NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

TECSEC, INC.,
Plaintiff-Appellant

v.

ADOBE SYSTEMS INCORPORATED,
Defendant-Appellee

SAS INSTITUTE, INC., SAP AMERICA, INC., SAP AG, CISCO SYSTEMS, INC., SYBASE, INC., SOFTWARE AG, SOFTWARE AG, INC., PAYPAL, INC., ORACLE CORPORATION, ORACLE AMERICA, INC.,
Defendants

2015-1686

Appeal from the United States District Court for the Eastern District of Virginia in No. 1:10-cv-00115-LMB-TCB, Judge Leonie M. Brinkema.

Decided: August 18, 2016

MICHAEL OAKES, Hunton & Williams LLP, Washington, DC, argued for plaintiff-appellant. Also represented by MICHAEL ALFRED O'SHEA; GREGORY N. STILLMAN, Norfolk, VA.

CHARLENE M. MORROW, Fenwick & West, LLP, Mountain View, CA, argued for defendant-appellee. Also represented by VIRGINIA KAY DEMARCHI; PHILLIP JOHN HAACK, San Francisco, CA.

Before PROST, *Chief Judge,* LINN, and TARANTO, *Circuit Judges.*

LINN, *Circuit Judge.*

TecSec, Inc. ("TecSec") challenges certain claim construction rulings and appeals from a grant of summary judgment of non-infringement by Adobe Systems, Inc. ("Adobe") of TecSec's U.S. Patents Numbers 5,369,702 ("'702 patent"), 5,680,452 ("'452 patent"), 5,717,755 ("'755 patent"), and 5,898,781 ("'781 patent"), collectively the Distributed Cryptographic Object Method patents ("DCOM patents"). *TecSec, Inc. v. Int'l Business Machines Corp.*, No. 1:10-cv-115 (E.D. Va. May 7, 2015) ("*TecSec V*"). Adobe contests TecSec's arguments and asserts a number of alternative grounds for affirmance. TecSec also requests that the case be reassigned to a different district judge on remand.

Because the district court erred in its construction of "selecting a label," because we find no merit in Adobe's alternate grounds for affirmance, and because we find nothing to warrant reassignment on remand, we vacate the district court's summary judgment of non-infringement and remand for further proceedings consistent with this opinion.

I. BACKGROUND

A. History of Proceedings

In 2010, TecSec filed suit in the Eastern District of Virginia seeking to enforce its DCOM patents against thirteen defendants. The district court has thus far restricted TecSec to proceeding against only one defendant at a time, beginning with IBM and now Adobe. The claims against the other defendants remain in this six-year old case for resolution on remand. The extended pendency of this litigation raises questions as to the efficiency of the district court's one-defendant-at-a-time approach. While the scheduling of proceedings is a matter within the sound discretion of the district court, it may wish to reconsider the prudence of that approach on remand.

B. TecSec's DCOM Patents

TecSec's DCOM patents are generally directed to methods and systems of multi-level encryption that allow encrypted files to be nested within other encrypted files. In addition to multi-level encryption, the DCOM patents further limit access by using labels in the form of a field of characters attached to the encrypted files.

TecSec's charges of infringement against Adobe are focused on Adobe's "Acrobat" program. TecSec asserted both method and system claims of the DCOM patents against Adobe. Claim 1 of the '702 patent is representative of the method claims asserted against Adobe, and is reproduced below, with emphasis on the primary contested claim construction and infringement issues:

> 1. A method for providing **multi-level multimedia security** in a data network, comprising the steps of:
>
> A) accessing an **object-oriented key manager**;

> B) selecting an object to encrypt;
>
> **C) selecting a label for the object;**
>
> D) selecting an encryption algorithm;
>
> E) encrypting the object according to the encryption algorithm;
>
> F) **labelling** the encrypted object;
>
> G) reading the object **label**;
>
> H) determining access authorization based on the object **label**; and
>
> I) decrypting the object if access authorization is granted.

’702 patent, col. 12, ll. 2-15. Claim 1 of the ’755 patent includes a modified step F, which reads” “labelling the encrypted first object wherein the labelling comprises creating a display header.” ’755 patent, col. 11, ll. 61-62.

Claim 8 of the ’702 patent is representative of system claims asserted against Adobe, and is reproduced in relevant part below, again emphasizing the primary contested issues on appeal:

> 8. A system for providing multi-level multimedia security in a data network, comprising:
>
> A) digital logic means, the digital logic means comprising:
>
> 1) a system memory means for storing data . . .
>
> 3) **an object labelling subsystem**, comprising logic means for limiting object access, subject to label conditions . . .
>
> 5) **an object label identification subsystem**, comprising logic for limiting object access, subject to label conditions . . .

> B) the encryption algorithm module working in conjunction with the object labelling subsystem to create an encrypted object such that the object label identification subsystem limits access to an encrypted object.

’702 patent, col. 12, l. 45 – col. 13, l. 19.

C. Adobe’s Acrobat Program

Adobe’s Acrobat program allows users to interact with files in portable document format (“PDF”). *TecSec V* at 5. Acrobat allows a PDF author to encrypt the document using one of two relevant encryption mechanisms: password protection or digital certificate security. Password protection grants access to the document upon entry of one of two correct passwords—an “owner” password or a “user” password. The owner password allows full access to the document, e.g. printing and saving, while the user password grants access according to the permissions assigned by the owner upon encryption. Digital certificate security allows the owner to select the digital certificates of authorized recipients of the file, and to group the recipients into groups with distinct access authorizations.

When a user initiates the encryption process, a screen is displayed, asking which encryption mechanism the user wishes to use, and what parts of the document to encrypt—“all document contents,” “all document contents except metadata,” or “only file attachments.” J. App’x at 3772. Once the user sets the type of security, permissions, and what to encrypt, and clicks “OK,” the user is returned to the Acrobat interface. Acrobat does not encrypt the data until the user saves the document. When saving, Acrobat creates an “encryption dictionary” containing all the information necessary to test a user’s authorization to access and manipulate the file.

When the data is secured using password security, the encryption dictionary contains a user password key and an owner password key, but not the passwords themselves. The keys are used to test the password entered for authorization. When the data is secured using digital certificate security, Acrobat creates and encrypts a random number "file key" for each recipient, which acts like the password key, and is also stored in the encryption dictionary. A user's digital certificate data is processed and the file key is used to test the user's authorization to access the data.

Acrobat also allows files to nest within a PDF document in what Acrobat calls a PDF envelope. The nested files may be in PDF format or any number of other formats. The nested files may also be separately encrypted. If the nested file is a PDF document, it may be encrypted using Acrobat. When accessed, nested files open in their native program, and, if encrypted, go through their own decryption process, which, in the case of a PDF file, can be performed through Acrobat.

D. Proceedings before the District Court

Prior to the completion of discovery, Adobe moved for entry of certain proposed claim constructions and for summary judgment of no infringement, contending that TecSec cannot show that Acrobat meets the "mult-level . . . security," "object-oriented key manager," "label/labelling," "object," "access authorization," and "display header" limitations of the claims. The district court limited discovery solely to those issues raised in Adobe's summary judgment motion.

After briefing, the district court held a hearing on the summary judgment motion. At that hearing, the court questioned both parties with respect to the proper construction of the "selecting a label" limitation—and particularly whether selecting a label is different from creating a label. This, despite the fact that neither party had disputed the "selecting a label" limitation or sought a ruling on its construction and despite the fact that Adobe had not asserted that element as missing from the accused Acrobat program. The district court recognized that under the circumstances, supplemental briefing might be in order and expressly stated that it was "not opposed to giving [the parties] further time to brief it." J. App'x at 3935. Both Adobe and TecSec declined the district court's invitation.

In its written opinion, the district court addressed both the claim construction issues raised by Adobe and Adobe's motion for summary judgment of non-infringement. In addressing claim construction, the court began by construing "selecting a label for the object." The court noted that while the parties did not propose a construction for that limitation and declined the opportunity to brief the issue, they clearly disputed whether selecting a label includes creating a label or selecting the components that go into a label. For that reason, the court stated that that it had a duty to resolve that dispute, citing *O2 Micro International, Ltd. v. Beyond Innovation Technology Co.*, 521 F.3d 1351, 1362 (Fed. Cir. 2008). *TecSec* V at 19. The court then concluded that "before an object can be selected, it must first be created." *Id.* at 20. Moreover, it construed the limitation as meaning "choosing a pre-existing label" and not merely selecting "the components used in its creation." *Id.* at 23.

The district court then turned to the disputed claim terms presented in Adobe's motion and noted that "[r]esolution of the meaning of those terms will also assist in early resolution of the claims that TecSec asserts against the remaining defendants." *Id.* The district court first construed "object oriented key manager" to mean "a software component that is capable of performing the process of generating, distributing, replacing, storing, checking on, and destroying cryptographic keys." *TecSec V* at 26. The court next construed "label" as having been expressly defined in the specification of the "702 patent to mean "a series of letters or numbers, separate from but associated with the sending of an object, which identifies the person, location, equipment, and/or organization which is permitted to receive the associated object." *Id.* at 32. The court went on to construe "labelling" to mean "attaching a label," *id.* at 32, and "access authorization" to mean "authorization to access an object," *id.* at 34. Finally, the district court construed "display header" to mean "a header for making visually perceptible to a user." *Id.* at 35.

In addressing the merits of Adobe's motion for summary judgment of non-infringement, the district court observed that "because failure to generate a genuine issue of material fact on a single claim term precludes a finding of infringement as a matter of law, the Court will only address a subset of those arguments." *Id.* at 36. It then proceeded to address only whether Acrobat met the "multi-level . . . security," "label" and "selecting a label" limitations.

It first concluded that there was evidence raising a genuine issue of material fact and defeating summary judgment of non-infringement as to whether Adobe's Acrobat met the "multi-level . . . security" limitation. Specifically, the court cited evidence of "the use of multiple sessions to provide multiple layers of encryption," noting that Acrobat can be used to encrypt PDFs and nest them within other encrypted PDF documents. *TecSec V* at 36-37.

The district court then turned to the question of whether Acrobat's encryption dictionary met the "label" limitation and specifically whether the encryption dictionary functioned to "identify a person, a location, equipment, or an organization" consistent with the court's construction of that limitation. *Id.* at 37. The court concluded that the label limitation could not be met when using password security because the encryption dictionary does not contain either the user or owner passwords and even if it did, such passwords are not linked to the identity of a particular user. The court, however, did not reach that same conclusion when considering the use of certificate security as it found evidence indicating that "the certificate IDs identify each of the individual recipients." *Id.* at 38. The district court found this to defeat Adobe's argument.

Finally, the court addressed the "selecting a label" limitation. Based on a claim differentiation argument centered on a different limitation appearing in claims 1 and 2, the district court perceived a difference between "selecting a label" and "creating a label." It then concluded that before one can select an object, the object must pre-exist. It went on to distinguish between selecting a label and selecting the components that go into the label, concluding that the limitation required that the label itself and not merely the label components must be selected. Accordingly, it construed the limitation to mean "choosing a pre-existing label." It then concluded that using either encryption scheme, Acrobat does not meet the "selecting a label" limitation because Adobe's encryption dictionary does not exist when the type of encryption (password protection or digital certificate security) and the information to be encrypted are selected, and because the encryption dictionary is "not created until the user saves the file." *Id.* at 40. Because the district court's construction of "selecting a label" required a "pre-existing" label—an element missing from the Acrobat program—the district court concluded that Adobe was entitled to summary judgment of non-infringement.

E. The Present Appeal

TecSec appeals the district court's summary judgement of non-infringement, claiming error: (a) in the district court's basing of its grant on the *sua sponte* construction of the "selecting a label" limitation; (b) in erroneously construing the "selecting a label" limitation to require that the label be pre-existing; (c) in adopting an unnecessarily narrow construction of the "label" limitation; and (d) in holding that the encryption dictionary with password security is not a label. In a second set of arguments, TecSec appeals the district court's claim construction of the "object-oriented key manager" and "display header" claim constructions—even though it recognized that those limitations did not form the basis of the district court's summary judgment decision—and contests a statement made by the district court in footnote 23 of its opinion with regard to the "labelling" limitation. Finally, it requests that the case be reassigned to a different judge on remand.

Adobe asserts as alternative grounds for affirmance that Acrobat does not meet: (a) the "object-oriented key manager" limitation; (b) the "display header" limitation; (c) the requirement for certain memory hardware as required by the asserted system claims; (d) the "label" limitation under either construction asserted by the parties; and (e) the "multi-level . . . security" limitation. Adobe also contends that the district court provided an alternative basis for summary judgment of non-infringement in footnote 23 of its opinion, i.e. that Acrobat did not infringe because it did not satisfy the "labelling the encrypted object" limitation. Finally, Adobe argues that no basis exists to reassign this case to a different judge. This court has jurisdiction under 28 U.S.C. § 1295(a)(1).

II. Discussion

A. Standards of Review

The Fourth Circuit reviews the grant of summary judgment de novo, viewing the facts and drawing all reasonable inferences in favor of the non-moving party, and asking whether there is a genuine issue of material fact. *PBM Prods., LLC v. Mead Johnson Co.*, 639 F.3d 111, 119 (4th Cir. 2011). At summary judgment, claim construction is reviewed de novo as an issue of law when based on intrinsic evidence without underlying factual findings. *Teva Pharm. USA, Inc. v. Sandoz, Inc.*, 135 S. Ct. 831, 841 (2015). We review subsidiary district court fact-finding, if any, for clear error. *Id.*

B. Asserted Procedural Error

TecSec first contends that the district court committed serious procedural error when it granted summary judgment on the basis of its *sua sponte* construction of selecting a label, without providing proper notice. Because we vacate the district court's summary judgment on the merits, we need not and do not address TecSec's assertion of procedural error, but instead turn directly to the issues raised.

C. The Issues Raised by TecSec

We begin by addressing the principal issues raised by TecSec. We address TecSec's second set of arguments, noted, *supra*, in our analysis of Adobe's alternative grounds for affirmance.

1. "Selecting a Label"

The principal argument raised in this appeal is whether the district court properly construed the "selecting a label" limitation and whether, under the proper construction, Adobe is entitled to summary judgment of no infringement. TecSec asserts that the district court both erred in its claim construction and in granting summary judgment of non-infringement, even under the district court's claim construction.

TecSec argues that the meaning of this term was never in dispute, that the plain and ordinary meaning should have been adopted, and that no construction should have been provided. It further argues that the district court improperly read into the limitation a "pre-existing" requirement not supported by the intrinsic record. According to TecSec, the district court added its pre-existing requirement based on a flawed claim differentiation argument relating to a different limitation. It also argues that selecting a label means selecting components for a label.

Adobe contends that the district court's claim construction correctly reflects the common sense understanding that one cannot "select" something that does not yet exist. Adobe cites a number of dictionary definitions to support its argument and refers to examples in the specification that explain that a user creates an object before selecting it for preview. It also argues that in a prior case involving two of the asserted DCOM patents, TecSec took the position that the plain meaning of the term "selecting" is "choosing." Adobe further argues support based on the district court's claim differentiation analysis and contends that there is no support in the specification for TecSec's assertion that selecting a label means selecting components for a label.

The district court construed "selecting a label for the object" as "choosing a *pre-existing* label," *TecSec V* at 5, explaining that in the context of the patent, "selecting a label" is necessarily distinct from creating a label. The primary basis for the district court's construction was its understanding of claim differentiation. In addition to the step of "selecting a label," claim 1 of the '702 patent contains the additional step of "*selecting an object* to encrypt." '702 patent, col. 12, l. 5 (emphasis added). Dependent claim 2 adds the step of "*creating an object* in an application prior to accessing the object-oriented key manager," '702 patent, col. 12, ll. 16-20 (emphasis added). The district court reasoned that under the doctrine of claim differentiation, "selecting an object" in claim 1 cannot mean "creating an object" as in claim 2 and necessarily excludes "creating that object." The court then concluded that selecting must mean the same thing in both the "selecting an object" and "selecting a label" limitations and that, therefore, "selecting a label" cannot include "creating a label." *See TecSec V* at 19-20.

The problem with this reasoning is that first, the "selecting an object" and "selecting a label" limitations are separate and different limitations. Moreover, while the doctrine of claim differentiation requires that the limitations in a parent claim be construed to be different in scope from those in dependent claims, it does not necessarily mean that they are mutually exclusive. The only requirement is that the limitation in the parent be at least broad enough to encompass the limitation in the dependent claim. *Tr. of Columbia Univ. in City of New York v. Symantec Corp.*, 811 F.3d 1359, 1370 (Fed. Cir. 2016) ("Thus, in a situation where dependent claims have no meaningful difference other than an added limitation, the independent claim is not restricted by the added limitation in the dependent claim. In such situations, construing the independent claim to exclude material covered by the dependent claim would be inconsistent."); *Aspex Eyewear, Inc. v. Marchon Eyewear, Inc.*, 672 F.3d 1335, 1348 (Fed. Cir. 2012) (holding that an independent claim including the limitation "magnetic member" includes ferromagnetic material in addition to a magnet, in light of dependent claim limiting "magnetic member" to a magnet); *Am. Med. Sys., Inc. v. Biolitec, Inc.*, 618 F.3d 1354, 1360 (Fed. Cir. 2010) (concluding that "[u]nder the doctrine of claim differentiation, those dependent claims [reciting the use of particular wavelengths] give rise to a presumption that the broader independent claims [reciting that laser radiation be 'absorbed substantially completely'] are not confined to that range").

Here, the district court's reliance on the doctrine of claim differentiation is flawed. The addition of the limitation "creating an object" in claim 2 signals that the "selecting an object" limitation in claim 1 must be *at least broad enough* to cover an object that has already been created, *not* that selecting an object necessarily *excludes* an object that will be created after it is selected. Moreover, it is beyond cavil that the plain and ordinary meaning of the term "selecting" can naturally refer to a choice of a not-yet extant object. Parties regularly select any number of things that do not exist when the selection is made and are only later made to order.

The district court also relied on the portion of the specification that "requires a user to actively choose a pre-existing label." *TecSec V* at 21. This too was error. First, as the district court acknowledged, it is improper to import limitations from the specification into the claims. Second, the specification does not in any way indicate or suggest that one cannot select a label that does not yet exist, such as a label identifying the location of a terminal that is not yet connected. Nothing in the intrinsic record precludes such a possibility, or limits the meaning of "selecting a label" to the selection of pre-existing labels.

Adobe's assertion that TecSec's argument on appeal is contrary to TecSec's prior position that "selecting" means "choosing" is inapposite. "Choosing" no more requires that the chosen label already exists than does "selecting."

Lastly, while the district court is correct that "selecting a label" is not the same as "selecting components for a label," the distinction is of no consequence given our elimination of the district court's "pre-existing" requirement.

We thus agree with TecSec that "selecting a label for the object" in the DCOM patents should be given its plain meaning, without a requirement that the label exist prior to being selected. Under the proper construction of this limitation, the district court's conclusion that Adobe is entitled to summary judgement of non-infringement cannot be sustained.

2. "Label"

The district court construed the term "label" to mean "a series of letters or numbers, separate from but associated with the sending of an object, which identifies the person, location, equipment, and/or organization which is permitted to receive the associated object." *TecSec V* at 32. The court's construction is based on the following passage from the background section of the specification of the '702 patent:

> *A file 'label' for purposes of this invention means a series of letters or numbers, which may or may not be encrypted, separate from but associated with the sending of a message, which identifies the person, location, equipment, and/or organization which is permitted to receive the associated message.* Using a secure labelling regimen, a network manager or user can be assured that only those messages meant for a certain person, group of persons, and/or location(s) are in fact received, decrypted, and read by the intended receiver.
>
> * * *
>
> A system such as that described above is disclosed in U.S. patent application Ser. No. 08/009,741, the specification of which is incorporated by reference herein.

'702 patent, col. 2, ll. 34-61 (emphasis added). The district court replaced "associated with the sending of a message" and "permitted to receive the associated message" in the first paragraph, with "associated with an object," and "permitted to receive the associated object," respectively.

TecSec argues that the district court's construction of "label" was error and that the term properly should be construed simply to mean "an identifier associated with an object." It contends that the district court improperly imported a limited definition from the background section of the specification that is merely descriptive of the meaning of “label” in the prior art and that was not intended as a definition by the patentee. TecSec further argues: (1) that the label definition in the first paragraph does not apply to the invention described in the written description but instead refers to the prior art patent application cited in the second paragraph above; (2) the passage associates the label with “the sending of a *message*,” not an *object*, and sending a message does not make sense in the context of the DCOM patents; (3) the claims here have no requirement for “sending” the object, as described in the passage; and (4) the patent uses the phrase “the present invention” to define the scope of the invention, but the first paragraph above uses the phrase “this invention.” TecSec also asserts that the specification in the ‘452 patent uses “label” in a broader and more flexible way than the meaning adopted by the district court and that its definition is consistent with the plain and ordinary meaning of the term and the intrinsic record.

Adobe counters by arguing that the district court’s construction was correct based on the express definition set forth in the specification of the DCOM patents and the incorporation by reference in the ’702, ’755, and ’781 patents of the same express definition appearing in U.S. Patent Application Serial No. 08/009,741.

TecSec’s arguments are unconvincing. “[O]ur cases recognize that the specification may reveal a special definition given to a claim term by the patentee that differs from the meaning it would otherwise possess.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1316 (Fed. Cir. 2005) (en banc). To give a term a special meaning, “the patentee must clearly express an intent to redefine the term.” *Thorner v. Sony Comp. Entm’t Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (internal quotes omitted). The DCOM patents here clearly manifest such an intent by using archetypal language of definition: “A file ‘label’ for purposes of this invention means . . . .” The most natural reading of the passage is as an indicator of the intended scope of the claims using that term. "Where, as here, the patentee has clearly defined a claim term, that definition 'usually . . . is dispositive; it is the single best guide to the meaning of a disputed term.'" *Jack Guttman, Inc. v. Kopykake Enterprises, Inc.*, 302 F.3d 1352, 1360-61 (Fed. Cir. 2002) (quoting *Vitrionics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)).

The "system such as that described above . . ." passage does not change the express definition, or indicate that the definition should not apply to the '702 patent. Nor is the explicit definitional language of the passage defeated by the message/object disparity. The heart of the definition is the role of the label in restricting access, and that definition is consistent with the use of label in the asserted patent. Finally, there is no indication in the patent that only the phrase, "the present invention," shall be used as a definition, and the phrase "this invention" shall be used informationally. Both can be strong indicators of a patentee's lexicographic intent.

TecSec's argument that the broader description of label in the '452 patent undermines the definition above is also unavailing. *See* '452 patent, col. 5, ll. 16-27.[1] We

[1] "A label is a field of characters attached to the encrypted file. The label may define a group of people that may have access to the file. The label may define the device at which the file may be accessed. The device may define a single person who may have access. A label may also define the type of access, that is, read only, write only, read and write, print only, etc., that authorized persons may have. A label may also define any combination of authorized people, devices, objects, and/or access type. Thus, the label is a flexible, powerful way to set forth with great specificity all conditions that must be fulfilled in order to gain the defined access to the file."

agree with the district court that the bulk of that excerpt is wholly consistent with the definition set forth in the ’702 patent and discussed above. Moreover, the definitional language in the ’702 patent is also present in the ’452 patent. *See* ’452 patent, col. 3, ll. 1-7. We also agree with the district court that because the ’452 patent was filed after the ’702 patent issued, the excerpt in the ’452 patent cannot change the express definition in the ’702 patent. *See TecSec V* at 29. Finally, we note that neither party has argued that the word “label” should take on a different meaning in the ‘452 patent than in the other DCOM patents. We thus agree with the district court’s claim construction of “label” as meaning “a series of letters or numbers, separate from but associated with the sending of an object, which identifies the person, location, equipment, and/or organization which is permitted to receive the associated object.”

TecSec also asserts that the district court erred in concluding that the encryption dictionary is not a label when Acrobat is used with password security, even under the district court’s construction. The district court reasoned that because Acrobat stores keys and not passwords and because “the user and owner passwords are not linked to the identity of a particular user,” the encryption dictionary does not “identif[y] the person . . . permitted to receive the object,” as required to meet the “label” limitation. TecSec argues that Acrobat’s encryption dictionary contains two different keys—a user key, and an owner key—and that Acrobat’s ability to distinguish between the two identifies the individual either as a “user” or an “owner,” which is all that is required to meet the claim limitation.

We agree with TecSec. The district court, in applying its claim construction to the password security feature of the Acrobat program, required the label to identify a “particular person,” as opposed to a group of persons authorized to have access. But nothing in the intrinsic record requires that the label identify a "particular" person. *See* '702 patent, col. 2, ll. 40-44 ("Using a secure labelling regimen, a network manager or user can be assured that only those messages meant for a certain person, *group of persons*, and/or locations(s) are in fact received, decrypted, and read by the intended receiver.") (emphasis added). The district court's construction of "label," with which we agree, is broad enough to encompass a label which identifies different classes or groups of users authorized to access the object. And while some labels may limit access to particular people, it does not necessarily follow that all claimed labels must do so. Moreover, the fact that the encryption dictionary contains password "keys" and not the passwords themselves is inapposite—nothing in the district court's construction or the intrinsic record indicates that the passwords themselves must be stored in the dictionary. It is sufficient that Acrobat's encryption dictionary stores the information needed to provide appropriate access to individuals having a proper owner or user password.

The court's construction thus does not foreclose reading the label limitation on the user and owner keys stored in the encryption dictionary when using password security in the Acrobat program. For this reason, the district court erred in ruling in Adobe's favor on its argument for summary judgement of non-infringement with respect to the password security option of the Acrobat program. The district court's determination in that regard is therefore vacated.

D. Adobe's Alternative Grounds for Affirmance

Adobe presents a number of alternative grounds for affirmance. TecSec contends that several of the district court's claim construction rulings relevant to these alternative grounds for affirmance were incorrect. We address each of these arguments in turn.

1. "Object-oriented Key Manager"

Before the district court, Adobe argued that the term "object-oriented key manager" should be construed to mean "a software component that manages the encryption of an object, on an object-by-object basis, to achieve multilevel security, including the process of generating, distributing, changing, replacing, storing, checking on, and destroying cryptographic keys." TecSec argued that the term means "software that controls access to the algorithm used to encrypt and decrypt objects." The district court largely agreed with Adobe. Finding the intrinsic record clear and unambiguous, with no need to resort to extrinsic evidence, the district court construed "object-oriented key manager" as "a software component that is capable of performing the process of generating, distributing, changing, replacing, storing, checking on, and destroying cryptographic keys." *TecSec V* at 23-26. The term appears only in the asserted method claims.

Adobe does not challenge the district court's claim construction but argues that under that construction, Adobe is entitled to summary judgment of non-infringement as a matter of law because Acrobat does not store or distribute any keys. According to Adobe's expert, "the key is not saved. The key is re-derived from the password." JA3574, 120:5-10. Adobe thus contends that because there is no evidence that Acrobat meets this limitation, the district court's judgment of non-infringement may be affirmed on this ground.

TecSec asserts that the district court was correct in not citing this limitation as a basis to find no infringement. Moreover, it contends that the term properly should have been given an even broader meaning and that the district court erred in not adopting the construction TecSec proffered before the district court.

We begin by addressing TecSec's claim construction argument. TecSec argued that the term means "software that controls access to the algorithm used to encrypt and decrypt objects." TecSec bases its argument on several parts of the intrinsic record. During prosecution of the '702 patent, TecSec submitted the following in response to an indefiniteness rejection directed at the phrase "key manager":

> Various methods have evolved to manage the distribution of keys. Such methods of distribution are collectively referred to as 'key management.' **[a]** The function of key management is to perform the process of generating, distributing, changing, replacing, storing, checking on, and destroying cryptographic keys. **[b]** Under normal circumstances, the key manager begins and ends a cryptographic session by controlling access to the algorithm used to encrypt and decrypt plain text objects. Thus, a user who wants to encrypt an object or decrypt an object must first access the key manager so that an encryption algorithm may be chosen.

J. App'x 3719-3720 (bracketed lettering added). TecSec also amended the specification of the '702 patent to incorporate this language. '702 patent, col. 1, l.61 – col.2, l. 4.

TecSec urges that the passage quoted above distinguishes "key management" and "key manager," and that a key manager need only perform the functions described in sentence [b] above, and not all the key management functions described in [a]. Adobe argues that the district court construction was correct, and that TecSec's proposed construction would result in a key manager that does not perform key management.

TecSec is correct that there is a distinction between "key management" and a "key manager," but TecSec's reference to the observation that a key manager "begins and ends a cryptographic session by controlling access to the algorithm used to encrypt and decrypt plan text objects" does little to aid in an understanding of what a "key manager" is. We agree with the district court that a key manager performs key management and that according to the definitional statement added to the specification of the DCOM patents, key management includes generating, distributing, changing, replacing, storing, checking on, and destroying cryptographic keys. It is that functionality that controls access to the encryption and decryption algorithm. But that is not to say that a key manager must perform all of those functions. We find no basis in the intrinsic record to support that strict a requirement.

The district court found no support in the written description for Adobe's inclusion of the requirement that the key manager "manages the encryption of an object, on an object-by-object basis, to achieve multi-level security." For that reason, the district court did not include that part of Adobe's proffer in its claim construction. But even if the district court was correct not to include the full text requested by Adobe because of a lack of support in the written description, it was error to ignore the words "object-oriented," which are part of the claimed expression itself.

We therefore modify the district court's claim construction and construe the term "object-oriented key manager" to mean "a software component that manages the encryption of an object by performing one or more of the functions of generating, distributing, changing, replacing, storing, checking on, and destroying cryptographic keys."

Adobe argues that it is entitled to summary judgment of non-infringement as a matter of law because Acrobat does not store or distribute any keys. TecSec points to evidence in the record that Adobe's Acrobat products include a security handler in the form of a software module which implements various aspects of the encryption process and controls access to the contents of encrypted documents. More specifically, this evidence shows that the security handler generates a key for encryption upon saving of a PDF document following a user's selection of a security method.

In light of this evidence, we cannot conclude as a matter of law that Adobe is entitled to summary judgment of non-infringement as failing to meet the properly construed "object-oriented key manager" limitation.

2. "Display Header"

Adobe argues that it is entitled to summary judgment of non-infringement as a matter of law because Acrobat does not show a "display header" to the user. The district court construed "display header" as "a header for making visually perceptible to a user." *Id.* Adobe argues that to meet the limitation as construed by the district court, the display header must be capable of being shown to the user, something it contends is not done using Acrobat.

The only support for Adobe's position is the testimony of its corporate representative, Mr. Kaufman, that it is not possible to view the content of the encryption dictionary. J. App'x at 3574. TecSec argues that Acrobat's security properties dialog box "can display label attributes," J. App'x at 3797, which are "derived from the information in the encryption dictionary," TecSec Reply Br. at 18, such as a "listing of various permission levels," whether a document is encrypted and document restrictions, and enables modifying security settings, J. App'x at 3797.

Adobe has not explained why the security properties dialog box does not meet the "display header" limitation, and therefore has failed to show a lack of a genuine issue of material fact with respect to this limitation.

TecSec argues that the district court erred in not giving this limitation its plain and ordinary meaning. We disagree and find the district court's construction fully supported by the intrinsic record.

3. Memory Hardware

Adobe makes a cursory argument that Acrobat does not include the memory hardware required by all asserted system claims, a fact Adobe contends TecSec never disputed. TecSec argues that the district court struck Adobe's argument regarding memory hardware and that it therefore had no reason to oppose it. *See TecSec V* at 35 n.20. TecSec also argues that Acrobat is installed on computers having memory, thus supporting TecSec's charge of infringement. In particular, TecSec points to the testimony of Adobe's corporate witness that he encrypted a PDF file within another encrypted PDF file using Acrobat installed on a computer, *see* J. App'x at 3565, and points to a blog post describing those same steps, *see* J. App'x at 3683. Adobe's cursory argument on this issue has no merit.

4. "Label" with Respect to Certificate Security

Adobe argues that even under the district court's construction of the term "label," the district court erred in concluding that a genuine issue of material fact was presented when using digital certificate security. Adobe reasons that TecSec's infringement theory identifies one "object" to be labelled—the strings and streams in the body of a PDF file—and a different object to be encrypted—the entire PDF file, including the header and the trailer. Because the claims require that the same object be labelled and encrypted, Adobe argues that Acrobat cannot infringe as a matter of law regardless of the type of security used.

We disagree with Adobe. All the encryption information is contained in the encryption dictionary, the part of the PDF that TecSec identifies as the label. Adobe does not explain the asserted disconnect between the object encrypted and the object labelled, apart from citing TecSec's claim charts. However, TecSec's claim charts allege that the same thing is given a label and encrypted. For example, for the "selecting a label" limitation, TecSec states that "Adobe Acrobat applies passwords to and/or sets permission levels for an object, such as a PDF file/document." J. App'x at 4089. The same object, "a PDF file" is identified as capable of being "encrypted with a password." J. App'x at 4090. The object identified throughout is a PDF file or a PDF document, regardless of whether the element being discussed is the label or the encryption. Adobe has failed to show a lack of a genuine issue of material fact as to the same. This argument thus fails to provide an alternative ground for affirmance.

5. "Multi-level . . . Security"

We have previously construed 'multi-level . . . security" in the preamble to be restrictive, and to require multiple layers of encryption, based primarily on TecSec's prosecution history. *TecSec, Inc. v. Int'l Bus. Mach. Corp.*, 731 F.3d 1336, 1345-46 (Fed. Cir. 2013). Adobe argues that Acrobat cannot nest an encrypted PDF within another encrypted PDF *within a single session of* Acrobat, and therefore Acrobat does not meet the claim limitation.[2] Adobe also argues that Acrobat can only encrypt one level of information because the encryption of the PDF envelope treats the encrypted data in a nested object in line with the data of the PDF envelope.

[2] Adobe also frames the multiple-sessions requirement through the lens of divided infringement, i.e. that Adobe is not responsible for the infringement because *the user* opens up multiple sessions of Acrobat, and Adobe does not direct or control the user's actions. This argument is incorrect for the same reasons described in the analysis that follows.

TecSec's position is that Acrobat performs multi-level security when a user encrypts a PDF, then attaches it to a separate PDF, and then encrypts that PDF. TecSec argues that the claim does not require that all this be performed within a single session window of Acrobat.

The district court agreed with TecSec and denied Adobe's motion, finding that the multi-window sequence described above provides evidence that Acrobat could be used to allow multi-level security. The district court also noted that "TecSec has also presented evidence that Adobe has instructed its customers that Acrobat could be used in that manner." *TecSec V* at 37.

We agree. To access the data in the nested PDF, a user would have to decrypt the PDF envelope, followed by decrypting the nested PDF. That Acrobat uses multiple windows to accomplish the nesting does not place Acrobat outside the scope of the limitation. Claim 1 recites "A method for providing multi-level multimedia security in a data network." Adobe's envelope feature "provid[es] multi-level multimedia security in a data network." That the mechanism provided requires multiple sessions of the accused product does not preclude infringement. There is at least a genuine issue of material fact whether Acrobat PDF envelopes infringe the multi-layer security limitation.

Relatedly, Adobe argues that because two sessions of Acrobat are required, each "object" at each level does not have its own "label." We agree with the district court that TecSec has presented ample evidence to defeat summary judgment of non-infringement of this element. To take just one example, Mr. Kaufman, Adobe's 30(b)(6) witness confirmed that an encrypted PDF attached to another PDF which was then encrypted, would yield separate encryption dictionaries (the alleged "label"), and could have different passwords or security types. J. App'x at 3629.

We see no error in the district court's conclusion that genuine issues of material fact preclude summary judgment of non-infringement on the basis of the multi-level security limitation.

6. Labelling and Footnote 23

In considering the "selecting a label" limitation, the district court added the following seemingly gratuitous footnote regarding a separate limitation directed to labelling:

> Although not briefed by the parties, there are other aspects of the DCOM Patents that Acrobat does not perform. For example, each asserted claim requires some form of "labelling." At TecSec's urging, "labelling" has been construed to mean "attaching a label." Acrobat does not attach an encryption dictionary to an encrypted PDF document; instead, it inserts the encryption dictionary into the (pre-existing) trailer for that file. Jones Dec. 68. Indeed, far from being attached to the encrypted object, "[t]he encryption dictionary is part of the trailer portion of a PDF document." Id. Thus, what TecSec alleges is a label is not "attached to" the object, it is part of the object.

TecSec V at 40 n.23.

TecSec argues that the district court's footnote is procedurally flawed because TecSec was not permitted discovery on this issue and was never given an opportunity to respond, in violation of Federal Rules of Civil Procedure 56(f). TecSec also contends that the substantive basis for the district court's decision is also flawed, because first, the system claims do not have a "labelling" limitation, but claim a distinct "object labelling subsystem," *see* Section E.1 *infra* at 29-30, and second, Acrobat meets the labelling limitation when the encryption dictionary is attached to a PDF file's trailer, which is itself attached to the encrypted PDF content.

Adobe finds no procedural fault with the district court's footnote and asserts it as an alternative basis for affirmance. It also contends that the district court was substantively correct. According to Adobe, Acrobat inserts the data for the encryption dictionary into a preexisting trailer in the PDF, making the encryption dictionary a *part* of the encrypted PDF file and not an attachment thereto. It therefore contends that Acrobat cannot meet the "labelling the encrypted object" limitation.

Federal Rule of Civil Procedure 56(f) allows a district court to grant summary judgment on a ground not raised by a party "[a]fter giving notice and a reasonable time to respond." *See also U.S. Dev. Corp. v. Peoples Fed. Sav. & Loan Ass'n*, 873 F.2d 731, 735 (4th Cir. 1989) (explaining that the exercise of a district court's power to enter summary judgment *sua sponte* is contingent on giving the losing party a reasonable opportunity to demonstrate genuine issue of material fact); *Matthews v. Thomas*, 385 F. App'x 283, 288 (4th Cir. 2010). It undisputed that the district court failed to provide TecSec with any opportunity to respond with respect to the "labelling" limitation. In this regard, the district court procedurally erred in making the statements set forth in footnote 23. We give that footnote no weight and do not address whether a genuine issue of material fact exists as to whether Acrobat meets the labelling limitation when it inserts the encryption dictionary into the trailer of the PDF document.

Adobe also argues that the district court erred in its claim construction of "labelling," and that under the proper claim construction—"labelling the encrypted object" means "attachment of a label to an object by software after encryption of that object," J. App'x at 2468—Acrobat does not meet this limitation because no label is attached to a single encrypted object but to a group of encrypted and non-encrypted data. Adobe's argument is convoluted and not persuasive. Adobe does not explain the presence of the temporal "after" in its construction, why the admittedly encrypted PDF content could not be considered a single encrypted object, or why the presence of unencrypted PDF components disallowed the labelling of the encrypted object. We therefore reject this ground as an alternative basis for affirmance.

E. Considerations on Remand

1. System and Method Claims

In granting summary judgment, the district court grouped the method and system claims together with respect to the selecting a label limitation, despite the fact that the system claims do not include that limitation, *in haec verba*. The system claims require an "object labelling subsystem" and an "object identification subsystem." The district court treated these limitations as necessarily containing the "selecting a label" limitation from the method claims. Without analysis, the court stated that "the [system] claims use only 'slightly different language to describe substantially the same invention [as the method claims].'" *TecSec V* at 39 n.22 (quoting *Ohio Willow Wood Co. v. Alps South, LLC.*, 735 F.3d 1333, 1342 (Fed. Cir. 2013)). The court also determined that TecSec waived any distinction between the claim types by grouping its infringement arguments together under method claim 1 as representative of all of the asserted claims.

TecSec argues that treating the system and method claims together was improper, and failed to give meaning to the explicit difference in claim language. Adobe counters that TecSec equated the "object labelling subsystem" language in the system claims to the "selecting a label" limitation in the method claims by explaining in its infringement contentions that Acrobat practiced the "object labelling subsystem" of the systems claims because

"Adobe Acrobat products select a label for an object." J. App'x at 2208.

We agree with TecSec that equating the limitations was improper. There is no indication that TecSec's argument in its infringement contentions used "selecting a label" as a term of art or to reference the meaning of that phrase in the method claims, rather than using it for its colloquial meaning. In other words, although the district court departed from an ordinary meaning of "selecting a label" in construing the method claims, TecSec has nowhere indicated that the distinct "object labelling subsystem" in the system claims should be bound by the same construction.

Adobe also argues that TecSec equated the two phrases in TecSec's brief in response to Adobe's summary judgment motion, in which TecSec put forth claim 1, a method claim, as representative of the DCOM patents. However, that statement was made before "selecting a label" was at issue because Adobe had not raised it in its opening brief, and it was first raised *sua sponte* by the district court at the summary judgment hearing. *TecSec V* at 19. TecSec was never confronted with a reason to explicitly consider the equivalence of the system and method claims with respect to the two terms. Moreover, the district court concluded that the scope of the system and method claims was identical without analysis of the relative claim scope. Determining the relative claim scope here is not an easy issue admitting of such a cursory conclusion. *Cf., e.g.*, *CLS Bank Int'l v. Alice Corp.*, 717 F.3d 1269, 1288-1292 (Fed. Cir. 2013) (en banc) (Lourie, J., concurring).

On remand, TecSec will have the opportunity to separately argue infringement of the method and system claims with respect to these limitations.

2. Doctrine of Equivalents

Adobe argues that TecSec has waived its opportunity to argue infringement of the "selecting a label" limitation under the doctrine of equivalents. We disagree. As explained above, that limitation entered this case via *sua sponte* consideration by the district court. TecSec was under no obligation to assert the doctrine of equivalents with respect to a limitation that Adobe did not even dispute was literally met by the accused product.

3. Reassignment

TecSec urges us to reassign this case to a different judge on remand. TecSec argues that Judge Brinkema has repeatedly held against TecSec, has raised dispositive issues *sua sponte*, has been reversed on appeal for many of those issues, and has pre-judged a § 101 issue that has not yet been raised.

Reassignment is only appropriate in exceptional circumstances. Here, reassignment is governed by Fourth Circuit law, which applies a three factor test for reassignment: 1) whether the judge would be reasonable expected to have substantial difficulty putting her views that were held to be incorrect out of her mind; 2) whether reassignment is necessary to preserve the appearance of justice; and 3) the degree of waste of judicial resources and duplication if the case were reassigned. *See United States v. Guglielmi*, 929 F.2d 1001, 1007 (4th Cir. 1991).

Nothing in this case merits reassignment on remand. Though Judge Brinkema has indeed ruled against TecSec several times, there is no indication that these rulings are biased, or are based on anything other than the exercise of her reasoned judgment and appropriate judicial discretion. Though Judge Brinkema has indeed raised more than one dispositive issue *sua sponte*, the Federal Rules of Civil Procedure specifically empower district courts to do so, subject to certain procedural requirements. *See* Fed.

R. Civ. P. Rule 56(f). Moreover, given the six-year journey of this case through the judicial system, and its multiparty complexity, reassignment would create significant unnecessary waste of judicial resources. Here, we are not persuaded that any of the factors in the Fourth Circuit's test are met. Reassignment thus is not appropriate in this case.

III. CONCLUSION

For the foregoing reasons, we modify the district court's construction of "selecting a label," affirm its construction of the term "label," vacate its determination that Acrobat's password security option cannot meet the "label" limitation, and vacate the grant of summary judgment of non-infringement. We also modify the district court's construction of "object-oriented key manager" and deny each of Adobe's alternative grounds for affirmance. We reject Adobe's request that the case be reassigned and remand the case for further proceedings consistent with this opinion.

VACATED AND REMANDED

IV. COSTS

Costs are awarded to TecSec.