IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

INTERTRUST TECHNOLOGIES CORP., *Plaintiff,* v. CINEMARK HOLDINGS, INC.,	Case No. 2:19-cv-00266-JRG LEAD CASE
AMC ENTERTAINMENT HOLDINGS INC., and	Case No. 2:19-cv-00265-JRG MEMBER CASE
REGAL ENTERTAINMENT GROUP, *Defendants.*	Case No. 2:19-cv-00267-JRG MEMBER CASE

CLAIM CONSTRUCTION ORDER

Before the Court is the opening claim construction brief of Intertrust Technologies Corporation ("Plaintiff") (Dkt. No. 88, filed on May 1, 2020),[1] the response of Cinemark Holdings, Inc., AMC Entertainment Holdings, Inc., and Regal Entertainment Group (collectively "Defendants") (Dkt. No. 101, filed on May 15, 2020), and Plaintiff's reply (Dkt. No. 103, filed on May 22, 2020). The Court held a hearing on the issues of claim construction and claim definiteness on June 17, 2020. Having considered the arguments and evidence presented by the parties at the hearing and in their briefing, the Court issues this Order.

[1] Citations to the parties' filings are to the filing's number in the docket (Dkt. No.) and pin cites are to the page numbers assigned through ECF.

Table of Contents

I. BACKGROUND

Plaintiff alleges infringement of ten U.S. Patents: No. 6,157,721 (the "'721 Patent"), No. 6,640,304 (the "'304 Patent"), No. 6,785,815 (the "'815 Patent"), No. 7,340,602 (the "'602 Patent"), No. 7,406,603 (the "'603 Patent"), No. 7,694,342 (the "'342 Patent"), No. 8,191,157 (the "'157 Patent"), No. 8,191,158 (the "'158 Patent"), No. 8,931,106 (the "'106 Patent"), and No. 9,569,627 (the "'627 Patent") (collectively, the "Asserted Patents").

The '721 Patent was filed on August 12, 1996 and incorporates U.S. Patent Application No. 08/388,107, which was filed on February 13, 1995. The patent's abstract provides:

> Secure computation environments are protected from bogus or rogue load modules, executables and other data elements through use of digital signatures, seals and certificates issued by a verifying authority. A verifying authority—which may be a trusted independent third party—tests the load modules or other executables to verify that their corresponding specifications are accurate and complete, and then digitally signs the load module or other executable based on tamper resistance work factor classification. Secure computation environments with different tamper resistance work factors use different verification digital signature authentication techniques (e.g., different signature algorithms and/or signature verification keys)—allowing one tamper resistance work factor environment to protect itself against load modules from another, different tamper resistance work factor environment. Several dissimilar digital signature algorithms may be used to reduce vulnerability from algorithm compromise, and subsets of multiple digital signatures may be used to reduce the scope of any specific compromise.

The '304, 157, and '158 Patents are related through common claims of priority. Each of these patents ultimately claims priority to U.S. Patent Application No. 08/388,107 through a series of continuation applications. The abstract of the '304 Patent provides:

> The present invention provides systems and methods for secure transaction management and electronic rights protection. Electronic appliances such as computers equipped in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated

> transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware- based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

The '815 Patent lists an earliest priority claim to U.S. Application No. 60/138,171, filed on June 8, 1999, and incorporates U.S. Patent No. 5,892,900 (the "'900 Patent") which was filed on August 30, 1996. The '900 Patent claims priority to U.S. Patent Application No. 08/388,107. The '815 Patent's abstract provides:

> Systems and methods are provided for protecting and managing electronic data signals that are registered in accordance with a predefined encoding scheme, while allowing access to unregistered data signals. In one embodiment a relatively hard-to-remove, easy-to-detect, strong watermark is inserted in a data signal. The data signal is divided into a sequence of blocks, and a digital signature for each block is embedded in the signal via a watermark. The data signal is then stored and distributed on, e.g., a compact disc, a DVD, or the like. When a user attempts to access or use a portion of the data signal, the signal is checked for the presence of a watermark containing the digital signature for the desired portion of the signal. If the watermark is found, the digital signature is extracted and used to verify the authenticity of the desired portion of the signal. If the signature-containing watermark is not found, the signal is checked for the presence of the strong watermark. If the strong watermark is found, further use of the signal is inhibited, as the presence of the strong watermark, in combination with the absence or corruption of the signature-containing watermark, provides evidence that the signal has been improperly modified. If, on the other hand, the strong mark is not found, further use of the data signal can be allowed, as the absence of the strong mark indicates that the data signal was never registered with the signature-containing watermark.

The '602 Patent lists an earliest priority claim to U.S. Application No. 60/138,171 and incorporates the '900 Patent. The '602 Patent's abstract provides:

> Systems and methods are disclosed for enabling a recipient of a cryptographically-signed electronic communication to verify the authenticity of the communication on-the-fly using a signed chain of check values, the chain being constructed from the original content of the communication, and each check value in the chain being at least partially dependent on the signed root of the chain and a portion of the communication. Fault tolerance can be provided by including error-check values in the communication that enable a decoding device to maintain the chain's security in the face of communication errors. In one embodiment, systems and methods are provided for enabling secure quasi-random access to a content file by constructing

> a hierarchy of hash values from the file, the hierarchy deriving its security in a manner similar to that used by the above-described chain. The hierarchy culminates with a signed hash that can be used to verify the integrity of other hash values in the hierarchy, and these other hash values can, in turn, be used to efficiently verify the authenticity of arbitrary portions of the content file.

The ’603 Patent lists an earliest priority claim to U.S. Application No. 60/151,790, filed on August 31, 1999, and incorporates the ’900 Patent. The ’603 Patent’s abstract provides:

> Systems and methods are provided for protecting electronic content from the time it is packaged through the time it is experienced by an end user. Protection against content misuse is accomplished using a combination of encryption, watermark screening, detection of invalid content processing software and hardware, and/or detection of invalid content flows. Encryption protects the secrecy of content while it is being transferred or stored. Watermark screening protects against the unauthorized use of content. Watermark screening is provided by invoking a filter module to examine content for the presence of a watermark before the content is delivered to output hardware or software. The filter module is operable to prevent delivery of the content to the output hardware or software if it detects a predefined protection mark. Invalid content processing software is detected by a monitoring mechanism that validates the software involved in processing protected electronic content. Invalid content flows can be detected by scanning the information passed across system interfaces for the attempted transfer of bit patterns that were released from an application and/or a piece of content management software.

The ’342 and ’106 Patents are related in that the ’106 Patent issued from an application that is a continuation of the ’342 Patent’s application. Each of these patents lists an earliest priority claim to Application No. 60/210,479, filed on June 9, 2000, and incorporates the ’900 Patent. The ’342 Patent’s abstract provides:

> Systems and methods are disclosed for managing and protecting electronic content and applications. Applications, content, and/or users can be given credentials by one or more credentialing authorities upon satisfaction of a set of requirements. Rights management software/hardware is used to attach and detect these credentials, and to enforce rules that indicate how content and applications may be used if certain credentials are present or absent. In one embodiment an application may condition access to a piece of electronic content upon the content’s possession of a credential from a first entity, while the content may condition access upon the application’s possession of a credential from a second entity and/or the user's possession of a credential from a third entity. Use of credentials in this manner enables a wide variety of relatively complex and flexible control arrangements to be put in place and enforced with relatively simple rights management technology.

The ’627 Patent lists an earliest priority claim to U.S. Application No. 60/209,454, filed on June 4, 2000, and incorporates the ’900 Patent. The ’627 Patent’s abstract provides:

> System and methods are disclosed for governing digital rights management systems and other applications through the use of supervisory governance applications and keying mechanisms. Governance is provided by enabling the supervisory applications to revoke access keys and/or to block certain file system calls, thus preventing governed applications from accessing protected electronic content.

II. LEGAL PRINCIPLES

A. Claim Construction

“It is a ‘bedrock principle’ of patent law that ‘the claims of a patent define the invention to which the patentee is entitled the right to exclude.’” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (quoting *Innova/Pure Water Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). To determine the meaning of the claims, courts start by considering the intrinsic evidence. *Id.* at 1313; *C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 861 (Fed. Cir. 2004); *Bell Atl. Network Servs., Inc. v. Covad Commc’ns Group, Inc.*, 262 F.3d 1258, 1267 (Fed. Cir. 2001). The intrinsic evidence includes the claims themselves, the specification, and the prosecution history. *Phillips*, 415 F.3d at 1314; *C.R. Bard, Inc.*, 388 F.3d at 861. The general rule—subject to certain specific exceptions discussed *infra*—is that each claim term is construed according to its ordinary and accustomed meaning as understood by one of ordinary skill in the art at the time of the invention in the context of the patent. *Phillips*, 415 F.3d at 1312–13; *Alloc, Inc. v. Int’l Trade Comm’n*, 342 F.3d 1361, 1368 (Fed. Cir. 2003); *Azure Networks, LLC v. CSR PLC*, 771 F.3d 1336, 1347 (Fed. Cir. 2014) (“There is a heavy presumption that claim terms carry their accustomed meaning in the relevant community at the relevant time.”) (vacated on other grounds).

“The claim construction inquiry … begins and ends in all cases with the actual words of the claim.” *Renishaw PLC v. Marposs Societa’ per Azioni*, 158 F.3d 1243, 1248 (Fed. Cir. 1998). “[I]n

all aspects of claim construction, 'the name of the game is the claim.'" *Apple Inc. v. Motorola, Inc.*, 757 F.3d 1286, 1298 (Fed. Cir. 2014) (quoting *In re Hiniker Co.*, 150 F.3d 1362, 1369 (Fed. Cir. 1998)). First, a term's context in the asserted claim can be instructive. *Phillips*, 415 F.3d at 1314. Other asserted or unasserted claims can also aid in determining the claim's meaning, because claim terms are typically used consistently throughout the patent. *Id.* Differences among the claim terms can also assist in understanding a term's meaning. *Id*. For example, when a dependent claim adds a limitation to an independent claim, it is presumed that the independent claim does not include the limitation. *Id*. at 1314–15.

"[C]laims 'must be read in view of the specification, of which they are a part.'" *Id*. (quoting *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc)). "[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Id*. (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)); *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed. Cir. 2002). But, "'[a]lthough the specification may aid the court in interpreting the meaning of disputed claim language, particular embodiments and examples appearing in the specification will not generally be read into the claims.'" *Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) (quoting *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1571 (Fed. Cir. 1988)); *see also Phillips*, 415 F.3d at 1323. "[I]t is improper to read limitations from a preferred embodiment described in the specification—even if it is the only embodiment—into the claims absent a clear indication in the intrinsic record that the patentee intended the claims to be so limited." *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 913 (Fed. Cir. 2004).

The prosecution history is another tool to supply the proper context for claim construction because, like the specification, the prosecution history provides evidence of how the U.S. Patent and Trademark Office ("PTO") and the inventor understood the patent. *Phillips*, 415 F.3d at 1317. However, "because the prosecution history represents an ongoing negotiation between the PTO and the applicant, rather than the final product of that negotiation, it often lacks the clarity of the specification and thus is less useful for claim construction purposes." *Id.* at 1318; *see also Athletic Alternatives, Inc. v. Prince Mfg.*, 73 F.3d 1573, 1580 (Fed. Cir. 1996) (ambiguous prosecution history may be "unhelpful as an interpretive resource").

Although extrinsic evidence can also be useful, it is "'less significant than the intrinsic record in determining the legally operative meaning of claim language.'" *Phillips*, 415 F.3d at 1317 (quoting *C.R. Bard, Inc.*, 388 F.3d at 862). Technical dictionaries and treatises may help a court understand the underlying technology and the manner in which one skilled in the art might use claim terms, but technical dictionaries and treatises may provide definitions that are too broad or may not be indicative of how the term is used in the patent. *Id*. at 1318. Similarly, expert testimony may aid a court in understanding the underlying technology and determining the particular meaning of a term in the pertinent field, but an expert's conclusory, unsupported assertions as to a term's definition are not helpful to a court. *Id*. Extrinsic evidence is "less reliable than the patent and its prosecution history in determining how to read claim terms." *Id*. The Supreme Court has explained the role of extrinsic evidence in claim construction:

> In some cases, however, the district court will need to look beyond the patent's intrinsic evidence and to consult extrinsic evidence in order to understand, for example, the background science or the meaning of a term in the relevant art during the relevant time period. *See, e.g., Seymour v. Osborne*, 11 Wall. 516, 546 (1871) (a patent may be "so interspersed with technical terms and terms of art that the testimony of scientific witnesses is indispensable to a correct understanding of its meaning"). In cases where those subsidiary facts are in dispute, courts will need to make subsidiary factual findings about that extrinsic evidence. These are the

> "evidentiary underpinnings" of claim construction that we discussed in *Markman*, and this subsidiary factfinding must be reviewed for clear error on appeal.

Teva Pharm. USA, Inc. v. Sandoz, Inc., 574 U.S. 318, 331–32 (2015).

B. Departing from the Ordinary Meaning of a Claim Term

There are "only two exceptions to [the] general rule" that claim terms are construed according to their plain and ordinary meaning: "1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows the full scope of the claim term either in the specification or during prosecution."[2] *Golden Bridge Tech., Inc. v. Apple Inc.*, 758 F.3d 1362, 1365 (Fed. Cir. 2014) (quoting *Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012)); *see also GE Lighting Solutions, LLC v. AgiLight, Inc.*, 750 F.3d 1304, 1309 (Fed. Cir. 2014) ("[T]he specification and prosecution history only compel departure from the plain meaning in two instances: lexicography and disavowal."). The standards for finding lexicography or disavowal are "exacting." *GE Lighting Solutions*, 750 F.3d at 1309.

To act as his own lexicographer, the patentee must "clearly set forth a definition of the disputed claim term," and "clearly express an intent to define the term." *Id.* (quoting *Thorner*, 669 F.3d at 1365); *see also Renishaw*, 158 F.3d at 1249. The patentee's lexicography must appear "with reasonable clarity, deliberateness, and precision." *Renishaw*, 158 F.3d at 1249.

To disavow or disclaim the full scope of a claim term, the patentee's statements in the specification or prosecution history must amount to a "clear and unmistakable" surrender. *Cordis Corp. v. Boston Sci. Corp.*, 561 F.3d 1319, 1329 (Fed. Cir. 2009); *see also Thorner*, 669 F.3d at 1366 ("The patentee may demonstrate intent to deviate from the ordinary and accustomed meaning

[2] Some cases have characterized other principles of claim construction as "exceptions" to the general rule, such as the statutory requirement that a means-plus-function term is construed to cover the corresponding structure disclosed in the specification. *See, e.g., CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1367 (Fed. Cir. 2002).

of a claim term by including in the specification expressions of manifest exclusion or restriction, representing a clear disavowal of claim scope."). "Where an applicant's statements are amenable to multiple reasonable interpretations, they cannot be deemed clear and unmistakable." *3M Innovative Props. Co. v. Tredegar Corp.*, 725 F.3d 1315, 1326 (Fed. Cir. 2013).

C. Definiteness Under 35 U.S.C. § 112, ¶ 2 (pre-AIA) / § 112(b) (AIA)

Patent claims must particularly point out and distinctly claim the subject matter regarded as the invention. 35 U.S.C. § 112, ¶ 2. A claim, when viewed considering the intrinsic evidence, must "inform those skilled in the art about the scope of the invention with reasonable certainty." *Nautilus Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 910 (2014). If it does not, the claim fails § 112, ¶ 2 and is therefore invalid as indefinite. *Id.* at 901. Whether a claim is indefinite is determined from the perspective of one of ordinary skill in the art as of the time the application for the patent was filed. *Id.* at 911. As it is a challenge to the validity of a patent, the failure of any claim in suit to comply with § 112 must be shown by clear and convincing evidence. *BASF Corp. v. Johnson Matthey Inc.*, 875 F.3d 1360, 1365 (Fed. Cir. 2017). "[I]ndefiniteness is a question of law and in effect part of claim construction." *ePlus, Inc. v. Lawson Software, Inc.*, 700 F.3d 509, 517 (Fed. Cir. 2012).

When a term of degree is used in a claim, "the court must determine whether the patent provides some standard for measuring that degree." *Biosig Instruments, Inc. v. Nautilus, Inc.*, 783 F.3d 1374, 1378 (Fed. Cir. 2015) (quotation marks omitted). Likewise, when a subjective term is used in a claim, "the court must determine whether the patent's specification supplies some standard for measuring the scope of the [term]." *Datamize, LLC v. Plumtree Software, Inc.*, 417 F.3d 1342, 1351 (Fed. Cir. 2005). The standard "must provide objective boundaries for those of skill in the art." *Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1371 (Fed. Cir. 2014).

D. Previous Constructions of Disputed Terms

D-1. Prior court constructions are entitled to reasoned deference.

The "importance of uniformity in the treatment of a given patent" suggests a level of deference to previous court constructions of disputed claim terms. *See Finisar Corp. v. DirecTV Grp., Inc.*, 523 F.3d 1323, 1329 (Fed. Cir. 2008) (quoting *Markman v. Westview Instruments, Inc.*, 517 U.S. 370, 390 (1996)); *Teva Pharm. USA, Inc. v. Sandoz, Inc.*, 574 U.S. 318, 329 (2015) (noting that "prior cases … sometimes will serve as persuasive authority"). While the "doctrine of *stare decisis* does not compel one district court judge to follow the decision of another … previous claim constructions in cases involving the same patent are entitled to substantial weight." *TQP Dev., LLC v. Intuit Inc.*, No. 2:12-CV-180-WCB, 2014 U.S. Dist. LEXIS 84057, at *21–22 (E.D. Tex. June 20, 2014) (Bryson, J.).

D-2. In some instances, a party may be estopped from pursuing a claim construction different from a prior court construction under the equitable doctrine of issue preclusion.

In some instances, previous court construction of a disputed term may trigger issue preclusion and bind a party to a previous construction. *Teva*, 574 U.S. at 329 ("prior cases will sometimes be binding because of issue preclusion") (citing *Markman*, 517 U.S. at 391). "Issue preclusion generally refers to the effect of a prior judgment in foreclosing successive litigation of an issue of fact or law actually litigated and resolved in a valid court determination essential to the prior judgment, whether or not the issue arises on the same or a different claim [for relief]." *New Hampshire v. Maine*, 532 U.S. 742, 748–49 (2001). "Issue preclusion prohibits a party from seeking another determination of the litigated issue in the subsequent action." *Soverain Software LLC v. Victoria's Secret Direct Brand Mgmt., LLC*, 778 F.3d 1311, 1315 (Fed. Cir. 2015) (quoting *State Farm Mut. Auto. Ins. Co. v. Logisticare Sols., LLC*, 751 F.3d 684, 689 (5th Cir. 2014)). Issue preclusion applies only if four conditions are met:

> First, the issue under consideration in a subsequent action must be identical to the issue litigated in a prior action. Second, the issue must have been fully and vigorously litigated in the prior action. Third, the issue must have been necessary to support the judgment in the prior case. Fourth, there must be no special circumstance that would render preclusion inappropriate or unfair.

State Farm, 751 F.3d at 689. Ultimately, issue preclusion is an "equitable doctrine" and the "discretion vested in trial courts to determine when it should be applied is broad." *Nations v. Sun Oil Co.*, 705 F.2d 742, 744 (5th Cir. 1983) (citing *Parklane Hosiery Co., Inc. v. Shore*, 439 U.S. 322, 331 (1979)).

III. AGREED CONSTRUCTIONS

The parties have agreed to constructions set forth in their Joint Claim Construction Chart Pursuant to Patent Rule 4-5(d) (Dkt. No. 104). Based on the parties' agreement, the Court hereby adopts the agreed constructions for these cases.

IV. CONSTRUCTION OF DISPUTED TERMS

A. "secure processing unit"

Disputed Term[3]	Plaintiff's Proposed Construction	Defendants' Proposed Construction
"secure processing unit" • '157 Patent Claims 69, 87, 89 • '158 Patent Claim 4	plain and ordinary meaning	processing circuitry that functions in a self-contained, trusted computing environment

The Parties' Positions

Plaintiff submits: The meaning of "secure processing unit" ("SPU") is plain given the plain meaning of the constituent terms "secure" and "processing unit"—it refers to a "processing unit

[3] For all term charts in this order, the claims in which the term is found are listed with the term but: (1) only the highest-level claim in each dependency chain is listed, and (2) only asserted claims identified in the parties' Joint Claim Construction Chart Pursuant to Patent Rule 4-5(d) (Dkt. No. 104) are listed.

with protection." The term is used in the '157 and '158 Patents according to this plain meaning. Defendants' proposed construction improperly confuses a SPU with a secure processing environment ("SPE"). For example, and as explained in the patents, the SPU provides a secure environment such as a SPE rather than functioning within a SPE. Dkt. No. 88 at 7–9.

In addition to the claims themselves, Plaintiff cites the following intrinsic and extrinsic evidence to support its position: **Intrinsic evidence**: '157 Patent col.20 ll.24–34, col.20 ll.48–54, col.44 ll.57–64, col.48 ll.3–22, col.48 ll.56–59, col.62 ll.23–26, col.67 ll.49–52, col.77 ll.52–55, col.77 ll.63–66. **Extrinsic evidence**: *Microsoft Press Computer Dictionary* at 84 (3d ed. 1997) (Plaintiff's Ex. K, Dkt. No. 88-11 at 4); *IBM Dictionary of Computing* at 533 (10th ed. 1993) (Plaintiff's Ex. L, Dkt. No. 88-12 at 4); *The New Oxford American Dictionary* at 1541 (2001) (Plaintiff's Ex. M, Dkt. No. 88-13 at 4).

Defendants respond: "Secure processing unit" ("SPU") is defined in the '157 and '158 Patents. The patents explain that the SPU is "the core secure transaction control arrangement" that "provide[s] a trusted environment" (quoting '157 Patent col.47 l.65 – col.48 l.3). The patents further explain that the SPU "processes information in a secure processing environment" having an "execution space" and a "self-contained computing and processing environment" (quoting *id*. at col.58 ll.14–15, col.77 ll.52–55, col.77 ll.63–64, col.86 ll.49–53). And the patents explain that the SPU is "a dedicated semiconductor arrangement" (quoting *id*. at col.20 ll.29–34). Dkt. No. 101 at 6–8.

In addition to the claims themselves, Defendants cite the following **intrinsic evidence** to support their position: '157 Patent fig.6, col.20 ll.29–34, col.47 l.65 – col.48 l.1, col.48 ll.3–13, col.58 ll.14–15, col.77 ll.52–55, col.77 ll.63–64, col.86 ll.49–53.

Plaintiff replies: The dedicated-circuitry SPU described in the ’157 and ’158 Patents is an exemplary embodiment; it is not definitional of a SPU. The patents also teach that other SPU embodiments use circuitry elements of a standard CPU to avoid the need for a special-purpose processor. Ultimately, the SPU is physical hardware that is “sufficiently secure so as to protect … VDE processes” (quoting ’157 Patent col.48 ll.37–59). It is not a logical construct such as Defendants’ proposed “computing environment.” Dkt. No. 103 at 4.

Plaintiff cites further **intrinsic evidence** to support its position: ’157 Patent col.20 ll.42–54, col.48 ll.31–59, col.58 ll.9–44, col.77 ll.52–56.

Analysis

The issues in dispute distill to whether “secure processing unit” is defined in the ’157 and ’158 Patents as Defendants propose. It is not. A “plain and ordinary meaning” construction, however, is not appropriate and leaves open the nature of “secure” in the term whereas the patents are clear that “secure” here refers to resistance to unauthorized use of information and processes. At the hearing, the Court proposed the construction adopted below and the parties agreed to the construction without argument.

The claims provide little guidance as to the meaning of “secure processing unit.” Rather, the claims primarily situate the “secure processing unit” within the claimed invention. For example, Claim 4 of the ’158 Patent provides (with emphasis added) as follows:

> **4**. A method utilizing an electronic appliance comprising a processor and a memory encoded with program instructions that, when executed by the processor, cause the processor to perform the method, the method comprising:
> receiving, at the electronic appliance, an electronic content item, the electronic content item being encrypted at least in part;
> storing the electronic content item in memory of the electronic appliance;
> receiving, at the electronic appliance, independently from the electronic content item via separate delivery and protected separately from the electronic content item, a rule specifying one or more permitted uses of the electronic content item;

> receiving, at the electronic appliance, a request to use the electronic content item;
> determining that the requested use of the electronic content item corresponds to a permitted use of the electronic content item specified in the rule; and
> using, at least in part, a decryption key to decrypt the electronic content item, the decryption key being stored in a ***secure processing unit*** contained in the electronic appliance.

The patents define "secure processing unit," though not concisely and not as Defendants suggest. For example, the '157 Patent provides as follows:

> VDE provides organization, community, and/or universe wide secure environments whose integrity is assured by processes securely controlled in VDE participant user installations (nodes). VDE installations, in the preferred embodiment, may include both ***software and tamper resistant hardware semiconductor elements***. Such a ***semiconductor arrangement comprises, at least in part, special purpose circuitry that has been designed to protect against tampering with, or unauthorized observation of***, the information and functions used in performing the VDE's control functions. ***The special purpose secure circuitry provided by the present invention includes at least one of a dedicated semiconductor arrangement known as a Secure Processing Unit (SPU)*** and/or a standard microprocessor, microcontroller, and/or other processing logic that accommodates the requirements of the present invention and functions as an SPU.

'157 Patent col.20 ll.19–34 (emphasis added). This states that "secure processing unit" refers to a "dedicated semiconductor arrangement" that protects information and processes against tampering and other unauthorized use. The patents also explain that the SPU may encompass a specially configured standard processor, such as one operating in "protected mode," and that it need not be a special-purpose processor:

> Designing VDE capabilities into one or more standard microprocessor, microcontroller and/or other digital processing components may materially reduce VDE related hardware costs by employing the same hardware resources for both the transaction management uses contemplated by the present invention and for other, host electronic appliance functions. This means that ***a VDE SPU can employ (share) circuitry elements of a "standard" CPU***. For example, ***if a "standard" processor can operate in protected mode*** and can execute VDE related instructions as a protected activity, then such an embodiment may provide sufficient hardware security for a variety of applications and ***the expense of a special purpose processor might be avoided***.

Id. at col.20 ll.42–54 (emphasis added). The patents further explain that the SPU may be implemented in software:

> The degree of trustedness of a VDE arrangement will be primarily based on whether ***hardware SPUs*** are employed at participant location secure subsystems and the effectiveness of the SPU hardware security architecture, software security techniques when ***an SPU is emulated in software***, and the encryption algorithm(s) and keys that are employed for securing content, control information, communications, and access to VDE node (VDE installation) secure subsystems.

Id. at col.44 ll.57–64 (emphasis added). This states that the SPU may be, but is not necessarily, special-purpose hardware. It may also be emulated in software. On this point, the patents further provide as follows:

> Secure Processing Units
>
> An important part of VDE provided by the present invention is the ***core secure transaction control arrangement, herein called an SPU (or SPUs)***, that typically must be present in each user's computer, other electronic appliance, or network. ***SPUs provide a trusted environment*** for generating decryption keys, encrypting and decrypting information, managing the secure communication of keys and other information between electronic appliances (i.e. between VDE installations and/or between plural VDE instances within a single VDE installation), securely accumulating and managing audit trail, reporting, and budget information in secure and/or non-secure non-volatile memory, maintaining a secure database of control information management instructions, and ***providing a secure environment*** for performing certain other control and administrative functions.
>
> ***A hardware SPU (rather than a software emulation)*** within a VDE node is necessary if a highly trusted environment for performing certain VDE activities is required. Such a trusted environment may be created through the use of certain control software, one or more ***tamper resistant*** hardware modules such as a semiconductor or semiconductor chipset (including, for example, a tamper resistant hardware electronic appliance peripheral device), for use within, and/or operatively connected to, an electronic appliance.

'157 Patent col.47 l.65 – col.48 l.22 (emphasis added). Thus, the SPU is a "core secure transaction control arrangement" that may be implemented as special-purpose hardware or in software. It provides a secure environment for managing and manipulating information. The patents further explain:

> Secure Processing Unit (SPU)
>
> The "VDE participants" may each have an "electronic appliance." The appliance may be or contain a computer. The appliances may communicate over the electronic highway 108. FIG. 6 shows a secure processing unit ("SPU") 500 portion of the "electronic appliance" used ***in this example*** by each VDE participant. ***SPU 500 processes information in a secure processing environment 503***, and ***stores important information securely***. ***SPU 500 may be emulated by software operating in a host electronic appliance***.
>
> SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It ***prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions***. Barrier 502 also controls external access to secure resources, processes and information within SPU 500. In one example, tamper resistant security barrier 502 is formed by security features such as "encryption," and hardware that detects tampering and/or destroys sensitive information within secure environment 503 when tampering is detected.

Id. at col.58 ll.9–29. Again, the SPU may be implemented in software, it is not necessarily a dedicated circuit.

On balance, the patents' description of the "secured processing unit" does not mandate Defendants' proposed construction. In some embodiments, the SPU is described as functioning in a self-contained, trusted computing environment. But these are exemplary embodiments and the description is that of a use of the SPU, not of defining attributes of the SPU. The definitional language regarding the SPU suggests rather that the defining nature of the SPU is that it protects information and processes against unauthorized use such as tampering and unauthorized viewing. This is what allows it to provide and operate within a trusted environment.

Accordingly, the Court construes "secure processing unit" as follows:

- "secure processing unit" means "processing unit that makes information and processes resistant to unauthorized use."

B. "secure electronic container"

Disputed Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
"secure electronic container" • '627 Patent Claim 1	plain and ordinary meaning	protected digital content that includes or consists of an encrypted version of the secret information

The Parties' Positions

Plaintiff submits: The plain meaning of "secure electronic container" refers to a collection of elements that may be used to securely hold digital information. The "container" does not necessarily hold "content" and it may be "secure" without being encrypted. For example, the '627 Patent describes that the secure electronic container may hold "protected digital information" that is not content. And the patent incorporates the '900 Patent, which describes that the container may be "encrypted or otherwise secured" such as through digital signatures (citing '900 Patent[4] col.13 ll.50–53, col.228 ll.27–44, col.257 ll.8–14). Dkt. No. 88 at 9–11.

In addition to the claims themselves, Plaintiff cites the following intrinsic and extrinsic evidence to support its position: **Intrinsic evidence**: '627 Patent fig.1, col.5 ll.6–16, col.10 ll.4–26; '900 Patent col.13 ll.50–56, col.13 ll.62–67, col.134 ll.39–41, col.228 ll.27–44, col.257 ll.8–14; '479 Application[5] at 7 (Plaintiff's Ex. BB, Dkt. No. 88-28 at 9). **Extrinsic evidence**: *Encarta World English Dictionary* at 1620 (1999) (Plaintiff's Ex. N, Dkt. No.88-14 at 5); *IBM Dictionary of Computing* at 603 (10th ed. 1993) (Plaintiff's Ex. L, Dkt. No. 88-12 at 5).

Defendants respond: "Secure electronic container" is used in the'627 Patent to refer to secure formatting that involves encryption of the protected or secret information. It is not a "container"

[4] U.S. Patent No. 5,892,900. The '900 Patent is incorporated by reference into the '627 Patent. '627 Patent col.4 ll.56–64.
[5] U.S. Patent Application No. 60/210,479. The '479 Application is incorporated by reference into the '627 Patent. '627 Patent col.10 ll.7–22.

in any ordinary sense of the word. As set forth in Claim 1 of the patent, the secure electronic container includes secret information that is extracted from the container by decrypting the container. Thus, the container necessarily includes or consists of an encrypted version of the secret information. Dkt. No. 101 at 8–10.

In addition to the claims themselves, Defendants cite the following **intrinsic evidence** to support their position: '627 Patent fig.1, col.5 ll.6–16, col.10 ll.4–26; '479 Application at 7:10–11 (Defendants' Ex. 1, Dkt. No. 101-1 at 9).

Plaintiff replies: The secure electronic container ("SEC") is not limited to "content" and while Claim 1 requires that "at least a portion of the SEC be decrypted to extract the secret information" reading this requirement into the SEC would improperly render other claim language superfluous. Dkt. No. 103 at 5.

Analysis

There appear to be two issues in dispute. First, whether the secure electronic container is necessarily limited to "protected digital content." It is not. Second, whether the secure electronic container of Claim 1 of the '627 Patent necessarily includes an encrypted version of the secret information. It does, but that is plainly expressed in other claim limitations and therefore not an inherent attribute of "secure electronic container." At the hearing, the Court proposed the construction adopted below and the parties agreed to the construction without argument.

Claim 1 of the '627 Patent provides significant context to inform the meaning of "secure electronic container":

> 1. A method performed by a system comprising a processor and a non-transitory computer-readable storage medium storing instructions that, when executed by the processor, cause the system to perform the method, the method comprising:
>
> receiving, by a secure control application executing on the system in a protected processing environment, a request to access ***protected content*** by a

> governed application executing on the system in a processing environment separate from the protected processing environment;
>
> ***extracting***, by the secure control application, ***secret information from a secure electronic container***, the secret information being configured to be used, at least in part, ***to decrypt the protected content***, wherein ***extracting the secret information comprises decrypting at least a portion of the secure electronic container to generate unencrypted secret information***; and
>
> sending, by the secure control application, the unencrypted secret information from the protected processing environment to the governed application executing in the processing environment separate from the protected processing environment.

As plainly stated in the claim, secret information is extracted from a secure electronic container and the extraction includes decrypting a portion of the secure electronic container. Thus, the claim expresses that "secure electronic container" includes an encrypted version of the secret information. This suggests that such attribute is not inherent to the "secure electronic container." *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1314 (Fed. Cir. 2005) (en banc) (noting that the use of the term "steel baffles" "strongly implies that the term 'baffles' does not inherently mean objects made of steel").

The '627 Patent's technical disclosure further informs the meaning of "secure electronic container." For instance, the patent states that the container can take on any suitable form and that containers are commercially available:

> As shown in FIG. 1, secure processing application 100 is used to access protected digital information 130 that is stored in a ***secure electronic container*** 106 and/or in protected database 104. ***The secure electronic container can take any suitable form***. For example, secure electronic container 106 might comprise a DigiBox® or DigiFile™ container produced by InterTrust Technologies Corporation, or ***<u>might</u> simply consist of an encrypted version of the protected digital information***. In other embodiments, ***other secure container formats—such as those described in the '900 patent or available commercially***—could be used.

'627 Patent col.5 ll.6–16. Thus, the container "might simply consist of an encrypted version of the protected digital information." It might not.

The ’900 Patent, incorporated into the ’627 Patent and referenced in the passage quoted above, further explains the “secure container”:

> VDE, in its preferred embodiment, employs object software technology and ***uses object technology to form “containers” for delivery of information that is (at least in part) encrypted or otherwise secured***. These containers ***may contain electronic content products or other electronic information*** and some or all of their associated permissions (control) information. These container objects may be distributed along pathways involving content providers and/or content users. They may be securely moved among nodes of a Virtual Distribution Environment (VDE) arrangement, which nodes operate VDE foundation software and execute control methods to enact electronic information usage control and/or administration models. The containers delivered through use of the preferred embodiment of the present invention may be employed both for distributing VDE control instructions (information) and/or to encapsulate and electronically distribute content that has been at least partially secured.

’900 Patent col.13 ll.50–67 (emphasis added). Thus, a container may be secured other than by encryption, a container may “contain” information and is not necessarily coextensive with the information, and a container may include information other than “content.” The ’900 Patent further provides:

> ***The “container” concept is a convenient metaphor used to give a name to the collection of elements required to make use of content or to perform an administrative-type activity***. Container 302 typically includes identifying information, control structures and content (e.g., a property or administrative data). The term “container” is often (e.g., Bento/OpenDoc and OLE) used to describe a collection of information stored on a computer system’s secondary storage system(s) or accessible to a computer system over a communications network on a “server’s” secondary storage system. The “container” 302 provided by the preferred embodiment is not so limited or restricted. In VDE 100, there is no requirement that this information is stored together, received at the same time, updated at the same time, used for only a single object, or be owned by the same entity. Rather, in VDE 100 the container concept is extended and generalized to include real-time content and/or online interactive content passed to an electronic appliance over a cable, by broadcast, or communicated by other electronic communication means.

’900 Patent col.134 ll.39–58. Thus, “container” has a customary meaning in art, it refers to a collection of information elements, a data structure, that may be related to but is not necessarily content.

In the context of these teachings, the Court rejects Defendants' proposed construction as improperly narrow. The term would benefit from some explication, however, given the breadth of the constituent words and that "container" is used metaphorically in the art.

Accordingly, the Court construes "secure electronic container" as follows:

- "secure electronic container" means "data structure that secures and includes or consists of content or other information."

C. "user's computing device" and "computing device"

Disputed Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
"user's computing device" • '342 Patent Claim 1	plain and ordinary meaning	same computer running both the application program [rendering application] and the rights management program [engine]
"computing device" • '106 Patent Claim 17		

Because the parties' arguments and proposed constructions with respect to these terms are related, the Court addresses the terms together.

The Parties' Positions

Plaintiff submits: The computing-device terms are used in the '342 and '106 Patents according to their plain and ordinary meanings; namely, to refer to electronic components or systems that perform computations. The patents provide examples, such as personal computers, servers, phones, and computer systems. Notably, a "computing device" is not limited to a single computer. Dkt. No. 88 at 11–13.

In addition to the claims themselves, Plaintiff cites the following intrinsic and extrinsic evidence to support its position: **Intrinsic evidence**: '342 Patent col.16 ll.3–43; '266 Patent[6] File Wrapper June 8, 2006 Amendment and Response to Office Action Filed with RCE at 10–11 (Plaintiff's Ex. S, Dkt. No. 88-19 at 12–13). **Extrinsic evidence**: *The American Heritage College Dictionary* at 380 (3d ed. 1997) (Plaintiff's Ex. O, Dkt. No. 88-15 at 5).

Defendants respond: The computing-device terms are limited to a single computer because a multiple-computer system was disclaimed during prosecution of the parent application to the '342 and '106 Patents. Specifically, the term "computing device" was added to the claims to express that a single computer runs both an application and a rights-management program, as distinct from the prior art in which the application and rights-management program run on different computers. Dkt. No. 101 at 11–14.

In addition to the claims themselves, Defendants cite the following **intrinsic evidence** to support their position: '106 Patent fig.9, col.16 ll.35–51, col.16 ll.54–59; '266 Patent File Wrapper December 8, 2005 Office Action at 4 (Defendants' Ex. 2, Dkt. No. 101-2 at 2–21, 6), June 8, 2006 Amendment and Response to Office Action Filed with RCE at 2–3, 10 (Defendants' Ex. 2, Dkt. No. 101-2 at 25–38, 26–27, 34), August 22, 2006 Office Action at 3–4 (Defendants' Ex. 2, Dkt. No. 101-2 at 39–60, 42–43); *Peinado*[7] at fig.1 (Defendants' Ex. 3, Dkt. No. 101-3); *England*[8] at fig.2, col.10 ll.26–36 (Defendants' Ex. 4, Dkt. No. 101-4).

[6] U.S. Patent No. 7,213,266. The '342 and '106 Patents are related to the '266 Patent through one or more continuation applications. '342 Patent, at [63] Related U.S. Application Data; '106 Patent, at [63] Related U.S. Application Data.
[7] U.S. Patent No. 6,775,655.
[8] U.S. Patent No. 6,820,063.

Plaintiff replies: Defendants' proposed construction threatens to improperly limit "computing device" to a "single, standalone personal computer," which would exclude described embodiments of the computing device. Dkt. No. 103 at 5–6.

Plaintiff cites further **intrinsic evidence** to support its position: '342 Patent fig.9, col.16 ll.49–51; '106 Patent col.35–39.

Analysis

The issue in dispute appears to be whether "computing device" in Claim 1 of the '342 Patent and Claim 17 of the '106 Patent is necessarily a single computer. It is not.

The claims at issue specify that in Claim 1 of the '342 Patent the same user's computing device executes/runs both the application and rights management program and that in Claim 17 of the '106 Patent the same computing device executes both the rendering application and the rights management engine. Specifically, Claim 1 of the '342 Patent provides (with emphasis added):

> 1. A method for managing the use of electronic content at a user's computing device, the method including:
>
> ***executing an application program on the user's computing device***, the application program being capable of rendering electronic content, the application program having at least a first digital certificate associated therewith, the first digital certificate being generated by or on behalf of a first entity comprising an association of one or more content providers, the first digital certificate being associated with the application program if the application program meets certain predefined criteria set by the association, the predetermined criteria including that the application program will handle the electronic content with at least a predefined level of security;
>
> requesting the application program to render a piece of electronic content, the piece of electronic content having at least a second digital certificate associated therewith, the second digital certificate being generated by or on behalf of a second entity different from the first entity, and the piece of electronic content further having associated therewith at least one electronic rule, the at least one electronic rule including data specifying one or more conditions associated with rendering the piece of electronic content, the one or more conditions including a condition that the piece of electronic content may be rendered by an application program having the first digital certificate associated therewith;

verifying, at the user's computing device, the association of the second digital certificate with the piece of electronic content;

using ***a rights management program running on the user's computing device*** to examine the data included in the at least one electronic rule and to determine that the piece of electronic content may be rendered by an application program having the first digital certificate associated therewith;

verifying the association of the first digital certificate with the application program using the rights management program; and

rendering the piece of electronic content using the application program, wherein the piece of electronic content comprises an authorizing document, and the second entity associates the second digital certificate with the authorizing document if the authorizing document origi- nated from a certified entity.

Claim 17 of the '106 Patent similarly provides (with emphasis added):

17. A method for managing the use of electronic content at a computing device, the method including:

receiving a piece of electronic content;

receiving, separately from the piece of electronic content, data specifying one or more conditions associated with rendering the piece of electronic content, the one or more conditions including a condition that the piece of electronic content be rendered by a rendering application associated with a first digital certificate;

executing a rendering application on the computing device, the rendering application being associated with at least the first digital certificate, the first digital certificate having been generated by a first entity based at least in part on a determination that the rendering application will handle electronic content with at least a predefined level of security;

requesting, through ***a rights management engine executing on the computing device***, permission for the rendering application to render the piece of electronic content;

determining, using the rights management engine, whether the one or more conditions specified by the data have been satisfied;

decrypting the piece of electronic content; and

rendering the decrypted piece of electronic content using the rendering application.

Given that the claims clearly express that the applications and right management program/engine are running on the same computing device, there is no need to include that in a construction of "user's computing device" or "computing device." Indeed, the fact that these execution-location limitations are expressed in the claims suggests that they are not inherent attributes of the computing-device limitations.

The ’342 and ’106 Patents further explain that the rendering application and rights management engine may, alternatively, be on the same system or distributed across multiple remote systems. For example, the patents provide:

> It should be appreciated that the system and relationships shown in FIG. 6 can be implemented in any suitable fashion. For example, ***rendering application 614, rights management engine 610, and content 604 may all be stored on the same system*** (e.g., in the memory of a personal computer), or ***may be distributed between multiple systems*** (e.g., rights management engine 610 and/or content 604 might be located on a system that is ***remote*** from the system on which rendering application 614 is running). Moreover, as shown in FIG. 6, content object 604, rules 602, and certificates 606 may be packaged together in a secure electronic container 608 that is accessible to the rights management engine 610. Alternatively, some or all of these objects may be packaged and/or delivered separately.

’342 Patent col.11 ll.41–54 (emphasis added). Again, this counsels against defining “computing device” as necessarily executing both the rendering application and rights management engine. And this explains that computer systems remote from each other are distinct, they are not the same computing device.

The patents provide further, structural, description of the “computing device” that suggests a broad meaning. For example, the patents teach:

> FIG. 9 shows an example of a computer system 900 that can be used to practice embodiments of the present invention. ***Computer system 900 may comprise a general-purpose computing device such as a personal computer or network server, or a specialized computing device such as a cellular telephone, personal digital assistant, portable audio or video player, television set-top box, kiosk, or the like.*** Computing device 900 will typically include a processor 902, memory 904, a user interface 906, a port 907 for accepting removable memory 908, a network interface 910, and a bus 912 for connecting the aforementioned elements. The operation of computing device 900 will typically be controlled by processor 902 operating under the guidance of programs stored in memory 904. Memory 904 will generally include both high-speed random-access memory (RAM) and non-volatile memory such as a magnetic disk and/or flash EEPROM. Some portions of memory 904 may be restricted, such that they cannot be read from or written to by other components of the computing device 900. Port 907 may comprise a disk drive or memory slot for accepting computer-readable media such as floppy diskettes, CD-ROMs, DVDs, memory cards, other magnetic or optical media, or the like. Network interface 910 is typically operable to provide a connection between computing device 900 and other computing devices (and/or networks of computing

> devices) via a network 920 such as the Internet or an intranet (e.g., a LAN, WAN, VPN, etc.). In some embodiments, computing device 900 includes a secure processing unit 903 such as that described in the '900 patent. A secure processing unit can help enhance the security of sensitive operations such as key management, signature verification, and other aspects of the rights management process.

'342 Patent col.16 ll.36–67 (emphasis added). Thus, "computing device" broadly encompasses devices such as personal computers, network servers, cellular telephones, personal digital assistants, portable audio or video players, television set-top boxes, kiosks, and the like. This teaching counsels against construing the term as "computer," which does not clearly encompass a cellular telephone or portable audio or video player and like devices. Further, this sets forth that distinct devices may be connected through a network "such as the Internet or an intranet," meaning that distinct devices do not necessarily become a single device when networked together. Combined with the teaching regarding "remote" systems, this further suggests that devices that are remote from each other are distinct.

Finally, the prosecution history of a related patent provides context informing the meaning of "computing device." Specifically, in prosecution of the '266 Patent, the applicant distinguished a prior-art reference (*Peinado*) on the grounds that *Peinado* teaches distributing execution of an application program and a rights management program, the application program to one computing device, the rights management program to another computing device, remote from the first, while the claims recited that both executed on the user's computing device:

> With regard to claim 1, Applicants respectfully submit that Peinado fails to teach. *inter alia,* using ***a rights management program running on a user's computing device*** to verify the association of a first digital certificate with an ***application program that is also executing on the user's computing device***, and verifying the association of a second digital certificate with a piece of electronic content which the application program has been requested to render.
>
> Instead, as understood Peinado describes ***a remote license server*** that may check a certificate associated with a component of a DRM system running on a user's system (see, e.g., Peinado at column 18, lines 54-67). ***Peinado does not teach that the DRM system itself would check a digital certificate associated with an***

> ***application program <u>running on the same computer system</u> as the DRM system***. Moreover, unlike claim 1, Peinado also fails to teach the association of a digital certificate with the piece of content that is to be rendered by the application program, or the verification of that digital certificate. Applicants have amended claim 1 to further clarify these distinctions.

'266 Patent File Wrapper June 8, 2006 Amendment and Response to Office Action Filed with RCE at 10, Dkt. No. 101-2 at 34. Thus, in *Peinado*, the license server and the user's system are distinct devices, they are remote from each other. As described in *Peinado*, the "license server" and user (DRM) system are distinct systems communicating via a network:

> Assuming that the location for obtaining a license 16 is in fact a license server 24 on a network, the license evaluator 36 then establishes a network connection to such license server 24 based on the web site or other site information and then sends a request for a license 16 from such connected license server 24 (steps 701, 703). In particular, once the DRM system 32 has contacted the license server 24 such DRM system 32 transmits appropriate license request information 36 to such license server 24.

Peinado at col.18 ll.49–57. The prosecution history reinforces the plain meaning of the claims in that distributing execution of the application program and rights management program to two devices, one to the user's device, the other to a remote server, is not the same a executing both the application program and rights management program on the user's device. It does not, however, justify rewriting "computing device" as "computer." Importantly, it does not mandate, as Defendants' argue, that a system of computing components somehow networked together is necessarily not a "computing device" by virtue of the network interconnects. Ultimately, whether a particular accused or prior-art computing structure qualifies as a "computing device" is an issue of fact for the jury.

Accordingly, the Court determines that these terms have their plain and ordinary meanings without the need for further construction.

D. "electronic appliance"

Disputed Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
"electronic appliance" • '157 Patent Claims 53, 69, 86 • '158 Patent Claim 4	one or more electronic components designed or configured to perform one or more specialized tasks	an electronic device designed to perform one or more specialized tasks

The Parties' Positions

Plaintiff submits: "Electronic appliance" is not limited to a discrete device or to any particular physical form, but rather encompasses a collection or system of interconnected electronic components that together are configured or designed to perform a task. The '157 and '158 Patents indicate the breadth of this term through description of a variety of electronic appliances ranging from hand-held devices to mainframe computers, and including systems of devices such as printers, keyboards, scanners, and displays. "Indeed, the claims do not recite 'electronic appliance' as a substantive limitation, but as a term for any equipment that comprises or performs the limitations." Dkt. No. 88 at 13–16.

In addition to the claims themselves, Plaintiff cites the following **intrinsic evidence** to support its position: '157 Patent fig.7, col.4 ll.62–64, col.33 ll.24–28, col.59 ll.1–14, col.59 ll.45–49, col.79 ll.38–44, col.223 ll.29–33, col.273 ll.7–12.

Defendants respond: The '157 and '158 Patents explain that "electronic appliance" refers to a "kind of electrical or electronic device" (quoting '157 Patent col.58 ll.58–67). The patents describe the inventions as directed to improving the "interoperability" of appliances, and thus it is important to clarify the boundary of an electronic appliance in order to understand how the appliances interoperate. In other words, "it is important to know when one appliance ends and another begins." While the patents describe an appliance which includes multiple devices (depicted in Figure 7),

the included devices are simply those "that are 'normally used within an electronic appliance' so that the appliance 'may communicate with the outside world,' and they are not excluded by Defendants' construction" (quoting *id*. at col.59 ll.1–14). Dkt. No. 101 at 14–17.

In addition to the claims themselves, Defendants cite the following **intrinsic evidence** to support their position: '157 Patent col.1 ll.52–56, col.8 ll.55–63, col.58 ll.58–67, col.59 ll.1–14, col.60 l.67 – col.61 l.3, col.157 ll.61–64, col.210 ll.30–33, col.222 ll.21–24, col.223 ll.14–15, col.223 ll.17–18.

Plaintiff replies: The patents explain that an "electronic appliance" "may be practically any kind of electrical or electronic device," not that the appliance necessarily is a device (quoting '157 Patent col.58 ll.58–59). And the patents describe embodiments of appliances that include multiple devices that would improperly be excluded by Defendants' proposed construction. The patents also identify a mainframe computer as an electronic appliance yet distinguish such a computer from a "device," further indicating that "electronic appliance" is not limited to a device. Dkt. No. 103 at 6–7.

Plaintiff cites further **intrinsic evidence** to support its position: '157 Patent col.58 ll.58–59.

Analysis

The issue in dispute distills to whether "electronic appliance" should be rewritten as "electronic device." It should not.

The claims provide significant context that informs the meaning of "electronic appliance." For instance, Claim 69 of the '157 Patent provides (with emphasis added):

> 69. A method performed by an ***electronic appliance comprising*** ***a processor and a memory encoded with program instructions that, when executed by the processor, cause the electronic appliance to perform the method, the method comprising***:
>
> receiving, by the electronic appliance, a first piece of electronic content, the first piece of electronic content being encrypted at least in part;

> receiving, by the electronic appliance, separately from the first piece of electronic content, a first key, the first key being associated with the first piece of electronic con- tent, and the first key being encrypted at least in part;
> decrypting, by the electronic appliance, the first key using (a) a second key and (b) a secure processing unit running on the electronic appliance, the second key being stored in memory of the secure processing unit;
> decrypting, by the electronic appliance, the first piece of electronic content using, at least in part, the first key; receiving, by the electronic appliance, separately from the first piece of electronic content, and via separate delivery, a first electronic object, the first electronic object specifying one or more permitted or prohibited uses of the first piece of electronic content;
> receiving, by the electronic appliance, a request to use the first piece of electronic content; and
> selectively granting, by the electronic appliance, the request in accordance with the first electronic object.

Thus, the claim itself defines the electronic appliance: it is composed of a processor and memory encoded with specific instructions, the specification of which instructions constitutes the bulk of the claim. The other claims at issue provide similar context: '157 Patent Claim 53 recites: "An electronic appliance comprising: a first processing unit, a second processing unit…, and computer readable media … storing … software comprising programming [for performing functions]." '157 Patent Claim 69 recites: "an electronic appliance comprising a processor and a memory encoded with program instructions that, when executed by the processor, cause the electronic appliance to perform the method, the method comprising: …." '157 Patent Claim 86 recites: "the electronic appliance comprising a processor and a memory encoded with program instructions that, when executed by the processor, cause the electronic appliance to perform the method, the method comprising: …." And '158 Patent Claim 4 recites: "an electronic appliance comprising a processor and a memory encoded with program instructions that, when executed by the processor, cause the processor to perform the method, the method comprising: …."

While the claims expressly set forth the essential structure of the "electronic appliance," the patents further provide that an "electronic appliance" may include a variety of devices, or it may be a unitary device. For example, the patents explain:

> FIG. 7 shows an example of an electronic appliance 600 including SPU 500. ***Electronic appliance 600 may be practically any kind of electrical or electronic device***, such as:
>
> a computer
>
> a T.V. "set top" control box
>
> a pager
>
> a telephone
>
> a sound system
>
> a video reproduction system
>
> a video game player
>
> a "smart" credit card.

'157 Patent col.58 ll.57–67 (emphasis added). The patents also provide:

> Electronic appliance 600 in this example ***may include a keyboard or keypad 612, a voice recognizer 613, and a display 614***. A human user can input commands through keyboard 612 and/or voice recognizer 613, and may view information on display 614. Appliance 600 ***may communicate*** with the outside world through any of the ***connections/devices normally used within an electronic appliance***. The connections/ devices shown along the bottom of the drawing are examples:
>
> a "modem" 618 or other telecommunications link;
>
> a CD ROM disk 620 or other storage medium or device; a printer 622;
>
> broadcast reception 624;
>
> a document scanner 626; and
>
> a "cable" 628 connecting the appliance with a "network."

Id. at col.59 ll.1–14 (emphasis added); *see also, id*. at col.222 ll.18–24 ("It may also be advantageous to provide multiple VDE electronic appliances 600 within the same workstation or other electronic appliance 600. For example, an electronic appliance 600 may include multiple electronic appliances 600 each of which have a SPU 500 and are capable of performing VDE functions."); *id*. at col.223 ll.29–33 ("Referring back to FIG. 7, scanner 626, modem 618,

telecommunication means 624, keyboard 612 and/or voice recognition box 613 could each comprise a VDE electronic appliance 600 having its own SPU 500."). Thus, "electronic appliance" is better described as a system of components, each which may be a device, and which together may comprise a device, rather than as necessarily a "device."

Accordingly, the Court construes "electronic appliance" as follows:

- "electronic appliance" means "one or more electronic components designed or configured to together perform one or more specialized tasks."

E. "rule" and "control information"

Disputed Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
"rule" • '158 Patent Claim 4	information specifying one or more permitted or prohibited uses	information, such as executable code or associated data, related to controlling use of a digital file
"control information" • '304 Patent Claim 24		

Because the parties' arguments and proposed constructions with respect to these terms are related, the Court addresses the terms together.

The Parties' Positions

Plaintiff submits: The terms "rule" and "control information" do not encompass anything simply "related to controlling use of a digital file." Rather, according to their ordinary meanings and their usage in the '304 and '158 Patents, the terms are plainly narrower. The terms refer to information that governs the use of protected material by specifying the permitted or prohibited uses of such material. For example, a "rule" or "control information" may specify who may use the material, how they may use it, and the cost for using it. While Plaintiff successfully argued for a different construction of "control" in a related patent before the Northern District of California in *Intertrust Techs. Corp. v. Microsoft Corp.*, 4:01-cv-01640-SBA (the "*Microsoft Case*"), the

presently proposed construction is substantively consistent with the previously-adopted construction,[9] and is simpler than the previous construction. In arguing to the California court that "control" encompasses data, and is not limited to executable code, Plaintiff imprecisely paraphrased the disclosure of the patents there at issue in a way that improperly suggests "control" (and thus "control information") encompasses a simple "key." The patents in the *Microsoft Case*—and the '304 and '158 Patents here—note that key information, rather than simply a key, may be control information (citing '158 Patent col.164 l.60 – col.165 l.3 (noting "associated critical key and/or other control information")). Dkt. No. 88 at 16–20.

In addition to the claims themselves, Plaintiff cites the following intrinsic and extrinsic evidence to support its position: **Intrinsic evidence**: '158 Patent col.6 ll.23–29, col.18 ll.12–15, col.31 ll.51–56, col.33 ll.11–15, col.52 ll.23–67, col.54 ll.23–26, col.55 ll.2–9, col.56 ll.55–63, col.164 l.60 – col.165 l.3, col.201 ll.33–55. **Extrinsic evidence**: *Encarta World English Dictionary* at 1567 (1999) (Plaintiff's Ex. N, Dkt. No.88-14 at 4); *The American Heritage College Dictionary* at 303 (3d ed. 1997) (Plaintiff's Ex. O, Dkt. No. 88-15 at 4); *Webster's New World College Dictionary* at 1254 (4th ed. 2001) (Plaintiff's Ex. P, Dkt. No. 88-16 at 4); *Collins English Dictionary* at 1345 (4th ed. 1998) (Plaintiff's Ex. Q, Dkt. No. 88-17 at 4).

Defendants respond: The term "control information" (and thus "rule") is defined in the '304 and '158 Patents more broadly than Plaintiff proposes. Specifically, the patents provide: "VDEF

[9] Plaintiff there proposed, and the California court adopted, that "control" means "[i]nformation and/or programming controlling operations on or use of resources (e.g., content) including (a) permitted, required, or prevented operations, (b) the nature or extent of such operations, or (c) the consequences of such operations." *Intertrust Techs. Corp. v. Microsoft Corp.*, 275 F. Supp. 2d 1031, 1060 (N.D. Cal. 2003) (the "*Microsoft Order*"). The California court addressed "control" as used in U.S. Patents No. 5,982,891, No. 6,185,683, and No. 6,253,193 and noted that "control is equivalent to control information." *Id*. at 1037, 1059–60. The '304 and '158 Patents are related to the patents in the *Microsoft Case* through a series of continuation applications. *See, e.g.*, '158 Patent, at [63] Related U.S. Application Data.

load modules, associated data, and methods form a body of information that for the purposes of the present invention are called 'control information'" (quoting '304 Patent col.18 ll.56–59). Plaintiff's proposed construction fails to encompass "associated data." Thus, "control information" expressly includes executable code (the load modules), associated data, and the control methods constructed from executable code and associated data. This includes "information specifying one or more permitted or prohibited uses" but it is not limited to this—it also includes related information such as a key. Indeed, Plaintiff admitted in the *Microsoft Case* that "a key is control information" (quoting Intertrust's Opening Claim Construction Brief at 17–18, *Microsoft Case* (N.D. Cal. Mar. 17, 2003), Dkt. No. 101-5 at 29–30). And the '304 and '158 Patents describe disabling "associated critical key and/or other control information" and that the "key information may be the actual decryption key" (quoting '304 Patent col.172 ll.4–19, col.196 ll.23–26). Thus, the patents state that a key is control information. Dkt. No. 101 at 18–22.

In addition to the claims themselves, Defendants cite the following **intrinsic evidence** to support their position: '304 Patent col.18 ll.56–59, col.26 ll.12–15, col.29 ll.47–48, col.33 l.35, col.56 ll.58–59, col.59 ll.35–52, col.71 ll.2–3, col.135 ll.11–13, col.172 ll.4–19, col.196 ll.23–26, col.265 l.61 – col.266 l.20, col.306 ll.60–62, col.309 ll.6–9; '304 Patent File Wrapper April 2, 2003 Updated Notice Regarding Related Litigation, Intertrust's Opening Claim Construction Brief at 17–18, *Microsoft Case* (N.D. Cal. Mar. 17, 2003) (Defendants' Ex. 5, Dkt. No. 101-5 at 29–30).

Plaintiff replies: The passage in the patents that Defendants contend defines "control information" does not. Rather, the passage "describes several forms of 'control information,' all covered by" Plaintiff's proposed construction. The patents further distinguish between control information and keys, describing them in the disjunctive: "control information … and/or keys" (quoting '158 Patent col.27 ll.4–9). Further, Defendants improperly equate keys and other

information described in the patent as related to or used by rules/control information with the rules/control information themselves. Dkt. No. 103 at 7–8.

Plaintiff cites further **intrinsic evidence** to support its position: '158 Patent col.27 ll.4–9, col.57 l.38 – col.58 l.7, col.161 l.34 – col.165 l.7, col.202 ll.3–12, col.210 ll.17–33.

Analysis

The issue in dispute distills to whether "rule" and "control information" in the '304 and '158 Patents are narrowly limited to information specifying one or more permitted or prohibited uses of protected material or broadly encompass any information related to controlling use of protected material. The Court rejects both proposed constructions and finds the proper construction somewhere between these two proposals. At the hearing, the Court proposed the constructions adopted below and the parties agreed to the proposed constructions without argument.

The claims provide significant context that informs the meaning of "control information"/ "rule." For instance, Claim 24 of the '304 Patent provides (with emphasis added):

> 24. A method for monitoring use of a digital file at a computing system, the method comprising:
> receiving the digital file;
> receiving a first entity's ***control information*** separately from the digital file;
> using the first entity's ***control information to govern, at least in part, a use of the digital file at the computing system***; and
> reporting information relating to the use of the digital file to the first entity;
> wherein at least one aspect of the computing system is designed to impede the ability of a user of the computing system to tamper with at least one aspect of the computing system's performance of one or more of said using and reporting steps.

This expresses that control information is used to "govern" use of the digital file. On its face, this "control information" is broader than simply specifying permitted or prohibited uses. A plain reading of this claim counsels against Plaintiff's proposed construction. Claim 4 of the '158 Patent similarly provides (with emphasis added):

> 4. A method utilizing an electronic appliance comprising a processor and a memory encoded with program instructions that, when executed by the processor, cause the processor to perform the method, the method comprising:
> receiving, at the electronic appliance, an electronic content item, the electronic content item being encrypted at least in part;
> storing the electronic content item in memory of the electronic appliance;
> receiving, at the electronic appliance, independently from the electronic content item via separate delivery and protected separately from the electronic content item, ***a rule specifying one or more permitted uses of the electronic content item***;
> receiving, at the electronic appliance, a request to use the electronic content item;
> ***determining that the requested use of the electronic content item corresponds to a permitted use of the electronic content item specified in the rule***; and
> using, at least in part, a decryption key to decrypt the electronic content item, the decryption key being stored in a secure processing unit contained in the electronic appliance.

The "rule" here appears coextensive with Plaintiff's proposed construction. Specifically, a use that is not "permitted" according to the "rule" would necessarily not correspond to a permitted use and would therefore be a prohibited use. This suggests that Plaintiff's proposed construction renders "specifying one or more permitted uses" in the claim superfluous. This too counsels against Plaintiff's proposed construction.

The '304 and '158 Patents set forth a definition of "control information." Specifically, the patents provide:

> VDE supports a general purpose foundation for secure transaction management, including ***usage control, auditing, reporting, and/or payment***. This general purpose foundation is called "VDE Functions" ("VDEFs"). VDE also supports a collection of "atomic" application elements (e.g., ***load modules***) that can be selectively aggregated together to form various VDEF capabilities called ***control methods*** and which serve as VDEF applications and operating system functions. When a host operating environment of an electronic appliance includes VDEF capabilities, it is called a "Rights Operating System" (ROS). ***VDEF load modules, associated data, and methods form a body of information that for the purposes of the present invention are called "control information."*** VDEF control information may be specifically associated with one or more pieces of electronic content and/or it may be employed as a general component of the operating system capabilities of a VDE installation.

> VDEF transaction control elements ***reflect and enact*** content specific and/or more generalized administrative (for example, general operating system) ***control information***.

'304 Patent col.18 ll.46–65 (emphasis added); *see also*, '158 Patent col.17 l.66 – col.18 l.15 (same). The phrase "VDEF load modules, associated data, and methods form a body of information that for the purposes of the present invention are called 'control information'" is definitional, not exemplary. In context, this passage explains each of the elements of the definition: "load modules," "associated data," and "methods." The "associated data" is data associated with the load modules. The "methods" are the control methods formed from the load modules. Collectively, these can be fairly and accurately represented as "information and/or programming controlling operations on or use of resources" as set forth in the *Microsoft Order*. 275 F. Supp. 2d at 1059–60.

Notably, the patents do not suggest that information simply "related" to control is "control information," as Defendants propose. Rather, "control information" is something that can be enacted, information that is for controlling. This is further explained in an exemplary embodiment:

> In the FIG. 5A example, container 302 may also contain "rules and controls" in the form of:
>
> a "Permissions record" 808;
>
> "budgets" 308; and
>
> "other methods" 1000.
>
> FIG. 5B gives some additional detail about permissions record 808, budgets 308 and other methods 1000. The "permissions record" 808 specifies the rights associated with the object 300 such as, for example, who can open the container 302, who can use the object's contents, who can distribute the object, and what other control mechanisms, must be active. For example, permissions record 808 may specify a user's rights to use, distribute and/or administer the container 302 and its content. Permissions record 808 may also specify requirements to be applied by the budgets 308 and "other methods" 1000. Permissions record 808 may also contain security related information such as scrambling and descrambling "keys."
>
> "Budgets" 308 shown in FIG. 5B are a special type of "method" 1000 that may specify, among other things, limitations on usage of information content 304, and

> how usage will be paid for. Budgets 308 can specify, for example, how much of the total information content 304 can be used and/or copied. The methods 310 may prevent use of more than the amount specified by a specific budget.
>
> "Other methods" 1000 define basic operations used by "rules and controls." Such "methods" 1000 may include, for example, how usage is to be "metered," if and how content 304 and other information is to be scrambled and descrambled, and other processes associated with handling and controlling information content 304.

'304 Patent col.59 ll.35–65. All these examples of control information appear more than merely related to control, but actually are for control. These examples also do more than simply specify permitted or prohibited uses. For example, "how usage will be paid for," "how much of the total information content 304 can be used and/or copied," and "how usage is to be 'metered'" do not simply specify permitted or prohibited uses.

Plaintiff's representations in the *Microsoft Case* do not broaden the scope of "control information" to encompass anything simply related to control. Specifically, Plaintiff represented the evidence as follows:

> 8(F) In this embodiment, the additional memory may be provided by additional one or more integrated circuits that can be contained within a secure enclosure, such as a tamper resistant metal container or some form of a chip pack containing multiple integrated circuit components, and which impedes and/or evidences tampering attempts; and/or disables a portion or all of SPU 500 or ***associated critical key and/or other control information*** in the event of tampering. '193 patent at 169:5–13.

PLR 4-3(b) – Identification of Supporting Evidence at 25, *Microsoft Case* (emphasis added) (here, Dkt. No. 88-24 at 4). Plaintiff went on to use and characterize this evidence as follows:

> Control information can consist of programming (e.g., load modules) or data. See, e.g., 8(D) (load modules, data and methods), ***8(F) (a key is control information)***, 8(G) (executable programming such as load modules), 8(H) (use of "and/or" making it clear that information can consist of methods, or load modules, or mediating data or component assemblies, 8(I) (software and parameter data).

Intertrust's Opening Claim Construction Brief at 17–18, *Microsoft Case* (N.D. Cal. Mar. 17, 2003) (emphasis added) (here, Dkt. No. 101-5 at 29–30). Fairly read, Plaintiff did not represent that any

key is control information, rather it represented that "a key" is control information, referring back to the "associated critical key" described in the '193 Patent at column 169, lines 5 through 13. On this record, the Court will not rule as a matter of claim construction that all keys are control information, as Defendants suggest.

Accordingly, the Court rejects both Plaintiff's and Defendants' proposed constructions and construes "rule" and "control information" as follows:

- "rule" means "information and/or programming controlling operations on or use of resources"; and
- "control information" means "information and/or programming controlling operations on or use of resources."

F. "load module"

Disputed Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
"load module" • '721 Patent Claim 9	executable program code and/or data used by executable program code	executable code such as a computer program or an applet

The Parties' Positions

Plaintiff submits: The '721 Patent explains that "load module" encompasses both executable code and associated data. For example, the patent provides that "the load module preferably comprises one or more computer instructions **and/or data elements**. … For example, load module [] may comprise all or part of an executable computer program **and/or associated data**" (quoting '721 Patent col.8 ll.18–29 (Plaintiff's emphases and modifications)). Claim differentiation further indicates that "load module" is not limited to executables. Specifically, Claims 9 and 29 are distinct only in that Claim 9 recites "load module" whereas Claim 29 recites "executable." Defendants'

proposed construction would improperly erase any distinction between these two claims. Dkt. No. 88 at 20–22.

In addition to the claims themselves, Plaintiff cites the following **intrinsic evidence** to support its position: '721 Patent col.3 ll.19–35, col.8 ll.18–29.

Defendants respond: As described in the '721 Patent and as set forth in the claims, a "load module" is necessarily executable. For instance, Claim 9 recites "executing the load module" which necessitates that the "load module" is executable. In another example, the patent explains that "[f]or a load module to operate and interact as intended, it ***must execute*** …" (quoting '721 Patent col.3 ll.32–35 (Defendants' emphasis and modifications)). Similarly, the patent repeatedly refers to "load modules or other executables." And Plaintiff itself represented load modules as executable programming in the *Microsoft Case*. This does not mean that a load module may not include data, only that it may not consist of only data. Dkt. No. 101 at 22–24.

In addition to the claims themselves, Defendants cite the following intrinsic evidence to support their position: '721 Patent col.1 ll.21–28, col.2 ll.29–38, col.3 ll.32–35, col.4 ll.55–65, col.5 l.3, col.5 ll.14–17, col.5 l.27, col.5 ll.41–45, col.5 ll.63–64, col.6 l.1, col.6 ll.5–11, col.6 ll.17–24, col.6 ll.42–43, col.6 l.51, col.6 ll.61–67, col.7 ll.4–17, col.20 ll.1–5, col.20 ll.12–19; '304 Patent File Wrapper April 2, 2003 Updated Notice Regarding Related Litigation, Intertrust's Opening Claim Construction Brief at 18, *Microsoft Case* (N.D. Cal. Mar. 17, 2003) (Defendants' Ex. 5, Dkt. No. 101-5 at 30).

Plaintiff replies: The '721 Patent expressly describes that "load module" may be executable code "and/or" associated data. That Claim 9 may otherwise indicate that the load module is executed is not reason to limit "load module" to executable code, which would contradict the

description. And other claims include "load module" without requiring that it be executed. Dkt. No. 103 at 8–9.

Plaintiff cites further **intrinsic evidence** to support its position: '304 Patent File Wrapper April 2, 2003 Updated Notice Regarding Related Litigation, Intertrust's Opening Claim Construction Brief at 18, *Microsoft Case* (N.D. Cal. Mar. 17, 2003) (Defendants' Ex. 5, Dkt. No. 101-5 at 30).

Analysis

The issue in dispute distills to whether "load module" necessarily includes executable code. It does. At the hearing, the parties agreed to the construction adopted below.

Claim 9 of the '721 Patent provides some useful context for interpreting "load module" (with emphasis added):

> 9. A method of distinguishing between trusted and untrusted load modules comprising:
> (a) receiving ***a load module***,
> (b) determining whether the ***load module has an associated digital signature***,
> (c) if the load module has an associated digital signature, authenticating the digital signature using at least one public key secured behind a tamper resistant barrier and therefore hidden from the user; and
> (d) conditionally ***executing the load module*** based at least in part on the results of authenticating step (c).

The Court agrees that the load module of Claim 9 is necessarily executable, else "executing the load module" would not be possible.

As described in the '721 Patent, the "load module" is necessarily executable. For example, the patent provides:

> The Ginter et al. patent disclosure describes, among other things, techniques for providing a secure, tamper resistant execution spaces within a "protected processing environment" for computer programs and data. The protected processing environment described in Ginter et al. may be hardware-based, software-based, or a hybrid. ***It can execute computer code the Ginter et al. disclosure refers to as "load modules."*** See, for example, ***Ginter et al. FIG. 23 and corresponding text***. These load modules-which can be transmitted from remote

> locations within secure cryptographic wrappers or "containers"—are used to perform the basic operations of the "virtual distribution environment." ***Load modules may contain algorithms, data, cryptographic keys, shared secrets, and/or other information that permits a load module to interact with other system components*** (e.g., other load modules and/or computer programs operating in the same or different protected processing environment). ***For a load module to operate and interact as intended, it must execute without unauthorized modification*** and its contents may need to be protected from disclosure.

'721 Patent col.3 ll.16–35 (emphasis added). This states that load modules "must execute." The patent elsewhere groups "load modules" with "other executables":

> The present invention provides improved techniques for protecting secure computation and/or execution spaces (as one important but non-limiting example, the protected processing environments as disclosed in Ginter et al) from unauthorized (and potentially harmful) ***load modules or other "executables" or associated data***. In one particular preferred embodiment, these techniques build upon, enhance and/or extend in certain respects, the load module security techniques, arrangements and systems provided in the Ginter et al. specification.
>
> In accordance with one aspect provided by the present invention, one or more trusted verifying authorities validate ***load modules or other executables*** by analyzing and/or testing them. A verifying authority digitally "signs" and "certifies" those ***load modules or other executables*** it has verified (using a public key based digital signature and/or certificate based thereon, for example).

Id. at col.4 ll.51–65 (emphasis added). Again, this states that a load module is executable.

The patent, while at times appearing to suggest that the load module may be only data, does not actually state such when read in the proper context. For example, the patent provides:

> FIG. 1 shows "load module" 54 as a complicated looking machine part for purposes of illustration only; the load module preferably comprises one or more computer instructions and/or data elements used to assist, allow, prohibit, direct, control or facilitate at least one task performed at least in part by an electronic appliance such as a computer. For example, ***load module 54 may comprise all or part of an executable computer program and/or associated data ("executable"),*** and may constitute a sequence of instructions or steps that bring about a certain result within a computer or other computation element.

Id. at col.8 ll.18–29 (emphasis added). This suggests that the "associated data" is somehow "executable" or, if not, that the load module never includes only the associated data. The *Ginter et*

al. specification referenced and incorporated into the '721 Patent provides a further description of "load module":

> Load Modules
>
> FIG. 23 is an example of a load module 1100 provided by the preferred embodiment. ***In general, load modules 1100 represent a collection of basic functions that are used for control operations***.
>
> ***Load module 1100 contains code and static data (that is functionally the equivalent of code***), and is used to perform the basic operations of VDE 100.
>
> …
>
> A load module 1100 is able to perform its function only when executed in the protected environment of an SPE 503 or an HPE 655.

'304 Patent[10] col.141 l.39 – col.142 l.3; *see also, id.* at col.29 ll.47–48 ("Said control information may include executable code (e.g., load modules) …."). This suggests that a load module is necessarily executable and that the data it may include is "functionally the equivalent" of code that can be executed.

On balance, the evidence indicates that the "load module" is necessarily executable and therefore necessarily includes executable code, while it may also include associated data.

Accordingly, the Court construes "load module" as follows:

- "load module" means "executable code and any associated data."

[10] The *Ginter et al*. specification that is incorporated into the '721 Patent refers to U.S. Application No. 08/388,107. '721 Patent col.1 ll.7–15. The '304 Patent ultimately claims priority to U.S. Application No. 08/388,107 through a series of continuation applications and thus shares the *Ginter et al*. specification. *See* '304 Patent, at [63] Related U.S. Application Data.

G. "rendering application"

Disputed Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
"rendering application" • '106 Patent Claim 17	application program that processes content for presentation	software program that plays content through an audio output (e.g., speakers) or displays content on a video output (e.g., a screen)

The Parties' Positions

Plaintiff submits: As described in the '106 Patent, a "rendering application" processes content for presentation, it does not merely play or display content. For example, the patent describes that rendering applications may process content "such as by accessing, using, moving, or otherwise manipulating the content" and by "'applying policies, rules, and/or controls to govern the use of content or the performance of events'" (quoting '106 Patent col.17 ll.5–11). Ultimately, rendering applications "*process* content prior to or during presentation by accessing and interpreting the content, applying rules and controls to govern use, sending the content to a rights management program for access clearance, manipulating the content according to user preferences … checking output drivers for integrity, and sending the final audio/visual signals to the output device(s)." In the *Microsoft Case*, Plaintiff agreed that "rendering" should be construed as "playing content through an audio output (e.g., speakers) or displaying content on a video output (e.g., a screen)." But that was for "rendering" in an unrelated patent, and it is not inconsistent with Plaintiff's currently proposed construction of "rendering application." Dkt. No. 88 at 22–24.

In addition to the claims themselves, Plaintiff cites the following **intrinsic evidence** to support its position: '106 Patent col.2 ll.18–19, col.2 ll.21–23, col.4 ll.21–25, col.5 ll.48–53, col.10 ll.8–11, col.10 ll.18–19, col.10 ll.49–50, col.15 ll.35–40, col.16 l.67 – col.17 l.11.

Defendants respond: In the *Microsoft Case*, Plaintiff submitted an agreed construction of "rendering" in U.S. Patent No. 6,253,193 (the "'193 Patent"). The '193 Patent is related to U.S. Patent No. 5,892,900 (the "'900 Patent") through a series of continuation applications. The '900 Patent is incorporated by reference into the '106 Patent. Thus, Plaintiff's agreement to the meaning of "rendering" in the '193 Patent should be given effect in the construction of "rendering application" in the '106 Patent. Further, Plaintiff's proposed construction here improperly conflates a general application with a "rendering application." As described in the '106 Patent, as represented by Plaintiff in the *Microsoft Case*, and as customarily used in the art, "rendering" refers to outputting content (playing or displaying content). Thus, the "rendering application" plays or displays content, which includes processing the content to play or display the content. Dkt. No. 101 at 25–27.

In addition to the claims themselves, Defendants cite the following intrinsic and extrinsic evidence to support their position: **Intrinsic evidence**: '106 Patent col.4 ll.14–20, col.5 ll.4–14, col.10 ll.18–19, col.15 ll.35–40, col.17 ll.4–5; '900 Patent[11] (Defendants' Ex. 16, Dkt. No. 101-16); '193 Patent[12] (Defendants' Ex. 15, Dkt. No. 101-15). **Extrinsic evidence**: *IBM Dictionary of Computing* at 572 (10th ed. 1993) (Defendants' Ex. 9, Dkt. No. 101-9 at 4); *Microsoft Computer Dictionary* at 382 (4th ed. 1999) (Defendants' Ex. 10, Dkt. No. 101-10 at 4).

Plaintiff replies: The "rendering application" is not an output device that plays or displays content, it is software that "process[es] information in order to ultimately cause an output device

[11] The '900 Patent is incorporated by reference into the '106 Patent. '106 Patent col.4 ll.14–20. The '900 Patent issued from a continuation-in-part application of U.S. Application No. 08/695,927 which is a continuation-in-part of U.S. Application No. 08/388,107. '900 Patent Certificate of Correction.

[12] The '193 Patent is related to U.S. Application No. 08/388,107 through a series of continuation applications.

to play/display content." Ultimately, "the patent describes an exemplary "rendering application" that performs numerous functions, including sending, processing, handling and presenting the content" and Defendants' proposed construction improperly excludes many of these functions. Dkt. No. 103 at 9–10.

Plaintiff cites further **intrinsic evidence** to support its position: '106 Patent col.3 ll.55–57, col.5 ll.53–57.

Analysis

The issue in dispute is whether the "rendering application" is necessarily an application for playing or displaying content. It is. At the hearing, the Court proposed the construction adopted below and the parties agreed to the proposed construction without argument.

Claim 17 of the '106 Patent provides context for understanding "rendering application." It recites (with emphasis added):

> **17.** A method for managing the use of electronic content at a computing device, the method including:
> receiving a piece of electronic content;
> receiving, separately from the piece of electronic content, data specifying one or more conditions associated with rendering the piece of electronic content, the one or more conditions including a condition that the piece of electronic content be rendered by a rendering application associated with a first digital certificate;
> ***executing a rendering application*** on the computing device, the rendering application being associated with at least the first digital certificate, the first digital certificate having been generated by a first entity based at least in part on a determination that the rendering application will handle electronic content with at least a predefined level of security;
> requesting, through a rights management engine executing on the computing device, ***permission for the rendering application to render the piece of electronic content***;
> determining, using the rights management engine, whether the one or more conditions specified by the data have been satisfied;
> decrypting the piece of electronic content; and
> ***rendering the decrypted piece of electronic content using the rendering application***.

Thus, the "rendering application" of the claims is plainly for "rendering" content.

The ’106 Patent also describes that a “rendering application” is for “rendering” (i.e., presenting) content. For instance, the patent provides:

> As shown in FIG. 9, memory 904 of computing device 900 may include a variety of programs or modules for controlling the operation of computing device 900. For example, memory 904 will typically include one or more ***content rendering applications*** 930 (such as document editors or viewers, electronic book readers, video players, music players, electronic mail or messaging programs, or the like) ***for presenting electronic content to users of the system***. In some embodiments, one or more of the ***rendering applications 930 may also be capable of*** applying policies, rules, and/or controls to govern the use of content or the performance of events. Alternatively, or in addition, these policies, rules, and/or controls may be applied by a rights management program 929 such as that described above and/or in the ’900 patent.

’106 Patent col.16 l.67 – col.17 l.11 (emphasis added). While this explains that the “rendering application” ***may*** have functionality beyond rendering (presenting), it unsurprisingly sets forth that “rendering” is the defining characteristic of the “rendering application.” And the “presenting” that the “rendering application” effects includes both audio (e.g., music players) and images (e.g., document editors).

The Court agrees with Defendants that Plaintiff’s representations in the *Microsoft Case* regarding the meaning of “rendering” are relevant to the meaning of “rendering application” here. As explained above, the ’900 Patent is incorporated by reference into the ’106 Patent. ’106 Patent col.4 ll.14–20. The ’900 Patent issued from a continuation-in-part application of U.S. Application No. 08/695,927 which is a continuation-in-part of U.S. Application No. 08/388,107. ’900 Patent Certificate of Correction. The relevant patent at issue in the *Microsoft Case*, the ’193 Patent, is related to U.S. Application No. 08/388,107 through a series of continuation applications. ’193 Patent, at [63] Related U.S. Application Data. Thus, the ’900 Patent and the ’193 Patent share priority claims and overlap with respect to their disclosed subject matter. Plaintiff represented in the *Microsoft Case* that “rendering” means “[p]laying content through an audio output (e.g., speakers) or displaying content on a video output (e.g., a screen)” in the ’193 Patent. Exhibit I to

Joint Claim Construction Statement – PLR 4-3(a) – Constructions on Which the Parties Agree, *Microsoft Case* (here, Dkt. No. 101-8 at 2). That proposed definition should also apply to "rendering" in the '900 Patent, which is incorporated into the '106 Patent. And—importantly—Plaintiff's *Microsoft-Case* definition comports with the use of "rendering" in the '106 Patent.

Accordingly, the Court construes "rendering application" as follows:

- "rendering application" means "application program that processes content to play it through an audio output (e.g., speakers) or display it on a video output (e.g., a screen)."

H. Order of the Processing and Evaluating Steps of '603 Patent Claim 1

Disputed Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
1. A method for protecting electronic media content from unauthorized use by a user of a computer system, the method including: receiving a request from a user of the computer system to use a piece of electronic media content; identifying one or more software modules responsible for processing the piece of electronic media content and enabling use of the piece of electronic media content by the user; ***processing*** at least a portion of said piece of electronic media content using at least one of the one or more software modules; ***evaluating*** whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner, the evaluating including at least one action selected from the group consisting of: evaluating whether the at least one of the one or more software modules make calls to certain system interfaces; evaluating whether the at least one of the one or more software modules direct data to certain channels; analyzing dynamic timing characteristics of the at least one of the one or more software modules for anomalous timing characteristics indicative of invalid or malicious activity; denying the request to use the piece of electronic media content if the evaluation indicates that the at least one of the one or more software modules fail to satisfy a set of predefined criteria. • '603 Patent Claim 1	The evaluation step must be performed at least in part during the processing step.	The "processing" and "evaluating" steps are limited to the order in which they are recited.

The Parties' Positions

Plaintiff submits: Claim 1 of the '603 Patent recites "processing at least a portion of … content," and an "evaluating" step that does not recite "at least a portion"; thus, "the evaluation

step could plausibly begin (and even be completed) before all of the content is processed." And the patent describes that the evaluation may occur during the processing. Dkt. No. 88 at 24–26.

In addition to the claims themselves, Plaintiff cites the following **intrinsic evidence** to support its position: '603 Patent col.11 ll.34–61, col.19 ll.16–24, col.22 ll.2–9.

Defendants respond: Claim 1 of the '603 Patent recites "evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner" and it is not possible to evaluate whether the software modules process in an authorized manner until the "processing" of the portion of the electronic media content is complete. This does not preclude processing of other portions of the electronic media content while evaluating whether the software modules process a portion in an authorized manner. Indeed, the ordering of the processing and evaluating steps was presented as a distinction over the prior art during prosecution of the '603 Patent. Specifically, Claim 1 was distinguished from art that evaluates whether the process is allowed to execute before the process is allowed to process the content. Dkt. No. 101 at 27–29.

In addition to the claims themselves, Defendants cite the following **intrinsic evidence** to support their position: '603 Patent File Wrapper September 29, 2006 Pre-Appeal Brief Request for Review at 2 (Defendants' Ex. 11, Dkt. No. 101-11 at 2–6, 3), January 7, 2008 Response to Office Action at 10 (Defendants' Ex. 11, Dkt. No. 101-11 at 7–20, 16).

Plaintiff replies: While the "'processing' step of claim 1 of the '603 patent must begin before the "evaluating" step, processing the entire piece of content is not completed before the evaluation begins." Dkt. No. 103 at 10–11.

Plaintiff cites further **intrinsic evidence** to support its position: '603 Patent File Wrapper September 29, 2006 Pre-Appeal Brief Request for Review at 2 (Defendants' Ex. 11, Dkt. No.

101-11 at 2–7, 3), January 7, 2008 Response to Office Action at 10 (Defendants' Ex. 11, Dkt. No. 101-11 at 7–20, 16).

Analysis

The issue in dispute is whether, in Claim 1 of the '603 Patent, the "processing at least a portion of said piece of electronic media content using at least one of the one or more software modules" necessarily occurs before "evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner." It does. But this does not require that all the content (i.e., all portions of the content) be processed before evaluating whether the modules process "the portion" in an authorized manner.

Claim 1 requires processing "at least a portion" of the content and then evaluating whether the software modules process "the portion" of the content in an authorized manner. Specifically, the claim recites "processing ***at least a portion of said piece of electronic media content*** using at least one of the one or more software modules; ***evaluating*** whether the at least one of the ***one or more software modules process the portion of the electronic media content*** in an authorized manner." '603 Patent col.23 ll.55–60. This language was explained by the applicant during prosecution of the '603 Patent:

> Claim 1 in the application recites "processing at least a portion of said piece of electronic media content using at least one of the one or more software modules," and "evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner." In Grecsek, the evaluation determines whether the process (110) is allowed to execute on the computer system. ***Before the evaluation, the process (110) should not be allowed to process protected resource. In contrast, the amended claim 1 requires processing a portion of the electronic media content, and evaluating whether the processing is in an authorized manner.*** Applicants respectfully submit that at least the "processing" and "evaluating"' steps discussed above are not disclosed in Grecsek.

'603 Patent File Wrapper January 7, 2008 Response to Office Action at 10 (emphasis added), Dkt. No. 101-11 at 16. In other words, the prior art did not allow processing before the evaluation, Claim 1 required processing before evaluation.

Neither Claim 1, nor Defendants' proposed ordering, requires that processing the entire piece of content is completed before the evaluation begins. Indeed, the claim specifically recites "processing **at least a portion** of said piece of electronic media content" and "evaluating whether the at least one of the one or more software modules process **the portion** of the electronic media content in an authorized manner." '603 Patent col.23 ll.55–60. Thus, the claim is expressly directed to processing "a portion." It does not require processing the "entire piece of content." Indeed, by processing a "portion" of the piece of content, then evaluating whether the processing of "the portion" was in an authorized manner even while processing another portion, the claim allows authorization during processing of the "piece of content."

Accordingly, the Court construes Claim 1 of the '603 Patent to require that "processing at least a portion of said piece of electronic media content using at least one of the one or more software modules" occurs before "evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner …."

I. "first entity's control information"

Disputed Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
"first entity's control information" • '304 Patent Claim 24	plain and ordinary meaning (beyond proposed construction for "control information")	indefinite

The Parties' Positions

Plaintiff submits: "The use of 'first entity's' in claim 24, rather than simply 'entity's,' is necessitated by the language of unasserted, dependent claim 25 that introduces the receipt of 'a

second entity's control information.'" The "first entity's control information" plainly refers to control information that is owned by the first entity. Dkt. No. 88 at 26–29.

In addition to the claims themselves, Plaintiff cites the following intrinsic and extrinsic evidence to support its position: **Intrinsic evidence**: '304 Patent col.10 ll.60–63, col.10 ll.65–67, col.129 ll.56–60. **Extrinsic evidence**: Jakobsson Decl.[13] ¶¶ 48–56 (Plaintiff's Ex. T, Dkt. No. 88-20); Meldal Decl.[14] ¶¶ 36–39 (Plaintiff's Ex. V, Dkt. No. 88-22).

Defendants respond: The phrase "first entity's control information" indicates that the control information is "possessed in some sense" by the first entity. But the nature of this possession is uncertain. For example, it is not clear if information simply sent by the first entity is properly the first entity's information or whether it requires something more, such as that the first entity created the information. Dkt. No. 101 at 29–30.

In addition to the claims themselves, Defendants cite the following intrinsic and extrinsic evidence to support their position: **Intrinsic evidence**: '304 Patent col.129 ll.56–60, col.328 ll.2–3, col.328 ll.7–8. **Extrinsic evidence**: Meldal Decl. ¶¶ 35–36 (Defendants' Ex. 12, Dkt. No. 101-12[15]); Jakobsson Decl. ¶¶ 49–50, 54–55 (Defendants' Ex. 13, Dkt. No. 101-13[16]).

Plaintiff replies: The first entity, as the owner of the control information, may or may not be the one who sends or creates the information. The claims neither require nor prohibit this. "First entity's control information" simply indicates "that information belongs to the first entity." Dkt. No. 103 at 11–12.

[13] Declaration of Markus Jakobsson Regarding Claim Construction
[14] Declaration of Dr. Sigurd Meldal Regarding Claim Construction
[15] This document is substantially the same as that submitted by Plaintiff as Dkt. No. 88-22.
[16] This document is substantially the same as that submitted by Plaintiff as Dkt. No. 88-20.

Analysis

The issue in dispute is whether the meaning of "first entity's control information" in Claim 24 of the '304 Patent is reasonably certain. It is. It plainly indicates that the control information belongs to the first entity.

Defendants' advocated uncertainty is not suggested or supported by a plain reading of Claim 24, which provides (with emphasis added):

> **24.** A method for monitoring use of a digital file at a computing system, the method comprising:
> receiving the digital file;
> receiving a ***first entity's control information*** separately from the digital file;
> using the first entity's control information to govern, at least in part, a use of the digital file at the computing system; and
> reporting information relating to the use of the digital file to the first entity;
> wherein at least one aspect of the computing system is designed to impede the ability of a user of the computing system to tamper with at least one aspect of the computing system's performance of one or more of said using and reporting steps.

Notably, the claim does not state receiving control information "from" a first entity or "created by" a first entity, it plainly uses "first entity's" to denote a possessive. In fact, Claims 26 and 27, which depend from Claim 24, specify that "the first entity's control information is received from a second entity" and "the first entity's control information and the digital file are separately received from a second entity," respectively. Defendants' proposal that "first entity's control information" in Claim 24 somehow may mean control information simply received from a first entity is thus not reasonable. In other words, "first entity's control information" plainly denotes that the control information belongs to the first entity.

Indeed, the parties and their experts agree that "first entity's" indicates that control information is possessed by the first entity. *See, e.g.*, Meldal Decl. ¶ 36 ("the claimed 'control information' is indicated by an apostrophe as being possessed in some sense by the claimed 'first entity'"), Dkt. No. 101-12 at 11; Jakobsson Decl. ¶ 54 ("'first entity's" is a possessive noun, a type

of noun that indicates ownership or possession"), Dkt. No. 88-20 at 16. Ultimately, while there may be a variety of ways in which the information might belong to the first entity, that goes to claim breadth rather than claim definiteness. *See BASF Corp. v. Johnson Matthey Inc.*, 875 F.3d 1360, 1367 ("the inference of indefiniteness simply from [a broad] scope finding is legally incorrect: breadth is not indefiniteness" (quotation marks omitted)).

Accordingly, Defendants have failed to prove that "first entity's control information" renders any claim indefinite and the Court determines that the term has its plain and ordinary meaning without the need for further construction.

J. "non-executable audio, video, and/or textual content"

Disputed Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
"non-executable audio, video, and/or textual content" • '157 Patent Claims 73, 88	plain and ordinary meaning	indefinite

The Parties' Positions

Plaintiff submits: The phrase plainly refers to audio, video, and/or textual content that is not executable. While other claims refer to "audio, video, and/or textual content" without reference to "non-executable," whether all "audio, video, and/or textual content" is necessarily non-executable is not at issue. And even if "audio, video, and/or textual content" is necessarily non-executable, inclusion of "non-executable" may be redundant but it does not make the meaning of "non-executable audio, video, and/or textual content" uncertain. Dkt. No. 88 at 29–32.

In addition to the claims themselves, Plaintiff cites the following intrinsic and extrinsic evidence to support its position: **Intrinsic evidence**: '157 Patent col.13 ll.54–59, col.57 ll.30–34, col.253 ll.21–26. **Extrinsic evidence**: Jakobsson Decl. ¶¶ 62–68 (Plaintiff's Ex. T, Dkt. No. 88-20); Meldal Decl. ¶¶ 41, 44 (Plaintiff's Ex. V, Dkt. No. 88-22).

Defendants respond: There is no way to meaningfully distinguish between "non-executable audio, video, and/or textual content," recited in Claim 73 and 88 of the '157 Patent, and "audio, video, and/or textual content," recited in Claim 1 of the patent. Specifically, and as argued by Plaintiff in the *Microsoft Case*, data is not executable (citing Intertrust's Opening Claim Construction Brief at 18, *Microsoft Case* (N.D. Cal. Mar. 17, 2003), Dkt. No. 101-5 at 30). Thus, audio, video, and/or textual content, which is data, is necessarily not executable. As different claim terms are presumed to have different meanings and claims should not be construed to render terms superfluous, the meaning of "non-executable audio, video, and/or textual content" is not certain. Further, Plaintiff fails to take a firm position on whether "audio, video, and/or textual content" is necessarily non-executable, exacerbating the uncertainty in the meaning of "audio, video, and/or textual content." Dkt. No. 101 at 30–32.

In addition to the claims themselves, Defendants cite the following intrinsic and extrinsic evidence to support their position: **Intrinsic evidence**: '304 Patent File Wrapper April 2, 2003 Updated Notice Regarding Related Litigation, Intertrust's Opening Claim Construction Brief at 18, *Microsoft Case* (N.D. Cal. Mar. 17, 2003) (Defendants' Ex. 5, Dkt. No. 101-5 at 30). **Extrinsic evidence**: Meldal Decl. ¶¶ 24, 40–42, 44–45 (Defendants' Ex. 12, Dkt. No. 101-12).

Plaintiff replies: Claim 73 and 88, the claims at issue here, are not directed to any "executable" audio, video, and/or textual content— "there is no dispute that the content recited in those claims is non-executable." And there is no dispute as to what it means for audio, visual, and/or textual content to be non-executable. Dkt. No. 103 at 12–13.

Analysis

The issue in dispute distills to whether the meaning of this term is not reasonably certain because "non-executable" may be redundant. The meaning is reasonably certain, despite any actual or potential redundancy.

A claim is not necessarily indefinite for redundancy of limitations. For example, the Federal Circuit has instructed that a "'whereby' clause that merely states the result of the limitations in the claim ***adds nothing to the patentability or substance*** of the claim" and that "clauses [that] merely describe the result of arranging the components of the claims in the manner recited in the claims . . . ***do not contain any limitations***." *Texas Instruments Inc. v. U.S. Int'l Trade Comm'n*, 988 F.2d 1165, 1172 (Fed. Cir. 1993) (emphasis added). Similarly, in the context of determining whether a limitation recited in a dependent claim is merely redundant of a limitation found in an independent claim, the Federal Circuit has noted: "Claim differentiation is a guide, not a rigid rule. If a claim will bear only one interpretation, ***similarity will have to be tolerated***." *ICU Med., Inc. v. Alaris Med. Sys.*, 558 F.3d 1368, 1376 (Fed. Cir. 2009) (quoting *Autogiro Co. of Am. v. United States*, 384 F.2d 391, 404 (Ct. Cl. 1967)) (emphasis added). Similarly, "[d]ifferent terms or phrases in separate claims may be construed to cover the same subject matter." *Nystrom v. Trex Co.*, 424 F.3d 1136, 1143 (Fed. Cir. 2005); *see also, Tandon Corp. v. United States ITC*, 831 F.2d 1017, 1023 (Fed. Cir. 1987) ("two claims which read differently can cover the same subject matter"). Taken in this light, the Federal Circuit's canon that claims should be construed "with an eye toward giving effect to all of their terms," *Haemonetics Corp. v. Baxter Healthcare Corp.*, 607 F.3d 776, 781 (Fed. Cir. 2010), should not be taken as a rigid rule that will render claims indefinite if it can not be followed. Rather, if there is only one reasonable interpretation of a claim then the meaning of the claim is reasonably certain, even with redundant terms. *See Nautilus, Inc. v. Biosig Instruments,*

Inc., 134 S. Ct. 2120, 2129 (2014) (35 U.S.C. § 112, ¶ 2 requires that the claims "inform those skilled in the art about the scope of the invention ***with reasonable certainty***" (emphasis added)).

Here, there is no dispute over whether "non-executable audio, video, and/or textual content" somehow encompasses executable audio, video, and/or textual content. It clearly does not. So there is no need to determine whether executable audio, video, and/or textual content is even technically possible. Ultimately, whether an accused or prior-art content qualifies as a "non-executable audio, video, and/or textual content" is an issue of fact for the jury.

Accordingly, Defendants have failed to prove that "non-executable audio, video, and/or textual content" renders any claim indefinite and the Court determines that the term has its plain and ordinary meaning without the need for further construction.

K. "in proximity"

Disputed Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
"in proximity" • '602 Patent Claim 25	in between any portions of the block of the data that immediately precede and follow the portion to which the error-check value corresponds	indefinite

The Parties' Positions

Plaintiff submits: "In proximity" is a term of degree informed by the '602 Patent's description of the invention. Specifically, the patent explains inserting error check values into data blocks "**in proximity** to the portions of the block to which they correspond" in order to "**receive and authenticate portions of the encoded block of data before the entire block is received**" (quoting '602 Patent col.4 ll.30–45 (Plaintiff's emphasis)). The patent describes that the error-check value is used to detect errors and "if an error is detected, the error check value is used as a replacement, and then the authentication process may continue with the next portion of data."

Thus, "the error check values should be inserted in between any portions of the block of the data that immediately precede and follow the portion to which the error-check value corresponds." Dkt. No. 88 at 33–36.

In addition to the claims themselves, Plaintiff cites the following intrinsic and extrinsic evidence to support its position: **Intrinsic evidence**: '602 Patent fig.7, col.4 ll.30–45, col.12 ll.4–41; '602 Patent File Wrapper October 9, 2007 Notice of Allowability at 3 (Plaintiff's Ex. AA, Dkt. No. 88-27 at 7); U.S. Patent Application No. 13/018,274[17] File Wrapper October 25, 2013 Office Action at 2 (Plaintiff's Ex. Z, Dkt. No. 88-26 at 4), February 14, 2014 Notice of Allowability at 2–3 (Plaintiff's Ex. CC, Dkt. No. 88-29 at 7–8). **Extrinsic evidence**: Jakobsson Decl. ¶¶ 75–88 (Plaintiff's Ex. T, Dkt. No. 88-20); Villasenor Decl.[18] ¶¶ 32, 37–40, 42–43 (Plaintiff's Ex. U, Dkt. No. 88-21).

Defendants respond: "[N]either the claims nor the specification of the '602 patent provide any objective boundaries for determining how closely the error-check value must be to its corresponding portion of the data block to be 'in proximity.'" Specifically, while the patent depicts error-check values directly adjacent to the corresponding portion of the data block, the patent does not provide anything informing "how far away from the portion of the data block the error-check value can be inserted before it is no longer 'in proximity.'" Plaintiff's proposed construction is based on an arbitrary determination of the closeness necessary to ensure error detection occurs early enough to enable the system "to receive and authenticate portions of the encoded data before the entire block is received" (quoting '602 Patent col.4 ll.30–45). This "can be achieved so long

[17] U.S. Patent Application No. 13/018,274, which issued as U.S. Patent No. 8,762,711, is related to the '602 Patent through a series of continuation applications. U.S. Patent No. 8,762,711, at [63] Related U.S. Application Data, available at http://patft.uspto.gov/.
[18] Declaration of John Villasenor, Ph.D. Regarding Claim Construction

as the error-check value is located at some point before the end of the data block." Dkt. No. 101 at 33–35.

In addition to the claims themselves, Defendants cite the following intrinsic and extrinsic evidence to support their position: **Intrinsic evidence**: '602 Patent fig.8, col.3 ll.29–31, col.3 ll.41–43, col.4 ll.30–45, col.5 ll.50–52, col.23 ll.38–59. **Extrinsic evidence**: Villasenor Decl. ¶¶ 29–35, 42–43 (Defendants' Ex. 14, Dkt. No. 101-14[19]); Jakobsson Decl. ¶¶ 74–84 (Defendants' Ex. 13, Dkt. No. 101-13).

Plaintiff replies: The '602 Patent "does not suggest inserting the error-check values (ECVs) beyond the bounds" set forth in Plaintiff's proposed construction. And the embodiments disclosed in the patent are encompassed by the proposed construction. Thus, the Court should adopt the proposed construction. Dkt. No. 103 at 13.

Analysis

The issue in dispute is whether the meaning of placing an error-check value "in proximity" to a portion of the block of data to which it corresponds in Claim 25 of the '602 Patent is reasonably certain. It is. But it is not what Plaintiff suggests. It refers to placing the error-check value proximate to the portion of the block of data, i.e., immediately preceding or following the block of data.

As used in the '602 Patent, "in proximity" is used according to it plain meaning indicating a location proximate to another. While "proximity" may have a plain meaning that denotes a degree of closeness, it also has a plain meaning that denotes an absolute state of being proximate or next. *See, e.g.*, *United States v. Gordillo*, 920 F.3d 1292, 1297 (11th Cir. 2019) (citing, inter alia, Webster's Third New International Dictionary (2002)). The patent uses "in proximity" according

[19] This document is substantially the same as that submitted by Plaintiff as Dkt. No. 88-21.

to this second meaning. The patent uses "in proximity" to denote the position of a check value, an error-check value, or a group of error-check value and check value relative to the portion of a block of data to which the value corresponds. '602 Patent col.3 ll.29–31, col.3 ll.41–43, col.4 ll.36–39. This is depicted in the patent as the position next to the relevant portion. *See id*. at fig.6, col.11 ll.4–17 (the check value S(H(C1))' is located immediately preceding the corresponding portion P1'), fig.8, col.13 ll.23–32 (the group of check value S(H(C1))' and error-check value H(P1)' immediately preceding the corresponding portion P1'). The Court agrees with Defendants that there is no description of "in proximity" that would inform a degree of closeness other than proximate—immediately preceding or following—the corresponding portion. But rather than rendering Claim 25 indefinite, this indicates that "in proximity" is used according to its plain meaning denoting the proximate, i.e., next or closest, position.

Accordingly, the Court holds that Defendants have failed to prove any claim is indefinite for reason of using "in proximity" and construes the term as follows:

- "in proximity" means "immediately preceding or following."

V. CONCLUSION

The Court adopts the constructions above for the disputed and agreed terms of the Asserted Patents. Furthermore, the parties should ensure that all testimony that relates to the terms addressed in this Order is constrained by the Court's reasoning. However, in the presence of the jury the parties should not expressly or implicitly refer to each other's claim construction positions and should not expressly refer to any portion of this Order that is not an actual construction adopted

by the Court. The references to the claim construction process should be limited to informing the jury of the constructions adopted by the Court.

SIGNED this 7th day of July, 2020.

ROY S. PAYNE
UNITED STATES MAGISTRATE JUDGE