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. 19, 1999.

Owner of patent for verifying digital documents sued competitor for infringement. The District Court, Ellis, J., construed claim language.

Claim construed.

34,954. Construed.

Nanda Krishna Alapati, Pennie & Edmonds, Washington, D.C., for Plaintiffs.

Terence P. Ross, Gibson, Dunn & Crutcher, Washington, D.C., for Defendant.

MEMORANDUM OPINION

ELLIS**, District Judge.**

Discovery in this patent infringement suit, as is typical in these matters, spawned three claim construction disputes which were resolved well in advance of trial. FN1 In the course of the trial, as is less typical, a fourth dispute arose. Recorded here is the resolution of the fourth claim construction dispute.

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

I.

The facts pertinent to the claim construction task are fully set out in the previous opinion and need not be repeated here. *See* Surety Technologies et al. v. Entrust Technologies, 71 F.Supp.2d 520, 1999 WL 1005021, at (E.D.Va.1999). It is sufficient to state that this is a suit brought by Telcordia Technologies ("Telcordia") and Surety Technologies ("Surety"), respectively the owner of and the exclusive licensee under U.S. Patent Reissue No. 34,954 ("the '954 patent"), against Entrust Technologies ("Entrust") for patent infringement.

Specifically, Surety claims that the use of Entrust's "Entrust/Timestamp" product, in conjunction with Entrust's public-key infrastructure, infringes claims 2, 3 and 4 of the '954 patent. Entrust denies any infringement and asserts, as affirmative defenses, (i) that claims 2, 3 and 4 of the '954 patent are invalid as anticipated, (ii) that claims 2, 3 and 4 of the '954 patent are invalid as obvious, and (iii) that the '954 patent is unenforceable on the ground that plaintiffs engaged in inequitable conduct before the U.S. Patent and Trademark Office.

A brief description of the '954 patent is warranted. FN2 The '954 patent claims three distinct methods for the secure time-stamping of digital documents. With the advent of digital documents, which can be easily altered without leaving any telltale marks, questions have arisen concerning how to verify that a particular digital document existed in a particular form at a particular time, and whether or not it has been altered. The '954 patent addresses this subject by providing a reliable system of verification whereby a digital document can be fixed in time and content by affixing to the document an indelible date and a witnessing signature.

FN2. For a more detailed description of the '954 patent and its underlying technology, *see* Surety Technologies, 71 F.Supp.2d at 523-24.

The '954 patent contains twenty-five claims. Claims 2, 3 and 4, the claims in issue, all of which depend on claim 1, disclose one of the three time-stamping methods, known colloquially as the "hash-and-sign" method. Claim 1 describes the general time-stamping method as follows: first, the digital document is transmitted from the originator to an outside agency, which creates a receipt consisting of a representation of the then-current time and at least a portion of a digital representation of the digital document. The outside agency then certifies the receipt by applying its verifiable digital cryptographic signature. FN3 Significantly, in claim 1, the document is not altered before it is transmitted to the outside agency.

FN3. "Digital cryptographic signatures" are described 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. For further explanation, *see* Surety Technologies, 71 F.Supp.2d at 523-24.

Claim 2, which contains the disputed term, "deterministic function algorithm," adds an important element to claim 1. FN4 In this claim, a deterministic function algorithm is applied to the digital document to generate a number, which is a representation of the digital document. It is, then, this number that is sent to the outside agency for time-stamping. At issue here is whether the application of the deterministic function algorithm necessarily condenses, or, in common parlance, "hashes" the digital document prior to transmission to the outside agency. "Hashing" a document compresses, and thereby encrypts, the document by creating 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.

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." U.S. Pat. No. 34,954, col. 8, l. 65 to col. 9, l. 2.

Claim 3 also adds an element to claim 1, on which it depends. 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. Finally, claim 4, which depends on claim 3, adds the important element of using a "one-way" hash function. A "one-way hash function" has a quite remarkable property: when applied to a digital document, it yields a hash value, or fingerprint, of the document that is unique to the document, and from which it is impossible to reproduce the original document. It is, in this latter respect, "one-way;" the hash function applied to the digital document yields the hash value, but one cannot recreate the document from the hash value. And, the hash value is a fingerprint of the document because if even one character or punctuation mark of the original document is changed, the application of the same one-way hash function yields a different hash value. In short, the use of the one-way hash function protects the contents of the document from disclosure while still allowing a third party to verify whether the document has been altered.

II.

The instant claim construction dispute concerns the meaning of the term "deterministic function algorithm" as used in claim 2 of the '954 patent. While the parties agree that a "deterministic function algorithm" is a formula or a series of steps such that, for a certain input, there is always the same output, the parties disagree as to whether a deterministic function algorithm, as used in claim 2, necessarily means a hash function that, when applied to a digital document, compresses the document. Plaintiffs assert that, in the '954 patent, "deterministic function algorithm"and "hash" are synonymous; defendant, on the other hand, argues that a hash function is a subset of the universe of deterministic function algorithms, and as a result the terms may not be used interchangeably.

[1] [2] [3] [4] It is settled law that the principal guide to the interpretation of claim language is intrinsic evidence, i.e., the claims, the specification and the so-called "file wrapper." *See* Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1582-83 (Fed.Cir.1996). If the intrinsic evidence provides a clear meaning for a term, the inquiry is at an end. *See id*. 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 id*. at 1584 n. 6. FN5 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 id*. 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).

FN5. *Vitronics* is often misread to state a rule of evidentiary exclusion. In fact, *Vitronics* does not preclude district judges from using extrinsic evidence for any purpose, except that it may *never* be used to alter or contradict the terms of the claims as defined by the specification and "file wrapper." In the great majority of cases, claim construction can be accomplished solely on the basis of intrinsic evidence. In such cases, the fact that a district judge consults or reviews extrinsic evidence is not error, unless, of course, the judge uses the evidence to alter or contradict the terms of the claims. Put another way, it is perhaps a pointless exercise, but not error, to consult extrinsic evidence in cases where the intrinsic evidence both adequately illuminates the technology and solves the claim construction puzzle.

[5] Analysis of the intrinsic evidence focuses first on the plain language of the claims. *See* Vitronics, 90 F.3d

at 1582. Here, the plain language is neither dispositive, nor especially helpful because the meaning of "deterministic function algorithm" is technical. In these circumstances, the next step in the claim analysis is to examine the patent specification, which often, as here, provides the answer to the meaning of the claim term. The specification of the '954 patent clearly reveals that the inventors of the '954 patent intended that claim 2 would add to claim 1 the step of condensing or "hashing" the document to be time-stamped. Thus, in discussing the hash-and-sign method claimed in claims 2, 3 and 4, the specification notes that, while claim 1 does not require any condensation of the document prior to its transmission to the outside agency for time-stamping, such a step would be highly desirable both to keep the contents of the document secret and to reduce the digital bandwidth of the transmission. FN6 According to the specification, such a step could be achieved through the application of a deterministic function, "which may, for example, be any one of a number of algorithms known in the art as 'one way hash functions.' " This language clearly reveals that the inventors of the '954 patent used deterministic function algorithm and hash function interchangeably, and that the purpose of the application of the deterministic function algorithm in claim 2 is to condensethe document prior to transmission, a step that would be accomplished through the application of a hash function. Indeed, the specification is so clear on this issue that, prior to trial, both parties regarded a deterministic function algorithm to be the same as a hash function. FN7

FN6. The specification states in pertinent part:
To ensure against interception of confidential document information during transmission, and to reduce the digital bandwidth required for transmission of the entire document, the author may optimally convert the digital document string to a unique number having vastly reduced digital size by means of a deterministic function which may, for example, be any one of a number of algorithms known in the art as "oneway [sic] hash functions."

U.S. Pat. No. 34, 954, col. 3, ll. 11-19.

FN7. Defendant, in its summary judgment brief, stated that claim 2 "simply adds the additional limitation to claim 1 that the transmission from the originator to the outside agent is hashed." The word "hash" never appears in claim 2; only the words "deterministic function algorithm" are used. But, as defendant's brief reflects, it is clear that in the context of the '954 patent, a deterministic function algorithm means a hash function.

Because the specification of the '954 patent makes clear that the inventors used the terms "deterministic function algorithm" and "hash" interchangeably, the inquiry is at an end. This is an instance, in other words, where the inventors plainly manifested their intent to act as the lexicographers of this term as used in their patent. Although extrinsic evidence, such as a technical treatise or dictionary, might reveal that, in the realm of pure mathematics, a hash function is a subset of the universe of deterministic function algorithms, under the rule in *Vitronics,* such evidence cannot be used to vary the meaning of "deterministic function algorithm" that the inventors of the '954 patent intended to use. *See* Vitronics 90 F.3d at 1582-83. Thus, the proper interpretation of "deterministic function algorithm" in the context of the '954 patent is that it is synonymous with hashing. This definition "fully comports with the specification and claims and so will preserve the patent's internal coherence." Markman, 517 U.S. at 389, 116 S.Ct. 1384.

The principle of claim differentiation confirms this result. In claim 1 of the '954 patent, a representation of the digital document is transmitted to the outside agency to be time-stamped; there is no requirement that the digital form of the document be altered prior to transmission. Claim 2 adds to claim 1 the step of applying a deterministic function algorithm to the digital document prior to transmission. The specification clearly reveals that the goal of this step is to condense, and thereby encrypt, the digital document. Under defendant's proferred broad definition of deterministic function algorithm, however, the function "1x" would qualify as a deterministic function algorithm. Yet, such a function would not alter the document in any way. If the step disclosed in claim 2 does not *by definition* alter the digital document, it would not add anything to claim 1, a result inimical to 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., 831 F.2d at 1023. The absence of any difference in the meaning or scope of claims 1 and 2 would make claim 2 superfluous; under the doctrine of claim differentiation, it must be presumed that such a difference exists. Consequently, claim 2 must be interpreted to add to claim 1 the step of altering, or in this case condensing, the digital document.

III.

In conclusion, a deterministic function algorithm as used in claim 2 of the '954 patent is defined as "a formula or series of steps such that for a certain input there is always the same output, and that condenses, or hashes, the digital document." An appropriate order has issued.

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