferred embodiments of the patent, which defendants’ experts now refer to as the “ordinary meanings” of the disputed claim terms. (*id.*)

Defendants’ artificial claim construction procedure -- using the patent specification and file history to determine the “ordinary meanings” of words -- would turn the settled law on its head. To the contrary, a correct methodology would *first* determine the ordinary meanings of the words in a claim limitation, and *then* look to the patent specification and file history to determine whether there was a clear and deliberate intent to modify that meaning (pp. 14-15, *supra*). Indeed, defendants’ Tygar was tongue-tied by the artificial methodology he had employed, finding it impossible to state the ordinary meanings of rather plain and simple words, such as “a,” “the,” and “or” (A082 at

74-75, A103-04 at 266-67), without a careful review of the patent specification and file history.

B. “Coding” Is Not Limited Only To Coding By
“Applying A Reversible, Symmetric Encryption
Algorithm.”

Defendants have refused to state a contention as to the meaning of the term “coding,” insisting that its meaning is “dependent on the context in which it is used” (D.I. 262). In their effort to avoid the application of any ordinary meaning, defendants conclude that it has *no* meaning. Defendants contend that the word “coding” has meaning only when combined with other claim terms, such as “with” or “using,” and that it refers narrowly in those instances to only one type of coding, namely “applying a reversible, symmetric encryption algorithm” (*id.*). Defendants’ contentions, like those of countless accused infringers before them, are simply an attempt to limit the scope of a claim term to examples shown in preferred embodiments (as they read them) in order to avoid infringement.

Defendants’ contentions are founded upon a myopic characterization of the patent specification as describing “only” reversible, symmetric encryption operations (A165-73). Even if the patent specification contained no examples of coding other than those that are “reversible” and “symmetric,” that alone would not warrant limiting the scope of that term as used in the claims. Defendants’ characterization of the patents is in fact unfounded, for the patents describe examples of coding that are neither “reversible” nor “symmetric.”

Defendants cannot dispute that the patent specification states broadly that information might be coded “without complete recovery of the original information”

(JA20 col. 5 l. 44) -- that is, coded *irreversibly* -- and gives numerous examples of how “irreversible” coders may be used. Defendants concede, as they must, that the “coding” referred to in certain patent claims, for example claim 35 of the ‘148 patent, must necessarily refer to irreversible coding (A164). Defendants argue, however, that where the claim language does not expressly require the coding to be irreversible, coding *must* be *reversible*. Defendants’ contention could not be more backwards. Rather, because Mr. Stambler did not specially define the word “coding” or expressly limit its scope in his patents, a “coding” operation in a claim may include either reversible or irreversible coding, *unless* other claim language requires an express modification.

Defendants’ contention that the term “coding” cannot include asymmetric encryption or decryption is at odds with the very language of the claims themselves. For example, claim 34 of the ‘302 patent claims that information is “coded” with a “secret key” and “uncoded” with a “non-secret key” (JA32 col. 30 l. 66 – JA33 col. 31 l. 2). The use of separate secret and non-secret keys for coding and uncoding is a defining attribute of public-key, *i.e.*, *asymmetric*, cryptography (*see* p. 6, *supra*). Coding and uncoding information using key *pairs* is also described in the specification (*e.g.*, JA19 col. 3 l. 41-44); and the specification gives at least one detailed example of a type of variable authentication number created using one key of a public/private key pair (JA5 Fig. 8B (“RVAN”)). Notably, in formulating his opinion of the meaning of the term “coding,” defendants’ expert failed utterly to take into account the abundance of prior art describing asymmetric coding that was considered by the Patent Office during prosecution of the patents (A087 at 96, A091 at 119). When he finally examined those references, Professor

Tygar had to agree that their descriptions of “coding” and “encoding” referred unequivocally to *asymmetric* cryptography (A089 at 102, A091 at 117).⁷

In his expert report, however, Professor Tygar had argued that symmetric and asymmetric algorithms are not generally “interchangeable,” and that the use of asymmetric cryptography in the particular examples described in the Stambler patents would require “substantial changes” and implementation of a complex “infrastructure” for public key management (A171). Professor Tygar admitted, however, to knowing of common applications, such as e-mail systems and computer networks, in which particular cryptographic tasks could be carried out using either symmetric or asymmetric encryption (A107-08). In fact, given a system that includes a symmetric encryption operation, that system can generally be modified to use asymmetric encryption to perform the same operation (*see* Declaration of Christian B. Hicks, filed contemporaneously herewith). As Mr. Hicks explains, not only is the ability to select between symmetric and asymmetric cryptosystems an embedded design feature in many computer security applications, but in some cases is actually an *explicit option* that is *selectable by the user* (e.g. *id.* ¶¶ 21, 27).

Indeed, for Professor Tygar to opine that symmetric and asymmetric cryptography cannot be interchanged raises serious questions as to his credibility, given that Professor Tygar himself obtained a patent in which he states that an asymmetric algorithm may be *freely substituted* for a symmetric algorithm. In his own U.S. Patent No. 6,076,078, Professor Tygar describes using a symmetric cryptographic process in one

⁷ Defendants’ position is also undermined by their contention that the “secret keys” of the patent claims are keys known only by one party (p. 33, *infra*), which is strictly a property of *asymmetric* coding.

embodiment of his invention, but adds that the process could just as well be implemented with *asymmetric* cryptography (A251-73 at col. 10, l. 66-col. 11, l. 4, emphasis added):⁸

The merchandise key (k) is a symmetric key used to encrypt merchandise. This key is released when the transaction commits and is stored by the archive. (If asymmetric cryptography is used to encrypt the merchandise, then $E_k[\text{merchandise}]$ should be interpreted as the date which when decrypted with key k will yield merchandise.

Professor Tygar, moreover, is not alone in his *pre-suit* view of the interchangeability of symmetric and asymmetric cryptography. Defendants' other claim construction expert, Dr. Birch, *also* obtained a patent involving encryption technologies before he began work on this lawsuit, and *also* stated in that patent that the encryption of his invention could be performed using either symmetric or asymmetric algorithms. As Dr. Birch declared in his patent, the encryption process required by his invention could be carried out using either the *symmetric* DES algorithm or the *asymmetric* RSA public key algorithm (A248 col. 10 l. 66 – A249 col. 11 l. 2).

The particular examples of reversible and symmetric “coding” operations found in certain preferred embodiments cited by the defendants are just that -- *examples*. The descriptions of these examples falls far short of “words or expressions of manifest exclusion or restriction, representing a clear disavowal of claim scope” that are needed to depart from the ordinary meaning of a claim term.

⁸ Betraying his stronger loyalty to the defense lawyers who hired him (at \$400 an hour), Professor Tygar reconciled the first point by contending that he found the quoted statement from his own patent incomprehensible, thereby jettisoning the patent now assigned to a former employer (A083-84).

C. “Credential” Is Not Limited Only To “Physical”
Credentials That “Can Only Be Authenticated By
The Issuing Entity.”

Defendants contend that a “credential” of the patent claims is limited to “a physical item that vouches for the holder’s identity and that can only be authenticated by the issuing entity” (A173-76). Once again, defendants’ contention is based upon a characterization of the patents as describing only one particular type of credential A173-78). As before, the examples cited by defendants are illustrative only, and represent no “clear and deliberate intent” to depart from the ordinary and accustomed meaning of the term “credential.”

At the outset, defendants’ proposed limitation of the term “credential” to a physical item is at odds with the stated objectives of the inventions, as well as the understandings of defendants’ experts. As the specification explains, one problem addressed by the patents is verifying of identity of parties to *electronic* transactions carried out using *computers* (JA18 col. 1 l. 43-44). According to defendants’ expert, Dr. Birch, “[e]verything associated with the narrative as well as the specification leads one to the conclusion that you’re talking about computers or computer communications” (A042 at 36)). Thus, as another of defendants’ experts, Professor Konheim, concluded, digital certificates are a type of Stambler “credential” (A065 at 19-20):

The description that Mr. Stambler gives is something which is called a credential, but I had already known well before 1992 of digital certificates. . . . The credentials have certain definitions which define how they are created and certain attributes. So those properties are properties of the certificate.

Moreover, defendants’ contention overlooks examples of credentials in the patent that must necessarily be in electronic, *i.e.*, non-physical form. For example, claim 19 of the

'302 patent specifies that the entity to which a credential is issued may be a *computer program*, which quite obviously could not possess a credential in any form other than electronic (A31).

The specification expressly provides that the invention contemplates the use of “*all types of credentials* and records; for example, motor vehicle registrations, social security cards, passports, birth certificates and all types of identification cards or *personal storage media*” (JA 21col. 8, ll. 54-58, emphasis added). Defendants’ Tygar construed this last term to mean “portable” storage media, and as limited therefore to “physical” storage media that could be presented for authentication in person (A098-109). Professor Tygar had overlooked, however, that where Mr. Stambler meant to restrict the term “credential” to such devices he used the actual term “portable storage media” in the patents, and not the more general term “personal storage media” (A102 at 260-61). Moreover, Professor Tygar’s artificial distinction between “portable” and “non-portable” electronic storage media finds no support in either the intrinsic evidence or any functional distinction. The actual term “personal storage media” certainly applies to, for example, a PC hard drive regardless of whether it is “portable” or not.

Defendants’ proposed constraint that the credentials of the patent claims “can only be authenticated by the issuing entity” is also unsupportable. Professor Tygar admitted that this artificial restriction is not even characteristic of the ordinary way in which a typical “physical” credential, such as a passport, is used for purposes of authentication (A101 at 255). The patents in fact give examples of procedures for authentication using a credential that do not involve intervention of the issuing authority

(e.g., JA23 col. 12 l. 28-55 (“alternatively” retrieving authentication data from credential rather than from issuing authority).

D. The “Secret Key” Of A Party Is Not Limited Only
To Secret Keys Known Only To The Party, Or To
Keys Associated With The Party Beyond The
Duration Of A Particular Transaction.

Based upon the properties of the particular “secret keys” used in certain preferred embodiments, defendants contend that the “secret keys” of the patent claims cannot be “temporary” or known to more than one party (A160-63). Defendants’ contention that a “secret key” must be information known only to one party is flatly inconsistent with the limitations defendants’ seek to impose on the term “coding.” Defendants contend that the only type of “coding” in the patents that utilizes a key is symmetric encryption, which by definition requires a shared secret key, that is, a key known to at least two parties. Coding using a key known only to *one party* is a property of *asymmetric* cryptography, which defendants contend (incorrectly) to be outside the scope of Mr. Stambler’s patents. As a matter of logic, both of defendants’ positions cannot be correct. And, as a matter of common sense, both are demonstrably wrong.

To the extent that defendants rely for their contention upon examples in the patent of keys known only to one party, those examples are once again exemplary, not exclusive. As explained above (pp. 15-18, *supra*), the patents describe coding using keys known by one party, as well as keys known by more than one party. Neither the specification nor the prosecution history states any specialized definition of the term “secret key,” or excludes any type of secret key (whether “temporary” or “permanent”) from the scope of the invention.

- E. “PIN” Is Not Limited Only To A PIN “Selected By” A Party, “Known Only To” That Party, Which “Cannot Exist In Uncoded Form,” Or Which “Cannot Be Recoverd From Other Information.”

Defendants contend that the “PIN” of any claim in the Stambler patents is limited to a PIN having the properties described in one portion of the patent specification, namely, a PIN that is “selected” be a party, “known only to” that party, that “does not exist in uncoded form,” and that “cannot be recovered from other information anywhere in the system. The description relied upon by defendants appears in a sentence that begins: “In accordance with *an embodiment* of the present invention . . .” (JA18 col. 2 l. 30-31, emphasis added). Defendants’ expert, Dr. Birch, confirmed that this was the sole basis for defendants’ narrow construction of the term “PIN,” which otherwise in his view refers in its ordinary sense to “an identification number of some kind” (A040-41 at 29-32).

The examples of the properties of one particular type of PIN used in an embodiment of the patents is not a “redefinition” of the term PIN, or a “manifest exclusion” of other types of PINs from the scope of the inventions. Accordingly, defendants’ attempt to narrow the construction of the term “PIN” from its ordinary and accustomed meaning should be rejected.

- F. “Variable Authentication Number” Is Not Limited Only To An Authentication Number “Created By Applying A Symmetric-Key Algorithm To At Least Some Information In Such A Way That That Information Can Be Recovered.”

Defendants contend that the “VAN” of any claim in the Stambler patents is limited to a VAN created using a reversible coding operation (D.I. 262; A136-55). According to defendants’ Tygar, based upon numerous examples in preferred

embodiments of the patents, the VAN is created by a reversible coding process, along with what he characterizes as a “telling paragraph” in the specification that refers to coding and uncoding a VAN (A138). The “telling paragraph relied upon by Professor Tygar, however, begins: “In accordance with *an embodiment* of the present invention . . .” JA18 col. 2 l. 10-11, emphasis added).

In support of defendants’ narrow construction, Professor Tygar also refers to a statement made by Mr. Stambler regarding in the prosecution history, not of the patents-in-suit, but of a *different* patent that is *not asserted* in this case. During that, Mr. Stambler stated that a “transaction variable” described in a certain prior art reference (“BrachtI”), which was formed using irreversible coding, was “not the functional equivalent of the VAN of the present invention” with respect to one particular proposed claim (“Claim 7”) (A149). Seizing upon this statement, Professor Tygar argues that, regardless of the fact that the statement was made in the context of one claim in an unasserted patent having expressly different elements from those in any claim in the patents-in-suit, it nevertheless applies as a binding limitation on any VAN described in any Stambler patent (*id.*). Professor Tygar had to acknowledge, however, that Mr. Stambler’s statement was not directed to the broad distinction between reversible and irreversible coding, but rather to the peculiar properties of the VAN that were required by other express language of Claim 7,⁹ but which the “transaction variable” of BrachtI lacked (A093-95)

⁹ The fact that the VAN was qualified by express limitations in claim 7 of that patent means not that they are inherent to the unqualified term but the contrary, for if VAN meant what Tygar says, the express limitations would be superfluous. (The text of claim 7 appears on page A149 at n.19.)

The specification clearly states that a VAN may include irreversibly coded information, and gives at least one example of a VAN that is created in a way that the information used to create the VAN cannot be recovered (JA17 Fig. 16 (“ADVAN”)). Even if defendants were correct that the all VANs described in the preferred embodiments of the patent are created in a particular way, that is still not a sufficient basis for reading that exemplary property of a VAN into the scope of the patent claims.

G. “Using A VAN” To Authenticate A Party Is Not Limited Only To “Verifying That Party’s Ability To Regenerate The Key That Was Used To Originally Generate The VAN.”

Defendants contend that the only way to “use” a VAN to authenticate a party is by verifying the party’s ability to “regenerate the key that was used to originally generate the VAN, and hence, to re-code or decode the VAN” (D.I. 262). The only basis for defendants’ contention is that the VAN is used for authentication in this manner in certain embodiments described in the specification (A155-59). The patents contain no specialized definition of what it means to “use” a VAN for authentication, and do not expressly exclude from the scope of the inventions any ways of using a VAN.¹⁰

H. Information “Associated With” A Party Is Not Limited Only To Information “Tied To The Identity” Of The Party “Beyond The Duration Of A Particular Transaction.”

Defendants contend that the only way for information to be “associated with” a party in the patent claims is if the information is “tied to the identity” of that party

¹⁰ Defendants’ contention regarding the meaning of the limitation “authenticating ... if the second error detection code (EDC2) corresponds to the third error detection code (EDC3)” as used in claim 34 of the ‘302 patent is similarly misplaced (A159). Authentication requires only that the error detection codes correspond.

“beyond the duration of a particular transaction” (D.I. 262). In keeping with their touchstone of claim construction, defendants base this contention upon the fact that some information in certain embodiments described in the patents is associated in some continuing sense with a party’s identity (A178-81). The patents contain no specialized definition of what it means for information to be “associated with” a party, and do not expressly exclude from the scope of the inventions any ways associating information with a party. Defendants’ artificial construction should be rejected.

I. “Instrument” And “Payment Instrument” Are Not Limited Only To “Documents.”

Defendants contend that the “instruments” or “payment instruments” of the claims of the ‘148 patent are limited only to “documents,” but have not explained the basis of this contention. Defendants contention is at odds with the express disclosure of the specification which addresses the problem of securing electronic documents and record access systems (JA18 col. 1. 54-62), and which specifically refers to using the inventions for a “paperless/cashless transaction system” (JA29 col. 24 l. 5-6). The term “instrument” is not specially defined in the patents, and no type of instrument, electronic or otherwise, is excluded.

J. “Storage Means” Is Not Limited Only To Discrete Computer “Files.”

Defendants contend that the term “storage means” must necessarily refer to computer files, because computer files are given as examples of storage means in various preferred embodiments (D.I. 262). The patents do not specially define “storage means,” however, or exclude from the scope of the invention any types of storage means, which may in the ordinary sense include hard disks, magnetic tapes, CDs, or locations

within a computer's random access memory. Information may be stored in a file, several files, or parts of files, all of which are "storage means."

K. "Storing In Escrow and In Trust" Is Not Limited
Only To Storing "Until The Credential Is Issued."

Defendants contend that the "storing" information "in escrow and in trust" as required by claim 12 of the '302 patent is necessarily limited to storing information in escrow and in trust "until the credential is issued" (D.I. 262). Defendants' expert, Dr. Birch, conceded that storing information "in escrow and in trust" could ordinarily refer to storing information until "some action takes place," without being limited to any action in particular (A042-43 at 37-38). Dr. Birch confirmed that the entire basis for defendants' narrow construction is that in one embodiment of the patent that involves issuing a credential, information is stored securely until the credential is issued (A043 at 38-39). The sole example relied upon by defendants does not purport to define the term "storing in escrow and in trust," however, and does not expressly exclude from the scope of the invention storing information after the credential has been issued.

L. A "Previously Issued" Credential Cannot Mean A
Credential Issued Before A Claim Step Needed For
Creation Of The Credential Has Been Performed.

According to defendants, the "previously issued" credential of claim 27 refers to a credential that is issued before the execution of any of the steps recited in the claim (D.I. 262). That interpretation is impossible, though, because the first step recited in the claim is part of the process of creating the credential. In the step of "creating the VAN by coding credential information with a secret key of the credential issuing entity," the "VAN" referred to is the VAN described in the preamble of the claim that is included

in the credential. Quite obviously, the credential cannot be “issued to” a party before it is created having all of the information the claim requires the credential to have.

M. The Step Of “Subsequently Granting” Cannot
Occur After The Entire Claimed Method Has Been
Carried Out.

Defendants contend that the last step recited in claim 12 of the ‘302 patent must occur “after the credential has been issued” (D.I. 262). As the last clause of the preamble of the claim makes clear, each of the claim steps recited is part of a “method for enrollment and issuing a credential” (JA30 col. 26 l. 17-18). For defendants to contend that the last step of the claim may (indeed, must) take place after the claimed method (of which the step is an integral part) has been completed defies common sense, as well as the plain language of the claim.

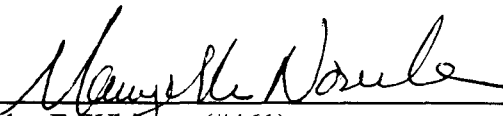
VI. CONCLUSION

For the foregoing reasons, Mr. Stambler respectfully requests the Court to construe the disputed claim terms as follows:

- “coding” means ““transforming information from one form to another”;
- “credential” means “A document or information obtained from a trusted source that is transferred or presented to establish the identity of a party”;
- “secret key” means a key that is unknown to parties who are not intended to know it;
- “PIN” is a personal number that can be used for identification;
- “variable authentication number” is a variable number that can be used for identification;
- authenticating a party “using the VAN” means using the VAN in the process of establishing the identity of a party;

- authenticating a party and information “if the second error detection code (EDC2) corresponds to the third error detection code (EDC3)” means establishing authenticity if the error detection codes correspond;
- information “associated with” a party is information that is in some way associated with a party;
- “instrument” means a document or communication containing instructions for a transaction;
- “storage means” means a place for storing information;
- “storing in escrow and in trust” means storing information securely;
- “previously issued” means issued prior to the transaction;
- “subsequently” granting access means granting access after the previous steps have been performed.

MORRIS, NICHOLS, ARSHT & TUNNELL



Douglas E. Whitney (#461)
 Maryellen Noreika (#3208)
 John D. Pirnot (#3767)
 1201 North Market Street
 P.O. Box 1347
 Wilmington, DE 19899-1347
 (302) 658-9200

Attorneys for Plaintiff Leon Stambler

OF COUNSEL:

David S. Shrager, Esquire
 Shrager Spivey & Sachs
 Two Commerce Square, 32nd Floor
 2001 Market Street
 Philadelphia, PA 19103

October 15, 2002

304673