United States District Court,
E.D. Virginia, Alexandria Division.

SURETY TECHNOLOGIES, INC., and Telcordia Technologies, Inc,
Plaintiffs.
v.
ENTRUST TECHNOLOGIES, INC,
Defendant.

No. Civ.A. 99-203-A

Nov. 4, 1999.

Patentee brought suit for infringement of patent for method of securing time-stamping of digital documents. The District Court, Ellis, J., construed terms in patent.

Patent construed.

34,954. Construed.

Nanda Krishna Alapati, Pennie & Edmonds, Washington, DC, for plaintiffs.

Terence P. Ross, Gibson, Dunn & Crutcher, Washington, DC, for defendant.

MEMORANDUM OPINION

ELLIS**, District Judge.**

The parties in this patent infringement suit dispute the meaning of three terms or phrases in the patent claims in issue, thereby necessitating the claim construction determinations recorded here.

I. The '954 Patent

Plaintiffs Telcordia Technologies ("Telcordia") and Surety Technologies ("Surety") are, respectively, the owner of and the exclusive licensee under U.S.Patent Reissue No. 34,954 ("the '954 patent"). They sue defendant Entrust Technologies ("Entrust"), alleging Entrust's sale of its "Entrust/Timestamp" product directly and contributorily infringes and induces the infringement of the '954 patent. Entrust denies any infringement and, as is typical in patent infringement cases, asserts a laundry list of affirmative defenses, including laches, inequitable conduct, estoppel, and various challenges to the patent's validity. As is also typical of patent infringement suits, the parties disagree as to the patent's scope; specifically, they dispute the meaning of three terms or phrases in the claims in issue. And where, as here, these terminological disputes are material to the infringement and validity issues presented, it is necessary for the Court to

construe the claims. FN1 Central to the claim construction task is an understanding of the patent, which, in turn, requires a brief discussion of the underlying technology.

FN1. *See* Markman v. Westview Instruments, 517 U.S. 370, 116 S.Ct. 1384, 134 L.Ed.2d 577 (1996).

The '954 patent claims an invention in the field of secure data communications. The purpose of devices in this field is to make electronic communications, such as e-mail, at least as secure, if not more so, than conventional communications. The '954 patent contributes to this field by providing a method for the secure time-stamping of digital documents. In doing so, the '954 patent draws upon science of cryptography, FN2 to create an electronic time-stamp that provides credible evidence that a particular electronic document existed in a particular form at a particular time, but without disclosing the contents of the document.

FN2. Cryptography in this context simply means the use of ciphers or codes to transform the plain text of documents into cipher or coded text.

This technology is useful in many contexts, including disputes over the priority of new inventions, where it is necessary to verify or prove a document's contents and the date on which it was created. Before the advent of electronic documents, inventors maintained indelibly dated and signed notes of their work in laboratory notebooks with sequentially numbered pages that were sewn together so that later efforts to tamper with or alter the notes might be discovered. As a further check, this notebook was reviewed regularly and signed by third parties to substantiate that the concepts disclosed in the notebook existed at least as early as the witnessed date. Electronic documents present a challenge to established methods of verification because, unlike laboratory notebooks, they can be easily revised without leaving any telltale signs, thereby raising doubt as to whether a given electronic document accurately states the date of its creation or reflects its original content.

The '954 patent seeks to address this general problem by providing a reliable system of verification whereby a digital document can be fixed in time and content by incorporating into the electronic context the essential characteristics of accepted *physical* document verification, namely affixing to the document an indelible date and a witnessing signature. The '954 patent accomplishes this by indelibly incorporating into the digital data of the document a representation of the contents of a document and an electronic stamp stating the time, so that it is not possible to change any bit of the resulting time-stamp without it being apparent. Next, the time at which the digital document is stamped is verified by a witnessing digital signature procedure that deters incorporation of a false time-stamp by transferring control of the time-stamping from the originator of the document to an outside agency.

The '954 patent's twenty-five claims cover three distinct methods of time-stamping digital documents. Claims 2, 3, and 4, the claims in issue, cover the "hash-and-sign" method, while the remaining claims variously cover the "receipt-linking" (claims 5-7) and the "pseudorandom witnessing" methods (claims 8-13). Accordingly, the principal focus here is on the hash-and-sign method. And, because the disputed claim terms all appear in claim 1, on which claims 2, 3 and 4 ultimately depend, FN3 a description of the "hash-and-sign" method necessarily begins with claim 1. Claim 1, which is quite broad, sets forth the following three-step method for time-stamping a digital document:

FN3. Claims 2 and 3 are dependent on and therefore must be read in conjunction with, claim 1. Claim 4

depends on claim 3, and consequently must be read in conjunction with both claim 1 and claim 3.

a) transmitting a digital representation of said document from an originator to an *outside agency;*
b) creating at said outside agency a receipt comprising a digital representation of then current time and at least a portion of a digital representation of said digital document; and

c) *certifying* said receipt at said outside agency by means of a *verifiable* digital cryptographic signature.

The disputed terms are underscored. Significantly, in claim 1 the contents of the digital document to be time-stamped are not altered.
Claim 2 adds an important element to claim 1. In this claim, a deterministic function algorithm is applied to the document to generate a number. FN4 In general, a deterministic function algorithm is a system or series of steps such that for a given input there is always the same output. In the context of claim 2, this function is known, in common parlance, as a "hash" function, and the steps of applying such a function to a digital document is commonly referred to as "hashing." "Hashing" a document yields a "hash value," a number that is shorter than the original unhashed document and, at the same time, unique to that document, i.e., a fingerprint of the document. In the words of the patent specification, hashing serves to "convert the digital document string to a unique number having vastly reduced digital size...." FN5 In short, claim 2 adds to claim 1 the step of hashing whereby the digital document is condensed and thereby encrypted.FN6 Claim 2 also includes sending at least part of the resulting "hash value" or number, in digital form, to the outside agency for a receipt to be certified by a digital cryptographic signature,FN7 as required by claim 1.

FN4. Claim 2 reads: "A method of time-stumping [sic] a digital document according to claim 1 wherein said transmitted digital document representation comprises at least a portion of the digital representation of the number derived by application of a deterministic function algorithm to said digital document."

FN5. U.S.Pat. No. 34,954, col. 3, ll. 14-16.

FN6. In the course of the trial, defendant disputed, for the first time, whether the application of the "deterministic function algorithm" to the digital document in claim 2 meant that the document was "hashed," i.e., reduced or condensed in size. Throughout discovery and indeed well into the presentation of the plaintiffs' case-in-chief, the parties proceeded on the mutually held premise that claim 2 added to claim 1 the step of hashing the document. Indeed, in its summary judgment brief, defendant asserted in agreement with plaintiffs, that claim 2 "simply adds the additional limitation to claim 1 that the transmission from the originator to the outside agent is hashed." Then, in the midst of plaintiffs' case-in-chief, defendant asserted that "deterministic function algorithm" as used in claim 2 did *not* mean "hashing." For the reasons stated in a forthcoming Memorandum Opinion, "deterministic function algorithm" as used in claim 2 of the '954 patent is defined as "hashing."

FN7. Digital cryptographic signatures are found in the prior art; they allow the sender and recipient of an electronic document to preserve the secrecy of a document's contents while authenticating the identity of both parties. In essence, the digital cryptographic signature acts as a "shrink wrap" around the representation of the document and the time-stamp. The origin and representation of the document and the time-stamp can

be verified, but any attempt to tamper with either the document or the time-stamp could be detected.

Claim 3 also adds elements to claim 1, on which it depends.FN8 Specifically, claim 3 requires that the outside agency's receipt include at least a portion of the number generated by the application of the deterministic function algorithm to the digital document. Put another way, claim 3 requires that at least a portion of the hash value of the digital document be included in the receipt created by the outside agency.

FN8. Claim 3 reads: "A method of time-stamping a digital document according to claim 1 wherein said receipted digital document representation comprises at least a portion of the digital representation of the number derived by application of a deterministic function algorithm to said digital document."

Finally, claim 4, which depends on claim 3, adds the important element of using a "one-way" hash function.FN9 A "one-way hash function" is one that is devised to yield a hash value or fingerprint of the document from which it is impossible to reproduce the original document. It is known as a "one way" hash function because one can go from the document to the hash value, but one cannot reproduce the document from the hash value. But, if the same hash function is applied to the same original document, the same hash value, i.e., fingerprint of the document, results. If even one character or punctuation mark in the original document is changed, then the hash value would also change. Thus applying the same hash function to the original document and to the time-stamped document and comparing the results would reveal whether the time-stamped document had been altered.

FN9. Claim 4 reads: "A method of time-stamping a digital document according claim 3 wherein said digital number representation is derived from the application of a one-way hashing algorithm."

To sum up, the "hash-and-sign" method covered in claims 2, 3, and 4 (plus claim 1) proceeds as follows. In the first step, an originator transmits a representation of a digital document to an outside agency for time-stamping. This representation may be the document's hash value, as determined by application of the one-way hash function. Next, the outside agency creates a time-stamp receipt containing a representation of the document and the current time. Finally, the outside agency then applies its verifiable digital cryptographic signature to the receipt to certify that it created the receipt.

Although plaintiff alleges only that defendant has infringed claims 2-4, the other two other time-stamping methods claimed in the '954 patent are nonetheless relevant to the claim construction task. Both methods are designed to increase the reliability of the time-stamp provided by the time-stamping agency. In the "receipt-linking" method, the originator again hashes the digital document to be time-stamped and transmits the hash value to the time-stamping agency. The time-stamping agency then links that hash value in a series with its own digital signature and the time, but in this method, the time-stamping agency also includes in the linked string the hash value from the *previous* certificate issued by the time-stamping agency. The time-stamping agency then hashes the linked string, including the previous certificate's hash value, to create a sort of "superhash." This superhash value is then transmitted back to the originator. Thus, each time-stamp issued by the time-stamping agency is linked to the preceding and succeeding time-stamp in a continuous chain. This allows one to locate the position of a particular time-stamp in the chain of time-stamps issued by that particular time-stamping agency, thereby providing additional confirmation of the time of receipt of the document by the agency.

In the "pseudorandom witnessing" method, the originator again hashes the digital document to be time-stamped, but rather than transmitting the hashed document to a particular time-stamping agent, the originator transmits it to several time-stamping services randomly chosen from among a pre-existing known universe of time-stamping services. The hash-and-sign solution is then carried out by each of these pseudorandomly selected agencies and the collection of digital signatures returned by the agencies constitutes the time-stamp certificate for the document. This goal of this method is to minimize the opportunity for the originator and the time-stamping agent to collude in falsifying the time-stamp because the originator has no way of knowing in advance which time-stamp agencies will be used. The existence of both the receipt-linking method and the pseudorandom witnessing method help shed light on the meaning of the disputed terms used in the hash-and-sign method claimed in claims 2, 3 and 4.

II. Claim Construction

[1] [2] [3] [4] *Markman* was a watershed event in patent litigation; it established, once and for all, that construction of a patent claim is a matter of law exclusively for the court. *See* Markman v. Westview Instruments, Inc., 517 U.S. 370, 116 S.Ct. 1384, 134 L.Ed.2d 577 (1996). The methodology the district courts must use in construing patent claims is found in the post- *Markman* Federal Circuit authority beginning with *Vitronics*. *See* Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576 (Fed.Cir.1996). In this regard, it is now clear that the principal guide to the interpretation of claim language is the so-called intrinsic evidence, namely, (i) the patent itself, the claims and specification and (ii) the patent's prosecution history, or "file wrapper," as it is colloquially known. *See* Vitronics, 90 F.3d at 1582-83. If, after consulting the intrinsic evidence, the proper meaning of the disputed terms is clear, then the inquiry is at an end. Extrinsic evidence consists of material outside the patent and its file history, such as expert testimony, dictionaries,FN10 learned treatises and the like. *See Markman,* 52 F.3d at 981. Typically, extrinsic evidence may only be used in aid of understanding the general technology, not to vary or contradict the terms of the claims. *See* Vitronics, 90 F.3d at 1584 n. 6. A greater role for extrinsic evidence is warranted only in those rare cases where the answer to the claim construction dispute cannot be found in the intrinsic evidence. *See* Vitronics, 90 F.3d at 1583.

FN10. Although dictionaries are technically extrinsic evidence, *Vitronics* teaches that courts "may also rely on dictionary definitions when construing claim terms so long as the dictionary definition does not contradict any definition found in or ascertained by a reading of the patent documents." Vitronics, 90 F.3d at 1584 n. 6.

[5] [6] [7] Analysis of the intrinsic evidence focuses first on the claims themselves. *See* Vitronics, 90 F.3d at 1582. When interpreting a claim, claim terms are to be given their ordinary and accustomed meaning unless it appears that the inventor has clearly stated an alternative definition in the patent specification or the file wrapper. *See id.;* Athletic Alternatives, Inc. v. Prince Mfg. Inc., 73 F.3d 1573, 1578 (Fed.Cir.1996). Put another way, claim language will be given its plain meaning unless the inventor, choosing to be his or her own lexicographer, uses terms in a manner other than their ordinary meaning and clearly discloses these special or alternative meanings in the patent specification or file history. *See* Vitronics 90 F.3d at 1582; Beachcombers v. WildeWood Creative Prods., Inc., 31 F.3d 1154, 1158 (Fed.Cir.1994). An important principle in aid of claim construction is the doctrine of claim differentiation, which presumes that there is "a difference in meaning and scope when different words or phrases are used in separate claims." Tandon Corp. v. United States Int'l Trade Comm'n, 831 F.2d 1017, 1023 (Fed.Cir.1987). Under the doctrine of claim

differentiation if the absence of such a difference in meaning or scope would make a claim superfluous, it is presumed that the difference between the claims is significant. *See id.*

[8] [9] [10] In the event the claim language alone is not dispositive, analysis should focus next on the patent's specification, including the drawings depicting the embodiments of the invention. The patent specification is "highly relevant to the claim construction analysis," and indeed, is "the single best guide to the meaning of a disputed [claim] term." Vitronics, 90 F.3d at 1582. Even though claims are to be read in view of the specification, it is axiomatic that the specification cannot be used to import into the claims limitations where no such limitations exist in the claims. *See Markman,* 52 F.3d at 980. A proposed claim interpretation that would exclude the preferred embodiment would rarely, if ever, be correct. *See* Vitronics, 90 F.3d at 1583.

[11] [12] [13] Courts may also consider the prosecution history of the patent to aid in interpreting claim terms. Because of the give-and-take between the patentee and the Patent Office that occurs during the patent application, statements made in the course of a patent's prosecution may shed light on the scope and meaning of claim terms. Thus, courts have broad power to look at the prosecution history of the patent to determine "the true meaning of language used in the patent claims," since this history may demonstrate the patentee's understanding and use of the relevant terms at the time of the application. *Markman,* 52 F.3d at 980. Nevertheless, the prosecution history may not be used to "enlarge, diminish, or vary the limitations in the claims." *Id.* And, a patentee may not construe the claims one way during prosecution in order to obtain allowance and in a different way during litigation to obtain a finding of infringement. *See* Southwall Technologies, Inc. v. Cardinal IG Co., 54 F.3d 1570, 1576 (Fed.Cir.1995).

[14] [15] [16] [17] If no ambiguity is found in the meaning of the terms of a claim after consideration of the specification and prosecution history, the inquiry is at an end. In those relatively unusual instances where the intrinsic evidence is *not* sufficient to resolve ambiguity in claim language, courts may resort to extrinsic evidence, including expert testimony, to resolve the dispute. *See* Vitronics, 90 F.3d at 1583. Ultimately, however, the interpretation to be given a term must be determined based on what the inventors actually invented and intended to envelop with the claim. *See* Renishaw PLC v. Marposs Societa' per Azioni, 158 F.3d 1243, 1250 (Fed.Cir.1998). "The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction." *Id.* These principles of claim construction must be brought to bear on the disputed elements of claims 1 through 4 of the '954 patent.

A. "Outside Agency"

[18] The first disputed term is "outside agent," as used in claim 1. Plaintiffs assert that outside agency merely means someone or something, i.e., a computer process, other than the originator of the digital document to be time-stamped. Thus, according to plaintiffs' view, the time-stamping outside agency could be a computer or other entity within the originator's company or business organization. Defendant disagrees, contending that the "outside agency" must be an independent or disinterested third party outside of and distinct from the originator's organization or company. This, defendant argues, follows from the purpose of the invention, which is to provide reliable evidence of the time a digital document was created, and such evidence cannot be reliable unless the time-stamping agency is wholly independent of and distinct from the originator and the originator's company. Anything less, defendant contends would not achieve the invention's purpose.

The first step is to consider the disputed term's plain meaning. Although often dispositive, the plain meaning is not so here. "Outside" by itself is ambiguous; the plain meaning of "outside" does not answer the question: outside of what? Or, more precisely, the claim's plain language does not answer the question whether an "outside agency" must be "outside" of the originator's company or organization. The answer to this question is instead found in the specification, which explains that the universe of document authors includes individuals, companies and even company departments and, that in one disclosed embodiment, the distributed authors may serve as outside agents "performing the time-stamping service for other members of the [author/originator] universe." FN11 This means that one company department may serve as the time-stamping outside agency for another department within the same company that originates or authors a document.

FN11. In pertinent part, the specification reads:
The method of the present invention presumes a number of document authors distributed throughout a communication network. Such authors may be individuals, companies, company departments, etc., each representing a distinct and identifiable, e.g., by ID number or the like, member of the universe. In one embodiment of the invention, this universe may constitute the clientele of the time-stamping agency (TSA), while in another embodiment the distributed authors may serve as agents individually performing the time-stamping service for other members of the universe.

U.S.Pat. No. 34,954, col. 2, ll. 55-64.

This point also finds expression in claims 8-12 of the '954 patent, which describe the pseudorandom witnessing method of time-stamping. In this method, the outside agency is selected at random from among a predetermined universe of possible agencies,including "for example, the multiplicity of authors utilizing the time-stamping process," FN12 which as the specification notes "may be individuals, companies, company departments." From this it is apparent that one company department may serve as the outside agency for another department of the same company. Thus, the claims, read in light of the specification make clear that an "outside agency," within the meaning of claim 1, need not be an entity or computer in a company or organization separate from or external to the originator's organization. Put another way, the "outside agency" could be a computer in the same department or company as that of the originator of the digital document to be time-stamped.

FN12. U.S.Pat. No. 34,954, col. 4, ll. 41-42.

[19] For its contrary view, defendant relies on the '954 patent's general goal of providing reliable evidence that a digital document existed in a particular form at a particular time. This position is flawed legally and factually. It is settled law that where, as here, "a specification does not *require* a limitation, that limitation should not be read from the specification into the claims." Intel Corp. v. ITC, 946 F.2d 821, 836 (Fed.Cir.1991) (emphasis in the original) (goal stated in the specification was not a limitation found in the claims and therefore could not be imported into the claims). Here, defendant derives from the specification that the invention's goal is to achieve time-stamping of digital documents in a fashion that is immune from interference or tampering by the document's originator, for only in this way is reliable time-stamping

achieved. The goal defendant points to in the specification is a limitation that is not required by the patent and hence may not be imported into the claims.

Quite apart from this legal obstacle to defendant's argument, it is also apparent that defendant's proposed restrictive definition of "outside agency" would not necessarily achieve the patent's goal of providing reliable evidence that a particular document existed in a particular form at a particular time. Defendant argues unpersuasively that unless the outside agency is separate from and external to the originator's company or organization, there is a risk that the originator will collude with the outside agent to alter the time-stamp or document. Yet, there is no reason to believe that an agent in the same company or organization as the originator is necessarily more susceptible to corruption or tampering by the originator than an agent outside of the originator's company or organization. Indeed, the risk of collusion may well be greater if the outside agent, although in a separate or distinct company, is a relative of the document's originator or somehow indented to her. If so, then, logically, defendant's proposed restrictive definition of outside agency should be amended to exclude even separate companies that employ the originator's relatives or persons indebted to the originator. This illustrates the fallacy of defendant's reliance on the patent's goal to construe "outside agency." In sum, interpreting "outside agency" to include persons or entities in the same company as the originator of the document is not inconsistent with the patent's goal of providing a reliable evidence that a document existed in a particular form at a particular time.FN13

FN13. In fact, it appears that the inventors realized that in some circumstances, using an outside agency, by itself, as taught in claims 2, 3 and 4 may not be dependable. Thus, the patent also discloses the "pseudorandom witnessing" method, in which the time-stamping agencies are randomly chosen from among a predetermined universe, so that the originator cannot know beforehand who the time-stamping agencies will be and thus cannot collude with them.

"*Verifiable*"

[20] The second disputed claim term is the word "verifiable," as used in the phrase "verifiable digital cryptographic signature" contained in paragraph (c) of claim 1. Plaintiffs assert that "verifiable" should be construed in accordance with its plain and ordinary meaning as "possible to prove the truth of with evidence or testimony." In the context of the '954 patent, a "verifiable digital cryptographic signature" would then mean the provision of significant evidence of the identity of the agency that applied the digital signature. Defendant, on the other hand, offers a more restrictive interpretation of "verifiable" as meaning "indelibly incorporated into the digital data comprising the receipt in such a way as to make any change apparent and to deter the incorporation of a false time statement."

Under the rule in *Vitronics,* when interpreting a claim, terms are to be given their ordinary and accustomed meaning unless it appears that the inventor has clearly stated an alternative definition in the patent specification or the file wrapper. *See* Vitronics, 90 F.3d at 1582. There is no indication in the patent that the inventors intended a special meaning for this term. The term "verifiable" is used in the patent in a way that is consistent with its plain and ordinary meaning, and hence no alternative definition is necessary. Specifically, the '954 patent describes the word "verifiable" as providing "any member of the unlimited universe with significant evidence of the identity of the transmitter of the message." FN14 Thus, a "verifiable digital cryptographic signature" shows that a particular time-stamp receipt was prepared by the outside agency applying the signature. And, contrary to defendant's assertion that "verifiable" includes deterring the application of a false time-stamp, the specification cites the well-known RSA verifiable

signature scheme, which has nothing to do with the application of a time-stamp, as an example of a "verifiable digital cryptographic signature." FN15

FN14. U.S.Pat. No. 34,954, col. 2, ll. 15-18. The patent further states:
[T]he TSA uses a verifiable signature scheme, of a type such as the public key method earlier noted, to certify the time-stamp prior to its transmittal to the author. Confirmation of the signature at a later time, such as by decryption with the TSA's public key, proves to the author and to the universe at large that the certificate originated with the TSA. *Proof of the veracity of the time-stamp itself, however, relies upon a following different aspect of the invention[, i.e., the receipt-linking embodiment].*

U.S.Pat. No. 34,954, col. 3, line 66 to col. 4, line 7 (emphasis added).

FN15. *See* U.S.Pat. No. 34,954, col. 6, ll. 29-39.

Support for the conclusion that "verifiable" as used in claim 1 should not be construed to include deterring the application of a false time-stamp can be found in the receipt-linking time-stamping method, which *does* have a means of verifying the accuracy of the time-stamp.FN16 In this method, the time-stamp prepared by the outside agency incorporates the time-stamp of the preceding and succeeding documents, which allows one to locate the position of a particular time-stamp in the chain of time-stamps issued by that particular time-stamping agency, thereby providing some certainty as to the time of receipt of the document by the agency. Claim 14 recites the limitations of the receipt-linking embodiment. Any attempt to read a requirement of the proof of veracity of the time of receipt from claim 14 into claim 1 is forbidden by the Federal Circuit's doctrine of claim differentiation. *See* Environmental Designs v. Union Oil Co., 713 F.2d 693, 699 (Fed.Cir.1983). Thus, defendant's proffered interpretation of "verifiable" cannot be adopted.

FN16. *See* U.S.Pat. No. 34,954, col. 4, ll. 5-7.

C. "Certifying"

[21] The final disputed term is the word "certifying," as used in paragraph (c) of claim 1 of the '954 patent. Plaintiffs assert that "certifying" should be defined in accordance with its plain and ordinary meaning as "confirming formally as true, accurate and genuine." In the context of the '954 patent, then, "certifying" would mean applying a verifiable digital cryptographic signature to show receipt by the outside agency. Defendants argue that "certifying" should be interpreted as meaning "to establish incontrovertibly (i) the identity of the party providing the receipt and (ii) that the contents of the receipt, particularly the time indication, are correct and have not been falsified." The short answer to defendant's contention is that claim 1 itself indicates that the "certifying" of the receipt is done "by means of a digital cryptographic signature scheme." FN17 Thus, the plain language of claim 1 and the patent specification define the meaning of "certifying" without ambiguity as simply meaning applying a verifiable digital cryptographic signature to the time-stamp receipt to show that it was prepared by the outside agency.

FN17. *See* U.S.Pat. No. 34.954, col. 8, ll. 62-64.

Moreover, it is clear that "certifying" as used in claim 1 does *not* indicate that the time in the receipt is correct because such an indication cannot be done by means of a "verifiable digital cryptographic signature." It is apparent from the preceding discussion of "verifiable" that the application of the "verifiable digital cryptographic signature" only provides proof (i) of the identity of the time-stamping agency and (ii) that the document has not been altered since the application of the time-stamp. The specification explains that the proof of the veracity of the time-stamp itself relies upon an additional aspect of the invention, namely the receipt-linking method, in which the time-stamping agency adds data from adjacent receipts to the document's time-stamp to prove the veracity of the time-stamp. Claims 1-4 do not recite the elements of the receipt-linking method; those are recited in claim 14. Any attempt to read a requirement of proof of the veracity of the time in the receipt from claim 14 into claim 1 is improper. *See* Environmental Designs, 713 F.2d at 699. Accordingly, the term certifying as used in claim 1 does not include proof of the veracity of the time in the receipt.

III. Conclusion

In summary, the Court construes the disputed elements of claim 1 of the '954 patent in the following way. "Outside agency" is defined as "some entity or something other than the originator of the digital document to be time-stamped." "Verifiable" as used in "verifiable digital cryptographic signature" is defined in accordance with its plain and ordinary meaning as "possible to prove the truth of with evidence or testimony." In the context of the '954 patent, a "verifiable digital cryptographic signature" means the provision of significant evidence of the identity of the agency that applied the digital signature. Finally, "certifying" is defined in accordance with its plain and ordinary meaning as "confirming formally as true, accurate and genuine." In the context of the '954 patent, "certifying" means applying a verifiable digital cryptographic signature to show receipt by the outside agency. "Certifying" does *not* include confirmation of the truth or accuracy of the time in the receipt. An appropriate order has issued.

E.D.Va.,1999.
Surety Technologies, Inc. v. Entrust Technologies, Inc.