

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DOLBY LABORATORIES, INC.,
Petitioner,

v.

INTERTRUST TECHNOLOGIES CORPORATION,
Patent Owner.

IPR2020-00664
Patent 9,569,627 B2

Before MICHAEL R. ZECHER, NABEEL U. KHAN, and
CHRISTOPHER L. OGDEN, *Administrative Patent Judges*.

KHAN, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

A. *Background and Summary*

Dolby Laboratories, Inc. (“Petitioner”) filed a Petition (Paper 2, “Pet.”) requesting an *inter partes* review of claims 1 and 4–8 (“the challenged claims”) of U.S. Patent No. 9,569,627 B2 (Ex. 1001, “the ’627 patent”). Intertrust Technologies Corporation (“Patent Owner”) timely filed a Preliminary Response (Paper 6, “Prelim. Resp.”). Petitioner and Patent Owner filed additional briefing with our authorization. *See* Papers 7, 9. On December 8, 2020, upon consideration of the Petition, Preliminary Response, the additional briefing, and the evidence cited, we determined that Petitioner established a reasonable likelihood that it would prevail with respect to at least one of the challenged claims in the Petition and instituted review to determine the patentability of the challenged claims on all grounds. Paper 10 (“Dec. Inst.”).

After institution, Patent Owner filed a Patent Owner Response (Paper 15, “PO Resp.”), Petitioner filed a Reply (Paper 18, “Pet. Reply”), and Patent Owner filed a Sur-Reply (Paper 19, “PO Sur-reply”). An oral hearing was held on September 13, 2021, and the hearing transcript is included in the record. Paper 27 (“Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision, issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73 (2019), addresses issues and evidence raised during the *inter partes* review. For the reasons that follow, Petitioner demonstrates by a preponderance of the evidence that claims 1 and 4–8 of the ’627 patent are unpatentable.

B. *Related Matters*

The parties identify four related district court cases involving the ’627 Patent: (1) *Dolby Laboratories, Inc. v. Intertrust Corporation*, No. 3:19-cv-

03371 (N.D. Cal.); (2) *Intertrust Technologies Corporation v. AMC Entertainment Holdings, Inc.*, No. 2:19-cv-00265 (E.D. Tex.); (3) *Intertrust Technologies Corporation v. Cinemark Holdings, Inc.*, No. 2:19-cv-00266 (E.D. Tex.); and (4) *Intertrust Technologies Corporation v. Regal Entertainment Group*, No. 2:19-cv-00267 (E.D. Tex.). See Pet. 4; Paper 16, 2. We refer to the three infringement actions filed by Patent Owner in the U.S. District Court for the Eastern District of Texas as the “Texas Actions.”

C. The '627 Patent

The '627 patent, titled “Systems and Methods for Governing Content Rendering, Protection, and Management Applications” is directed to systems and methods for governing application programs used to render, protect, or otherwise access or use electronic content. Ex. 1001, code (54), 2:13–18. The application giving rise to the '627 patent was filed on March 25, 2016, and claims priority ultimately to U.S. Provisional App. No. 60/209,454, filed on June 4, 2000. *Id.* at codes (21), (22), (60), (63).

According to the '627 patent, a supervisory application, which governs a second application, may be used to access protected digital information stored in a secure electronic container and extract secret information needed by the second application to access protected content. Ex. 1001, 2:23–30. The supervisory application may revoke the second application's authorization to process protected content by revoking access to the secure container. *Id.* at 2:30–34. In another embodiment, a supervisory management system may revoke the second application's ability to access or grant access to content if it is determined that the second application is not adequately enforcing certain rules that govern the content's use. *Id.* at 2:34–45.

Figure 1 of the '627 patent is reproduced below.

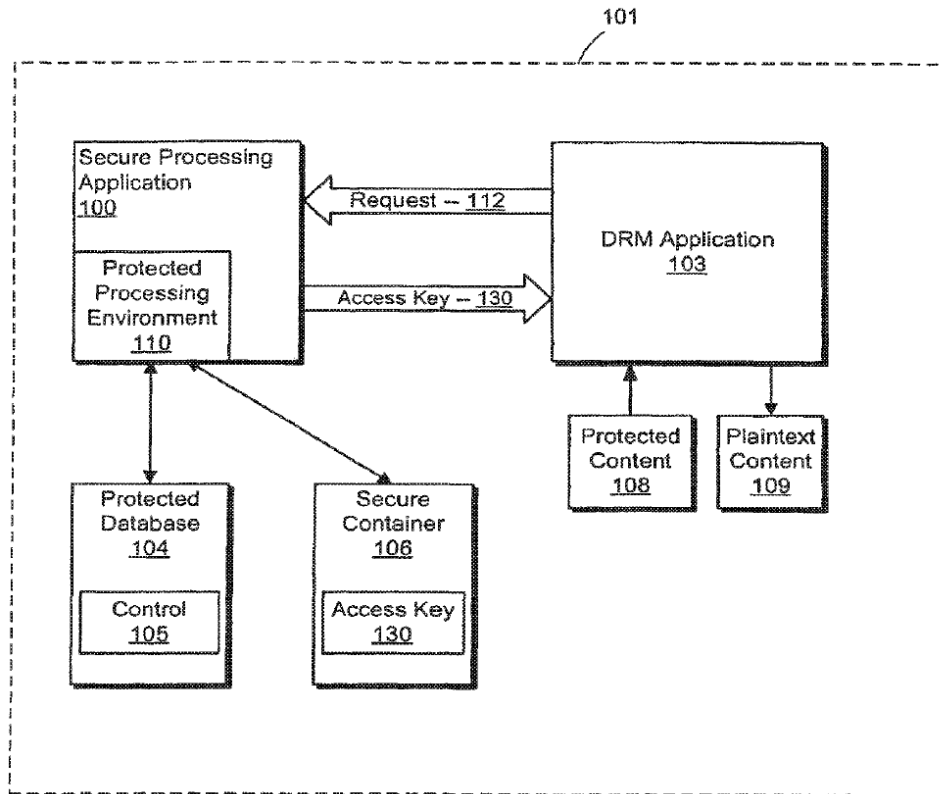


Figure 1 depicts a system that uses a supervisory digital rights management (“DRM”) system for governing operation of other DRM systems. Ex. 1001 at 3:47–49. As shown in Figure 1, system 101¹ has installed thereon a secure processing application 100, which contains protected processing environment 110 and protected database 104. *Id.* at 4:34–36, 4:42–44. Application 103, which may be installed on or remote from system 101, may be supervised or governed by secure processing application 100. *Id.* at 4:36–41.

In operation, secure processing application 100 may extract secret information from secure container 106 or protected database 104 and forward it (or related information) to application 103 in response to request

¹ System 101 may be installed on a personal computer (“PC”) client, computing device, or commerce service. Ex. 1001, 4:35–36.

112 from application 103 to access protected content 108. Ex. 1001, 5:23–30. Application 103 needs the secret information to access protected content 108 and render or make available plaintext content 109. *Id.* at 5:30–32. For example, secret information may be access key 130 extracted by decrypting the relevant portion of secure container 106. *Id.* at 5:25–27. Secure processing application 100 may revoke application 103’s authorization to process protected content 108 by revoking application 103’s access to or use of the secret information. *Id.* at 5:36–40. For example, control 105 could be delivered to secure application 100 indicating that application 103 is not to be granted access (or certain types of access) to the secret information contained in secure container 106 or in protected database 104. *Id.* at 5:40–44. In some embodiments, the content owner or system administrator may set necessary criteria or minimal requirements (relating to operation or security) that application 103 must satisfy to render or process protected content 108. *Id.* at 5:50–57. If it is discovered that application 103 is no longer meeting these requirements, its ability to access or manage content may be revoked. *Id.* at 5:57–61.

Figure 3B of the ’627 patent is reproduced below.

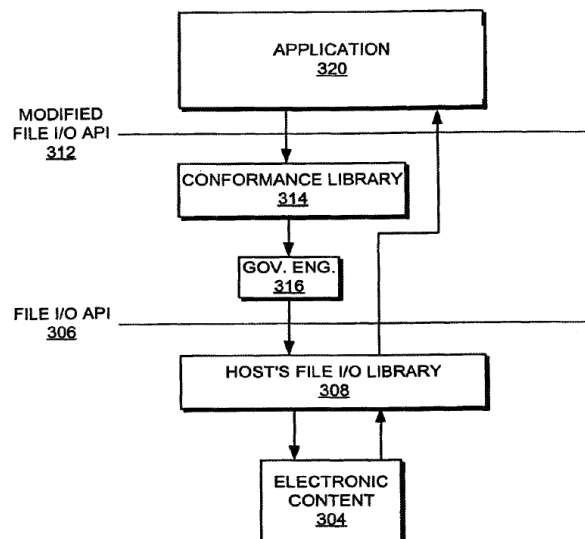


Figure 3B depicts a system for governing content rendering or management application in accordance with an embodiment of the '627 patent. Ex. 1001, 3:55–57. As shown in Figure 3B, application 320 may request access to a piece of electronic content 304 by making a call to the host system's modified application programming interface (“API”) 312. *Id.* at 8:25–28. Calls may be routed from conformance library 314 to governance engine 316, which determines whether to grant or deny the application's request. *Id.* at 8:28–32. If the supervisory application determines the request should be granted, it routes the request to the host system's input/output (“I/O”) library 308 via the host system's modified API 312. *Id.* at 3:32–35. The host system may then perform the necessary operations to retrieve electronic content 304 for application 320. *Id.* at 3:35–37.

D. Illustrative Claims

Of the challenged claims, only claim 1 is independent. Claims 4–8 depend from claim 1 either directly or indirectly. Ex. 1001, 12:6–61.

Claim 1, reproduced below with formatting and bracketing, is illustrative.

1. [1pre] 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:

[1a] 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;

[1b] 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

[1c] 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.

Ex. 1001, 12:6–28.

E. Prior Art and Asserted Grounds

Petitioner asserts that claims 1 and 4–8 would have been unpatentable based on the following grounds:

Ground	Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1	1, 4–8	103(a) ²	Gammie ³
2	1, 4–8	103(a)	Shamoon ⁴

In addition, Petitioner relies on the Declaration of Dr. Vijay K. Madiseti (Ex. 1002) in support of the asserted grounds of unpatentability. *See generally* Pet.; Pet. Reply. Patent Owner relies on the Declaration of Dr. Markus Jakobsson (Ex. 2024) in support of Patent Owner’s Response. *See generally* PO Resp.

II. ANALYSIS

For the reasons discussed below, we determine Petitioner has shown, by a preponderance of the evidence, that claims 1 and 4–8 would have been

² The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. § 103, effective March 16, 2013. Because the application from which the ’664 patent issued claims priority to applications filed before this date, the pre-AIA version of § 103 applies.

³ Gammie, US 5,237,610, Aug. 17, 1993 (Ex. 1010, “Gammie”).

⁴ Shamoon, WO 99/48296, Sept. 23, 1999 (Ex. 1009, “Shamoon”).

obvious over Gammie and that claims 1 and 8 would have been obvious over Shamoon. We, however, determine Petitioner has not shown by a preponderance of the evidence that claims 4–7 would have been obvious over Shamoon.

A claim is unpatentable under 35 U.S.C. § 103(a) if “the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) when in evidence, objective evidence of obviousness or nonobviousness, i.e., secondary considerations. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Additionally, the obviousness inquiry typically requires an analysis of “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2016) (requiring “articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”)). Furthermore, Petitioner does not satisfy its burden of proving obviousness by employing “mere conclusory statements,” but “must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016).

We start first with the analysis of the level of skill in the art and claim construction, and then move to analyzing the remaining *Graham* factors.

A. Level of Ordinary Skill in the Art

Petitioner contends that a person of ordinary skill in the art at the time the '627 patent was filed (a "POSITA") would have had a minimum of a bachelor's degree in computer science, electrical engineering, mathematics, or a related field, and approximately four years of professional experience or equivalent study in the design of secured electronic systems. Pet. 13–14. Petitioner further states that additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education. *Id.* at 14 (citing Ex. 1002 ¶¶ 1–53).

Patent Owner sets forth a similar definition, stating that a POSITA would have a Bachelor of Science degree in electrical engineering and/or computer science, and three years of work or research experience in the fields of secure transactions and encryption, or a Master's degree in electrical engineering and/or computer science and two years of work or research experience in related fields. PO Resp. 12. Patent Owner, however, states that the positions set forth in its Response would be the same under either party's proposal. *Id.*

The parties' proposals do not differ in any meaningful way with respect to the issues in dispute. We adopt Petitioner's definition of a POSITA, except that we delete the qualifier "a minimum" to eliminate vagueness as to the appropriate level of education. The qualifier expands the range without an upper bound, i.e., encompassing a Ph.D. degree and beyond, and thus does not meaningfully indicate the level of ordinary skill in the art. This definition of a person of ordinary skill in the art is supported by the testimony of Dr. Madisetti and is commensurate with the level of ordinary skill as reflected in the asserted prior art and the '627 patent. We

note, however, that our analysis would be the same under either party's definition of a POSITA.

B. Claim Construction

In *inter partes* reviews, we interpret a claim “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b).” *See* 37 C.F.R. § 42.100(b). Under this standard, we construe the claim “in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” *Id.* Only claim terms that are in controversy need to be construed and only to the extent necessary to resolve the controversy. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

1. Whether the Preamble of Claim 1 is limiting

Patent Owner argues the preamble of claim 1 is limiting. PO Resp. 13–15. Patent Owner argues that “the preamble’s recitation of ‘system’ provides antecedent basis for the term ‘the system’ found in two locations in the claim’s body.” PO Resp. 14–16. Patent Owner also argues that the claim body’s recitation of “the system” indicates that both the secure control application and the governed application of claim 1 are executed on the same system. PO Resp. 15; PO Sur-reply 2.

Petitioner argues that, “even if the preamble is limiting, it has been met by the art.” Pet. Reply 3. Petitioner argues that the preamble language recites only a generic processor and type of storage medium, both of which would be evident from the body’s recitation of steps performed by an executing application. Thus, according to Petitioner, the preamble adds nothing essential to the claim that the claim body does not already require.

Generally, a preamble does not limit a claim. *Allen Eng'g Corp. v. Bartell Indus., Inc.*, 299 F.3d 1336, 1346 (Fed. Cir. 2002). Here, we need not decide whether the preamble limits claim 1 because Petitioner establishes by a preponderance of the evidence that Gammie and Shamoon each respectively teach the preamble of claim 1, as we explain in the sections further below. See §§ II.C.2.a, II.D.2.a.

2. “*secure control application*”

Petitioner asserts the term “secure control application” recited in claim 1 should be construed to mean “an application that manages access to protected content.” Pet. 14–16 (citing Ex. 1002 ¶¶ 88–90). To support this proposed construction, Petitioner states that the ’627 patent describes the “secure control application” as “a first application” that “act[s] as a supervisory digital rights managements system that controls a second application.” *Id.* at 15 (quoting Ex. 1001, 2:46–49, 4:23–33); *see also id.* at 15–16 (citing Ex. 1001, 4:45–48, 4:49–5:1, 5:23–44, 6:25–31). Patent Owner applies Petitioner’s proposed construction in its Response and contends that construction of this term is not necessary to resolve the parties’ controversy. PO Resp. 24.

Based on the arguments presented by the parties, and the fact that Patent Owner does not dispute the construction, we adopt Petitioner’s proposed construction for “secure control application.”

3. “*secure electronic container*”

Petitioner argues “secure electronic container” should be construed to mean “a security formatting of electronic information, such as an encrypted version of the information.” Pet. 16–17 (citing Ex. 1002 ¶¶ 91–93). To support this proposed construction, Petitioner argues that the ’627 patent states that “[t]he secure electronic container can take any suitable form,”

and provides examples of a ‘secure electronic container’ as comprising ‘a DigiBox® or DigiFile™ container produced by InterTrust Technologies Corporation, or might simply consist of an encrypted version of the protected digital information.’” *Id.* at 17 (quoting Ex. 1001, 5:9–14); *see also id.* at 16–17 (citing Ex. 1001, 2:25–27, 5:6–9, 5:14–16, 5:23–30, 10:18–26; Ex. 1006, 7:10–11).

Although Patent Owner argues that Petitioner’s construction is inconsistent with the construction ordered by the District Court in the Texas Actions, Patent Owner applies Petitioner’s proposed construction in its Response and contends that construction of this term is not necessary to resolve the parties’ controversy. PO Resp. 12–13.

Based on the arguments presented before us, we agree that no explicit construction of this term is necessary for our Decision.

4. “governed application”

Patent Owner proposes the term “governed application” be construed to mean “an application that accesses content subject to certain rules or policies, including those imposed by the security module.” PO Resp. 13. Patent Owner argues that the ’627 patent describes the governed application as one whose operation is governed by a set of rules or policies—i.e., those imposed by a supervisory application, such as the claimed secure control application. *Id.* at 13 (citing Ex. 1001, 2:37–45, 2:52–57, 4:45–58, 6:31–35, 7:58–67, 9:1–10, 11:39–45; Ex. 2024 ¶¶ 47–48).

Petitioner does not propose a construction for this term, arguing instead that it be given its plain and ordinary meaning and that construction of this term is unnecessary. *See* Pet. Reply 2. Alternatively, Petitioner argues that the cited references teach the claim limitation even under Patent Owner’s construction. *See* Pet. Reply 10, 18; Pet. 19–20, 28–29, 35–36, 44.

We agree with Petitioner that the term “governed application” should be given its plain and ordinary meaning. The term “governed application” is recited in independent claim 1. Dependent claim 4 adds that the governed application “satisfies one or more requirements.” Ex. 1001, 12:43–47. Patent Owner argues that the governed application of claim 1 be subject to certain rules or policies, but fails to explain how these rules and policies differ from the “one or more requirements” of claim 4. *See Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 911 (Fed. Cir. 2004) (“[T]he presence of a dependent claim that adds a particular limitation raises a presumption that the limitation in question is not found in the independent claim.”).

Furthermore, Patent Owner’s proposed construction requires the governed application to be subject to certain rules or policies imposed by the “security module.” The term “security module” appears nowhere in the ’627 patent or claims, and its inclusion in the construction of the term would create confusion regarding whether claim 1 includes the additional limitation of a security module separate from its other limitations. Patent Owner’s proposed construction would, therefore, add ambiguity rather than providing clarity to the claim beyond the plain meaning of the term itself.

5. “*a request to access protected content*”

Patent Owner argues the plain and ordinary meaning of “a request to access protected content” is “an electronic communication that identifies an item of protected content to which access is desired.” PO Resp. 16. Patent Owner makes two points with respect to this proposed construction. First, it argues the specification of the ’627 patent makes clear that the “request” identifies a “particular item of protected content” to be accessed. *Id.* at 16 (citing Ex. 1001, 5:23–32, 8:23–37, Figs. 1, 3B). Second, Patent Owner

stresses that the “request” and the “secure electronic container” are different terms that must have different meanings. *Id.* at 16–18 (citing Ex. 1001, 6:11–22, Fig. 2; Ex. 2024 ¶ 54). Specifically, Patent Owner argues the “request to access protected content” must be a communication that is different from merely receiving the “secure electronic container” containing secret information. PO Resp. 17. Patent Owner cites Figures 1 and 2 of the ’627 patent along with disclosures that indicate that the request to access protected content is different than the secure electronic container. *Id.* at 17–18 (citing Ex. 1001, 5:23–32, 6:11–22).

Petitioner argues that the term should be given its plain and ordinary meaning and that Patent Owner’s “attempt to fabricate and import non-existent limitations about the form of the request should be rejected.” Pet. Reply 3–4. Regardless, Petitioner argues that, even under Patent Owner’s proposed construction, Petitioner has not equated the claimed “request to access protected content” with the claimed “secure electronic container” because for both the obviousness ground based on Gammie and the obviousness ground based on Shamoan, it has identified different disclosures as teaching the two claim terms. *Id.* at 4–5 (citing Pet. 28, 32, 47).

For the reasons explained below, we agree with Petitioner that it has not equated the claimed “request to access protected content” with the claimed “secure electronic container.” Based on the arguments presented before us, we agree that no explicit construction of this term is necessary for our Decision.

6. *“implementing a control action preventing the secret information from being provided to the governed application”*

Patent Owner argues that “implementing a control action” should be construed as “carrying out an active operation that governs” (PO Resp. 20), and “preventing the secret information from being provided to the governed application” means “stopping the secret information from being sent to the governed application” (*Id.* at 22). Patent Owner argues that implementing a control action requires an active/affirmative operation. *Id.* at 20. According to Patent Owner, the specification of the ’627 patent supports a construction requiring an active operation, describing the control action as “revoking” the application’s access to secure information. *Id.* at 21 (citing Ex. 1001, 5:36–40; Ex. 2024 ¶ 60). Similarly, Patent Owner argues the ordinary and customary meaning of “preventing” means to “stop.” *Id.* at 22 (citing Ex. 2026). Patent Owner argues that “[s]topping” something is an active step that is consistent with the active step of “implementing” an “action.” *Id.* Patent Owner argues that preventing requires more than just simply not providing the secret information. *Id.* at 23 (citing Ex. 2024 ¶ 64).

Petitioner argues that construction of this term is unnecessary because the trial grounds “relies on teachings of software, that when executed, causes the claimed secret information not to be provided, and thus stops it from being sent.” Pet. Reply 6. Furthermore, Petitioner argues that the specification of the ’627 patent supports the control action being a passive action because it states that “[r]evocation can also be handled by using expiring credentials and/or certificates.” *Id.* at 6 (quoting Ex. 1001, 11:49–50; Ex. 1005, 294:52–295:7).

In its Sur-reply, Patent Owner argues that dependent claim 7 encompasses the embodiments where revocation of access is an active step

but does not encompass the '627 patent's embodiment of waiting for credentials to expire. PO Sur-reply 5 (citing Ex. 1001, 5:36-46, 7:36-43, 11:56-61).

We agree with Petitioner. The '627 patent provides several examples of preventing secret information from being provided to the governed application, including “revoking application 103's access to, or use of, the secret information” (Ex. 1001, 5:38–39), or revoking keys (*Id.* at 7:36), but makes clear that “[r]evocation can also be handled by using expiring credentials and/or certificates” (*Id.* at 11:49–51). We, therefore, agree with Petitioner that, in light of the '627 patent's disclosure, the control action of dependent claim 7 need not be an active step. Moreover, Patent Owner does not sufficiently explain why dependent claim 7 would encompass the examples from the '627 patent describing the revocation of secret information but not encompass expiring credentials or certificates that are explicitly described as one way of handling revocation.

Patent Owner cites a dictionary definition to support its argument that “preventing” means to “stop,” but that very same dictionary also states that “preventing” means to “keep from occurring” which we determine supports a construction that encompasses more passive implementations such as letting credentials expire. Ex. 2026, 1049.⁵

For the aforementioned reasons, we determine that “implementing a control action preventing the secret information from being provided to the governed application” does not require an active operation. Based on the

⁵ Patent Owner does not paginate Exhibit 2026. We therefore refer to page numbers of the dictionary itself in our citations.

arguments presented by the parties we need not further construe this term to resolve the dispute between the parties.

C. Obviousness over Gammie

Petitioner contends claims 1 and 4–8 are obvious over Gammie. Pet. 18–41. Below we provide a brief overview of Gammie and then analyze Petitioner’s contentions as they relate to “the scope and content of the prior art” and “any differences between the claimed subject matter and the prior art.” *Graham*, 383 U.S. at 17–18.

1. Overview of Gammie

Gammie, titled “Independent External Security Module for a Digitally Upgradeable Television Signal Decoder,” generally relates to the field of scrambling and transmission systems and is directed to “an external security module for a television signal decoder of a broadcast, satellite, or cable television transmission system.” Ex. 1010, 1:15–19. Gammie describes a system having a program source, an encoder, a transmission means, and a single receiving decoder. *Id.* at 1:60–62. Gammie further describes a signal scrambling process in which a key is encrypted, and each subscriber wishing to receive the signal is provided with a decoder having an identification number unique to the decoder. *Id.* at 1:65–2:1. According to Gammie, the decoder for paying subscribers may be authorized with a key to descramble or decrypt the scrambled or encrypted signal, and the decoder for non-subscribers and all would-be pirates are denied that information. *See, e.g., id.* at 2:1–8.

Figure 7 of Gammie is reproduced below.

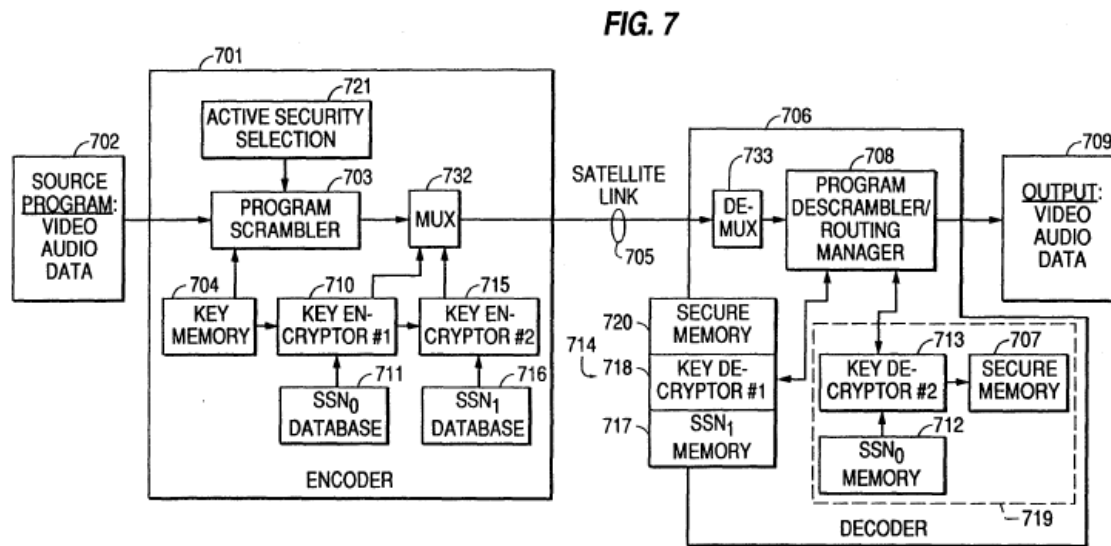
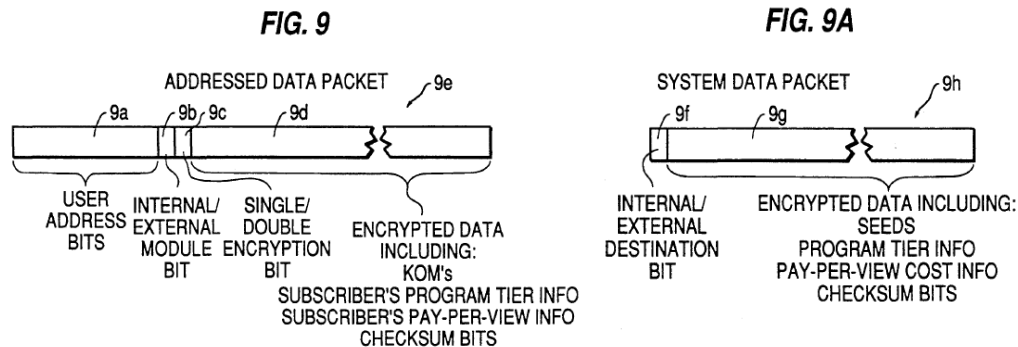


Figure 7 of Gammie depicts an encryption system including encoder 701 for encoding source program 702 for transmission over satellite link 705 to decoder 706. Ex. 1010, 11:59–62. A key memory of the encoder may contain keys of the month (“KOM”) for encrypting a “seed” used to encrypt source program 702. *Id.* at 12:7–10. In particular, a KOM may be encrypted in first key encryptor 710 with first secret serial number SSN_0 , and further encrypted in second key encryptor 715 with second secret serial number SSN_1 . *Id.* at 12:10–15. The encrypted KOM, the encryption seed, and the scrambled or encrypted program content, may be multiplexed together via multiplexer 732 and transmitted via satellite link 705 to decoder 706 as data packets. *See, e.g., id.* at 3:40–57, 8:7–14, 12:17–19, 12:33–38, 13:25–29, 13:67–14:2.

Figures 9 and 9A of Gammie, which depict two examples of these data packets, are reproduced below.



Figures 9 and 9A of Gammie depict authorization and control data in the form of addressed data packet 9e (including the encrypted KOM) and system data packet 9h (including the encryption seed). Ex. 1010, 12:37–40, 13:11–15. More specifically, encrypted data 9d of the addressed data packet 9e may include the encrypted KOM, along with subscriber or program related data and checksum bits, for determining whether a particular subscriber or decoder is authorized to receive and decrypt or view a particular program. *Id.* at 12:55–63. Encrypted data 9g of the system data packet 9h may include the encryption seed, along with program or channel related data and checksum bits. *Id.* at 13:18–25.

Using demultiplexer 733 illustrated in Figure 7 above, decoder 706 may receive and demultiplex the authorization and control data (including the addressed and system data packets) from the scrambled or encrypted program content. *See* Ex. 1010, 3:37–40, 12:20–22, 14:66–67. Routing manager 708 may then route each addressed data packet and system data packet to its specified security module (either internal security module 719 within decoder 706 or external security module 714 mounted on decoder 706). *Id.* at 12:42–50, 12:66–13:10, 13:15–18, 14:16–19. The authorization and control data received by the security module may be processed and used

by conditional access software or program authorization software (“CA/PA software”) within the security module to determine whether a particular program is to be decrypted, depending upon the subscriber’s tier or pay-per-view account. *See id.* at 12:59–63, 13:10–44, 14:19–24. If so authorized, the security module may decrypt the addressed data packet to recover the KOM, and use the decrypted KOM to decrypt the encryption seed from the system data packet. *See id.* at 13:30–36, 14:9–12. The seed may then be sent from the security module through the routing manager to a video descrambler or audio data decryptor to descramble the program’s video or decrypt its audio and output the descrambled or decrypted program content to the subscriber. *See id.* at 2:58–62, 10:47–50, 13:36–39.

2. Analysis of Claim 1

a) Preamble [1pre]

The preamble of claim 1 recites: “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.” Ex. 1001, 12:6–10.

Petitioner argues that, to the extent the preamble is treated as limiting, Gammie teaches the features recited therein. Pet. 24–25 n.4 (citing Ex. 1002 ¶¶ 54–60, 108–109). Petitioner relies on Figures 7 and 4 of Gammie for showing many of the elements of the preamble so we reproduce the relevant portions of those figures below to aid in our discussion of Petitioner’s contentions.

FIG. 7

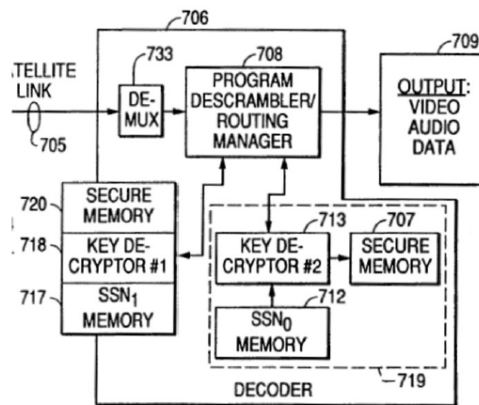
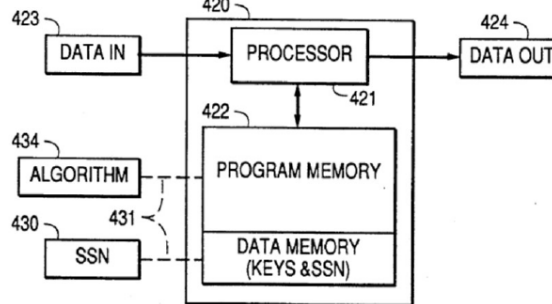


**FIG. 4
PRIOR ART**



A portion of Figure 7 is reproduced above alongside Figure 4 of Gammie. Petitioner argues the recited “system” is taught by Gammie’s encryption system, including its decoder, depicted above as element 706 in Figure 7. Pet. 24 (citing Ex. 1010, Fig. 7, 12:31–35, 13:40–63, 14:42–61, 15:26-42, 18:46-54). Petitioner argues the recited “processor” is taught by Gammie’s processor 870 of the decoder, key decryptors 713 and 718, and processor 421 depicted in Figures 8, 7, and 4, respectively, of Gammie. *Id.* at 24 (citing Ex. 1010, 19:54–58, 23:3–10, 23:43–49, Figs. 4, 7, 8, 10). Petitioner further argues that the recited “non-transitory computer-readable storage medium” is taught by Gammie’s secure memory 707 and 720, and program memory 422. *Id.* at 24–25 (citing Ex. 1010, Figs. 4, 7). Finally, Petitioner argues that the recited “instructions” are taught by Gammie’s disclosure of a program stored in program memory. *Id.* at 25 (citing Ex. 1010, 3:40–4:12).

Patent Owner argues that the preamble of claim 1 requires a non-transitory computer-readable storage medium storing instructions that cause the system to perform all three method steps, including the “receiving,” “extracting,” and “sending” steps. PO Resp. 25. Patent Owner contends,

however, that the memory identified by Petitioner fails to address the “receiving” and “sending” limitations of claim 1. *Id.* (citing Ex. 2024 ¶ 67). For example, Patent Owner argues that Gammie’s security memory modules 707 and 720 of Figure 7 merely store the user address, credits used for pay-per-view, the KOMs, subscriber tier information, and subscriber pay-per-view information. *Id.* at 26 (citing Ex. 1010, 13:58–63, 14:9–16, 15:30–32, 16:10–13, 19:31–39, Fig. 9). Similarly, the program memory 422, according to Patent Owner, “simply contains a decryption algorithm 434, the secret serial number 430, and keys.” *Id.* at 26 (citing Ex. 1010, 5:13–33, Fig. 4; Ex. 2024 ¶ 68). This stored data may relate to the “extracting” limitation, according to Patent Owner, but it does not relate to the “receiving” and “sending” limitations. *Id.* at 26 (citing Ex. 2024 ¶ 69).

In response, Petitioner argues that the secure memory 707 and 720 is not limited to storing only the data that Patent Owner identifies. Pet. Reply 7. According to Petitioner, Gammie’s security modules contain CA/PA software, which receives packets, decrypts and extracts the seeds/keys and sends that information to decrypt a program. *Id.* (citing Ex. 1002 ¶¶ 108–117, 120–121, 125). Thus, Petitioner argues, the processor and security modules cause all three of the method steps to be executed. *Id.*

In its Sur-reply, Patent Owner contends that Petitioner’s reliance on the CA/PA software is a new theory that should be ignored because it was not presented in the Petition. PO Sur-reply 6–7. Moreover, Patent Owner argues that the CA/PA software is not disclosed as being stored in either the secure memory or the program memory identified by Petitioner. *Id.* at 6 (citing Ex. 1010, 14:19–24). Finally, Patent Owner argues that Gammie contains no disclosure that the CA/PA software performs the recited steps of claim 1 and instead describes the software as merely “determining whether a

particular program is to be decrypted depending upon a subscriber's tier, pay-per-view account, etc.” *Id.* at 7–8 (quoting Ex. 1010, 14:19–24).

Based on our review of the evidence of record, we are persuaded by Petitioner's arguments that Gammie teaches the preamble of claim 1. Gammie discloses a system that includes decoder 706 comprising security modules 714 and 719, each of which include secure memory 707 and 720. Ex. 1010, Fig. 7; Ex. 1002 ¶¶ 108–109. Gammie describes the conditional access software or program authorization software as being “contained within the security module[s].” *Id.* at 14:19–24. Thus, the record shows Gammie's security modules have non-transitory computer-readable storage medium (the secure memory) that stores the CA/PA software which Petitioner alleges performs all three steps of the claim.⁶ Moreover, Dr. Madisetti provides credible testimony that Gammie's security modules include a secure microprocessor with memory 421, and that a POSITA would have understood that such a processor and memory would store instructions that execute the method of claim 1. Ex. 1002 ¶ 109.

We do not agree with Patent Owner's argument that Petitioner's reliance on the CA/PA software is a new theory not discussed in the Petition. Initially, we note that Petitioner explicitly relies on such software for each of the three major steps recited in claim 1 in its Petition. *See* Pet. 25, 31, 34. Furthermore, Petitioner identified the “program stored in program memory” of the security module in its Petition as the recited “instructions” of claim 1 (Pet. 25), which when combined with Gammie's disclosure that the “conditional access software or program authorization software [is]

⁶ For the reasons stated below, we agree with Petitioner that the CA/PA software performs the “receiving,” “extracting,” and “sending” steps.

contained within the security module” (Ex. 1010, 14:19–24) provides evidence that reliance on the CA/PA software is not a new theory.

As we explained above, a POSITA would have understood that secure memory 707 and 720 of Gammie’s security modules would store not just the data cited by Patent Owner (e.g. user address, credits used for pay-per-view, the KOMs, subscriber tier information, subscriber pay-per-view information, and decryption algorithms), but also the CA/PA software and that, based on Petitioner’s allegations, this software was cited as performing the “receiving” step and the “sending” step, along with the “extracting step” of claim 1. Thus, we disagree with Patent Owner that the secure memory of the security modules is limited to only storing information related to the “extracting” step rather than also storing instructions related to the “receiving” and “sending” steps.

Finally, we disagree with Patent Owner that Gammie’s CA/PA software does not perform the steps of the claim. We explain our reasoning further below in our analysis of the subsequent limitations of claim 1.

b) Limitation 1a

Limitation 1a recites “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.” Ex. 1001, 12:11–16.

Petitioner contends that the receipt of “authorization and control data” by the CA/PA software on Gammie’s security modules 714/719 or security elements 814/819 (collectively “security modules”) teaches the “receiving” step of claim element 1a. Pet. 25. In particular, Petitioner asserts that Gammie’s CA/PA software contained within the security modules is a

“security control application” (*see, e.g., Id.* at 25 (citing Ex. 1002 ¶ 111), 27 (citing Ex. 1010, code (57), 9:37–41, 9:59–10:4, 14:4–6, 14:16–24; Ex. 1002 ¶ 113)) and that the application running on Gammie’s “program descrambler/routing manager 708” is a “governed application” that accesses protected content (*Id.* at 29 (citing Ex. 1010 14:20–24; Ex. 1002 ¶ 113)). Petitioner further contends the security modules constitute a “protected processing environment.” *Id.* at 26 (citing Ex. 1010, 4:66–5:12, 14:16–24; Ex. 1002 ¶¶ 111–112).

Petitioner asserts the communication of the “authorization and control data” to the software within the security module constitutes a “request to access the protected content” because the purpose of the communication is to provoke a response in the form decryption information needed to access program content. Pet. 28–29 (citing Ex. 1010, 12:55–63, 12:38–40, 12:46–55, 14:2–6, 14:16–19, 15:15–26; Ex. 1002 ¶¶ 114–115). Petitioner further contends that, although not explicitly described as a request, a POSITA would have understood Gammie as teaching a “request to access protected content” because the software on the Gammie’s security modules “conditionally releases decryption information to the descrambler/decryptor only in response to a particular communication thereto.” *Id.* at 28 (citing Ex. 1010, 12:50–66, 13:11–29, 14:19–24; Ex. 1002 ¶¶ 116–117).

Petitioner further argues the governed application (i.e., program descrambler/routing manager 708) executes in a processing environment separate from the protected processing environment of the security modules. Pet. 30–31. Petitioner contends that the program descrambler/routing manager 708 executes in the display and communications processor (“DCP”) 870. *Id.* According to Petitioner, the DCP is an environment that is separate from the security modules. As support, Petitioner cites to Figure

8 of Gammie showing the DCP as separate from the security modules and to disclosures indicating that the security modules are secure and, therefore, constructed so that they cannot be read, executed or modified from outside the security module. *Id.* at 30 (citing Ex. 1010, 5:1–54, 14:30–41, 14:62–15:7, 15:32–38, 23:26–30, 23:67–24:8, Fig. 8; Ex. 1002 ¶¶ 118–119).

Patent Owner disputes Petitioner’s allegations regarding limitation 1a for two reasons: 1) Patent Owner argues that Gammie’s authentication and control data is not a request to access protected content (PO Resp. 27–32) and 2) Patent Owner argues Gammie does not disclose a “governed application” (PO Resp. 32–34). Before we analyze each of these arguments, we first note that we are persuaded by Petitioner’s arguments regarding the undisputed aspects of limitation 1a. For example, we agree that Gammie’s security modules execute in a protected processing environment separate from the remaining components of the decoder, including the descrambler/routing manager that Petitioner relies upon to teach the governed application. Figure 8 of Gammie depicts the DCP and the security modules as separate. Furthermore, Gammie explains that “[t]here is no mechanism for reading or modifying the contents of program memory 422 [of the security modules] via the data inputs” (Ex. 1010, 5:10–12), which supports Petitioner’s argument that the security modules cannot be read, executed or modified from outside and, therefore, are protected and separate from other processing environments, including the DCP. Finally, Dr. Madisetti provides credible testimony that, based on the aforementioned disclosures, the security modules execute in a protected processing environment separate from the processing environment of the DCP. Ex. 1002 ¶ 119.

We now turn to Patent Owner’s two arguments, which we analyze separately below.

(1) Request to access protected content

Patent Owner asserts that Gammie’s “authorization and control data is contained in ‘addressed data packets 9e’ and ‘system data packets 9h.’” PO Resp. 28 (citing Ex. 1010, 12:35–38, 14:68–15:3, Figs. 9, 9A). Neither of these two types of packets, according to Patent Owner, teach the claimed “request to access protected content.” *Id.* at 28–31.

Addressed data packets are not a request for anything, contends Patent Owner. PO Resp. 29. Instead, Patent argues that they merely supply the decoder with subscriber authorization data (e.g. KOM and subscriber tier information) defining the level of access available to the subscriber, rather than request to access any content. *Id.* (citing Ex. 2024 ¶¶ 75–76). Additionally, Patent Owner argues, the addressed data packets are not “content-specific” in that they do not identify any particular program for which access is desired. *Id.* at 29–30 (citing Ex. 1010, 12:55–59, 13:11–29). For both of these aforementioned reasons, Patent Owner argues that addressed data packets are not a request to access protected content.

Patent Owner acknowledges, however, that unlike addressed data packets, system data packets *are* content-specific. Pet. 28 (acknowledging that system data packets include a seed to decrypt a program, pay-per-view cost information, and other information that is program specific). Still, Patent Owner takes issue with the Petition’s reliance on system data packets arguing that Petitioner has mapped the system data packets to both the claimed “secure electronic container” and the claimed “request to access protected content.” PO Resp. 30–31 (citing Pet. 28; Ex. 1002 ¶¶ 113–117). This “dual mapping of Gammie’s system data packets 9h as both the

‘request’ and ‘secure electronic container’ is improper” according to Patent Owner. *Id.* at 31.

In reply, Petitioner emphasizes that the Petition identified receiving the authorization and control data as a whole, including both the addressed data packets and the system data packets together, as teaching the receiving a request limitation, not receiving each of those types of packets separately. Pet. Reply 8 (citing Pet. 28). Petitioner contends that the address data packets do, in fact, include program specific information in the form of program tier information. *Id.* (citing Ex. 1010, 12:55–63; Fig. 9).

Regardless of whether addressed data packets contain content specific information, Petitioner contends that Patent Owner has acknowledged that system data packets do. Pet. Reply 9. As to the system data packets, Petitioner argues that it has not mapped them both to the “request” and the “secure electronic container.” Petitioner emphasizes that the “request” was identified as the *communication* of authorization and control data in the Petition, whereas the “secure electronic container” was identified to be the encrypted seed or key that is contained in the system data packets. *Id.* at 4 (citing Pet. 28, 32).

In the Sur-reply, Patent Owner argues that addressed data packets and system data packets are two disparate types of data and that Petitioner has failed to account for their distinction in arguing that they together constitute a request to access protected content. PO Sur-reply 9. Additionally, Patent Owner disagrees that program tier information in the addressed data packets is content-specific information, arguing that program tier information simply defines the subscriber’s authorized program tier. *Id.* at 10 (citing 12:55-63, 14:19-24).

Based on the evidence of record, we are persuaded that Gammie teaches the claimed “request to access protected content” for the reasons given by Petitioner, outlined above. We credit Dr. Madisetti’s testimony that the authorization and control data is provided from the program descrambler/routing manager to the conditional access software or program authorization software in the security modules in order to receive the access seed and/or key necessary to decrypt a particular program or content if the decoder is authorized to do so. Ex. 1002 ¶ 114. Dr. Madisetti provides credible testimony that a POSITA would have understood the communication of the authorization and control data as a request to access protected content because that communication causes Gammie’s secure control application to respond with information necessary to access the protected content. *Id.* ¶ 116. Thus, we agree with Petitioner that Gammie’s communication of the authorized and control data to the software within the security module constitutes a “request to access the protected content” because the purpose of the communication is to provoke a response in the form decryption information needed to access program content.

Because Patent Owner has acknowledged that system data packets include content-specific information, we need not address Patent Owner’s argument that the addressed data packets are not content-specific. PO Resp. 28 (citing Ex. 1010, 13:11–29, Fig. 9a). Instead we address Patent Owner’s argument that Petitioner has erred in mapping the system data packets to both the claimed “request” and to the claimed “secure electronic container.” Here, we agree with Petitioner that the Petition specifically identified the *communication* of the authorization and control data (which includes the system data packets) as the request rather than the data itself. Pet. 28 (“The communication of authorization and control data to the conditional access

software or program authorization software . . . is a ‘request to access protected content’ because the purpose of the communication is to provoke a response in the form decryption information needed to access program content.”). We, therefore, do not agree that Petitioner has mapped the system data packets to both the recited “request” and the recited “secure electronic container.”

Patent Owner argues that the addressed data packets and system data packets are disparate types of information that should not be lumped together as the claimed request to access protected content. PO Sur-reply 9. But Petitioner identifies both of these types of packets together because Gammie itself associates these two types of packets with each other, referring to them collectively as “authorization and control data.” Ex. 1010, 12:35–38. To the extent Patent Owner raises this issue in support of Patent Owner’s larger point that Petitioner has erred by mapping the system data packets to both the recited “request” and the recited “secure electronic container” as indicated above, we disagree that Petitioner has mapped the system data packet to both limitations of the claim.

(2) Governed application

Patent Owner contends that under either its proposed construction or under the plain meaning of the term, the claimed “governed application” refers to an application that accesses content subject to certain rules or policies, but that the program descrambler/routing manager, identified by Petitioner as the “governed application,” does not access content subject to any rules or policies. PO Resp. at 33 (citing Ex. 1010, 13:36–39, 15:32–42, 17:7–11). According to Patent Owner, any rules or policies associated therewith that are cited by Petitioner apply to the subscriber not the descrambler. *Id.* at 33–34. For example, according to Patent Owner,

Gammie’s “user tier information” applies to the subscriber but not the descrambler. *Id.* at 34 (citing Ex. 1010, 12:55–59, 14:19–24; Ex. 2024 ¶ 85).

Petitioner argues that Gammie teaches a governed application under Patent Owner’s proposed construction or under the plain meaning of the term. Pet. Reply 10. Petitioner argues Gammie’s decoder is subject to rules because it must be authorized by the security module before the seed is released in order to access the protected content. *Id.* (citing Ex. 1010, 2:1–3, 12:55–63, 14:19–24; Pet. 19–20, 28–29, 35–36). According to Petitioner, examples of the rules and requirements include program and service tiers, and pay-per-view event authorization. *Id.* (citing Ex. 1010, 14:19–24, 17:11–16). Petitioner argues that the plain meaning of “governed application” does not require the rules to be specific to the descrambler/decryptor, and regardless, Gammie teaches a governed application even under Patent Owner’s proposed construction because it discloses that “the decoder may be individually authorized” and that the authorization is based on “decoder specific data.” *Id.* at 11 (citing Ex. 1010, 2:1–3, 12:55–63). Finally, Petitioner argues that the rules that apply to the subscriber or decoder, also apply to the internal descrambler/decryptor. *Id.* (citing Ex. 1010, 12:55–63, 13:30–39).

Based on the evidence of record, we are persuaded that Gammie teaches the claimed “governed application” according to its plain meaning and even under Patent Owner’s narrower proposed construction. Gammie teaches that authorization and control data includes “user tier information, pay-per-view information, other subscriber specific or decoder specific data.” Ex. 1010, 12:55–59. Using this data, Gammie “determines whether a particular subscriber or decoder is authorized to receive and decrypt a

particular program or view pay-per-view programs.” *Id.* at 12:60–63. Note that Gammie explicitly discusses “decoder specific data” and determining whether a particular “decoder is authorized to receive and decrypt a particular program” not just the subscriber. *Id.* This makes sense. After all, it is the decoder not the subscriber that accesses and decrypts the program. Thus, the authorization data that provides the rules that govern which subscribers are allowed to access data must also apply to the decoder itself in order for those rules to be enforced. Put another way, there is no evidence in the record that the subscriber is allowed to access content, but the subscriber’s decoder is not allowed to access content, or that the subscriber is not allowed to access content, but the subscriber’s decoder is allowed to access content. There is evidence in the record, on the other hand, as evidenced by Gammie’s disclosures above, that the rules that apply to the subscriber also apply to the decoder and its internal descrambler/decryptor. Pet. Reply 10–11 (citing Ex. 1010, 12:55–63, 14:19–24, 17:11–16).

c) Limitation 1b

Limitation 1b recites “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.” Ex. 1001, 12:17–24.

Petitioner argues that Gammie’s secure control application (e.g. CA/PA software) contained in the security module performs the step of extracting secret information from the secure electronic container by decrypting the seed or key number from the encrypted version of the seed in the system data packets. Pet. 31–32 (citing Ex. 1010, 11:59–12:15, 13:30–

39, 23:67–24:8). Petitioner contends that the system data packet is a secure electronic container because it is encrypted and includes the encrypted seed. Pet. 32 (citing Ex. 1010, 7:38–42, 8:15–39, 11:59–12:15; Ex. 1002 ¶¶ 120–121).

Petitioner further contends that the secret information (e.g. the seed or key number) is used to decrypt the protected content (the program). Pet. 33 (citing Ex. 1010, 13:30–39, 11:59–12:15). Petitioner relies on Gammie’s disclosure that a program is encrypted with a seed and that the decoder uses the seed (the “secret information”) to decrypt the program content. Pet. 33 (citing Ex. 1010, 11:59–12:15; 13:30–39; 15:27–50, 23:67–24:8; Ex. 1002 ¶¶ 61–63, 122).

Finally, Petitioner argues that Gammie’s security modules decrypt the secure electronic container (decrypt the encrypted seed using the key of the month) to generate the unencrypted secret information (e.g. unencrypted seed). Pet. 33–34 (citing Ex. 1010, 13:30–39, 23:67–24:8; Ex. 1002 ¶¶ 123–124).

Patent Owner does not separately dispute Petitioner’s allegations regarding this limitation. Based on the evidence of record, we are persuaded by Petitioner’s arguments which we determine are supported by the cited evidence outlined above.

d) Limitation [1c]

Limitation 1c recites “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.” Ex. 1001 12:24–28.

Petitioner contends that Gammie’s secure control application (CA/PA software) sends the unencrypted secret information (the unencrypted seed)

from the protected processing environment (security modules 714/719/814/819) to the governed application (decoder's program descrambler) executing in the processing environment separate from the protected processing environment (the display and communications processor (DCP) which is separate from the security modules). Pet. 35 (citing Ex. 1010, 13:36–39, 15:30–42; Ex. 1002 ¶ 125).

Patent Owner does not separately dispute Petitioner's contentions regarding this limitation. We are persuaded by Petitioner's arguments which we determine are supported by the cited evidence. For example, Gammie discloses that "the seed is sent from the security module through routing manager to video descrambler 873 or audio data decryptor so as to decrypt a program video or audio." Ex. 1010, 13:36–69. This disclosure supports Petitioner's argument that the unencrypted secret information (the seed) is sent to the governed application (the descrambler). We also agree with Petitioner that the security modules and the DCP are separate processing environments as explained in our analysis of limitation 1a above.

e) Conclusion

For the aforementioned reasons we are persuaded that Gammie teaches all the limitations of independent claim 1.

3. Claims 4–6

Claim 4 depends from claim 1 and further recites "prior to sending the secret information to the governed application, determining, by the secure control application, that the governed application satisfies one or more requirements." Ex. 1001, 12:44–47. Petitioner argues the CA/PA software conditionally releases the secret information (e.g., seed) if a decoder is authorized to receive and decrypt it based on one or more requirements. Pet. 36 (citing Ex. 1010, 12:55–63, 14:19–24, 17:11–16). According to

Petitioner, these requirements include authorization data such as program and service tiers, and pay-per-view event authorization, of a subscriber's individual decoder. *Id.*

Claim 5 depends from claim 4 and further recites that “the one more requirements comprise at least one security requirement.” Petitioner contends that each decoder is assigned a unique user address and corresponding secret serial number (SSN). Pet. 37 (citing Ex. 1010, 3:24-26, 9:59-10:1, 14:4-6); Ex. 1002 ¶¶ 128-130). According to Petitioner, the security modules must also contain the same decoder's SSN to decrypt the key present in the data packets. *Id.* Thus, Petitioner argues that the SSN of the security module must match with the SSN of its mating decoder in order for the security module to decrypt the protected content. *Id.* Petitioner further argues that, if a matching SSN is not found, the security module is considered to be unauthorized and the decryption of the key and seed would fail and protected content would not be accessed. Petitioner argues that the requirement of the decoder and security modules having matching SSNs is a “security requirement” as recited in claim 5. Pet. 37.

Claim 6 depends from claim 4 and further recites “the one or more requirements comprise at least one requirement for processing the protected content.” Petitioner argues that the authorization data, such as the program service tiers and pay-per-view event authorization, cited for claim 4, teach the one or more requirements for processing the protected content recited in claim 6 because those requirements are checked to “conditionally release seeds to decrypt specific programs.” Pet. 38 (citing Ex. 1010, 17:11-16, 19:19-24; Ex. 1002 ¶ 131).

We are persuaded by Petitioner's arguments which we determine are supported by the cited evidence. We agree that authorization data such as

program and service tiers, and pay-per-view event authorization are requirements that must be satisfied in order for the CA/PA software to release the seed to the decoder so that it can descramble the program.

Ex. 1010, 12:55–63, 14:19–24, 17:11–16. We determine, therefore, Gammie teaches the limitations of claims 4 and 6. We also agree with Petitioner that Gammie checks to see if the external security module is properly paired up with a decoder by checking that the SSNs match each other so that an unauthorized security module is not used to improperly access content. Thus, the requirement of having matching SSNs is a security requirement, as recited in claim 5. *Id.* at 3:24–26, 9:59–10:1, 14:4–6; Ex. 1002 ¶¶ 128–130.

Patent Owner raises many of the same arguments here as it did for claim 1, arguing that “Gammie does not disclose a ‘governed application,’ at all” and that Gammie determines “that the **subscriber** is authorized to view the program” not the decoder or descrambler. PO Resp. 35 (citing Ex. 1010, 12:55–59, 14:19–24, Fig. 9; Ex. 2024 ¶ 87). We do not agree with Patent Owner’s arguments for the same reasons stated above in our claim 1 analysis of whether Gammie teaches the recited “governed application.”

Additionally, with respect to claim 5, Patent Owner argues that the subscriber’s program tier or the subscriber’s credits does not teach a security based requirement, which Patent Owner argues is a requirement that the decoder be functioning as intended or that it has not been tampered with. PO Resp. 35–36 (citing Ex. 1001, 5:50–61, 5:1–5, 6:40–51; Ex. 1005, 6024–28, 65:8–9, 67:21–26, 176:6–16; Ex. 2024 ¶ 88). We do not agree with Patent Owner’s argument. Petitioner cited to the requirement that the security module’s SSN match the decoder’s SSN in order for the security module to successfully decrypt the program. Pet. 37. Gammie discloses that this requirement “discourages copying the replaceable external security

module, as each replaceable security module will only work with its mating decoder.” Ex. 1010, 9:66–10:1. Thus, we agree with Petitioner that the requirement that the SSN for the external security module match the SSN of the decoder is a security based requirement because it discourages copying of the external module. Patent Owner’s arguments directed at the subscriber’s program tier or credits do not address Petitioner’s reliance on matching SSNs.

4. *Claim 7*

Claim 7 depends from claim 4 and further recites:

determining, by the secure control application, that the governed application no longer satisfies the one or more requirements; and

implementing a control action preventing the secret information from being provided to the governed application in response to a subsequent access request.

Ex. 1001, 12:54–59.

Petitioner argues that Gammie teaches a secure control application (CA/PA software) determining that the governed application no longer satisfies the one or more requirements of claim 4. Pet. 39. According to Petitioner, it does so, for example, by determining whether there has been a change in programming tier, or by determining if there are insufficient credits to watch a requested program. *Id.* at 39–40 (citing Ex. 1010, 4:2–7, 12:59–63, 14:19–24, 19:26–39; Ex. 1011, 4:33–37, 16:12–14; Ex. 1002 ¶¶ 73–76, 132–133). As support for its contentions, Petitioner relies on Block,⁷ incorporated by reference in Gammie, which discloses preventing a subscriber from viewing programs if the cost of the program is greater than

⁷ Block et al., U.S. Patent No. 4,484,217, Nov. 20, 1984 (Ex. 1011, “Block”).

the existing credit balance of the subscriber. *Id.* at 40 (citing Ex. 1011, 4:33–37, 16:12–14). Petitioner argues that Gammie teaches implementing a control action preventing the secret information from being provided to the governed application in response to a subsequent access request. *Id.* at 40. For example, Petitioner argues that, if sufficient authorization requirements are not met, the secure control application does not send the seed to the descrambler for viewing the program. *Id.* at 39–40 (citing Ex. 1002 ¶¶ 73–76, 132–133).

Patent Owner makes several arguments disputing Petitioner’s allegations regarding claim 7. Patent Owner argues that the Petition fails to identify what in Gammie maps to the claimed “subsequent access request.” PO Resp. 37–39. Patent Owner argues that the inherent ambiguities created by Petitioner’s identification of Gammie’s control and authorization data, consisting of addressed data packets and system data packets, as the “request” in claim 1, are exacerbated with respect to claim 7, because it becomes harder to ascertain how the addressed data packets or system data packets of the subsequent request of claim 7 relate in time to those of the first request of claim 1. *Id.* at 38–39.

Patent Owner also argues that Petitioner fails to explain several aspects of its contentions, including explaining why disclosures from different embodiments of Gammie would be combined (PO Resp. 39–40), how the decoder makes the decisions to deauthorize the decoder (PO Resp. 40), and how passages from Block relate to Gammie’s teaching of decoder deletion of SSN from the encoder side SSN database (PO Resp. 41).

Patent Owner further argues the credit based payment scheme for pay-per-view programmed described in Gammie fails to teach the temporal relationship between the initial “request” from claim 1, and the “subsequent

access request” of claim 7, and fails to teach the prior satisfaction of one or more requirements of claim 4 and no longer satisfying those requirements as required by claim 7. PO Resp. 42. For example, Patent Owner argues that Gammie does not disclose a scenario where sufficient credits exist to watch a pay-per-view event and allowing viewing of the event, but then determining that the subscriber can no longer cover the cost of that pay-per-view event and preventing the seed from being provided to the descrambler in response to a subsequent access request. *Id.* at 43.

Patent Owner argues the limitation “implementing a control action preventing the secret information from being provided to the governed application” requires an active operation that stops the secret information from being provided to the governed application, and cannot be satisfied by “not providing the secret information to the governed application.” PO Resp. 43–44 (Ex. 2024 ¶ 100).

Patent Owner argues that changes to the subscriber’s programming tier do not satisfy the limitations of claim 7. This is because, according to Patent Owner, changing a subscriber’s programming tier is a new requirement. PO Resp. 45. Thus, according to Patent Owner, determining that a subscriber is not authorized to view a program because the subscriber’s programming tier no longer allows the subscriber to view the program, is a determination that the governed application does not satisfy a *new* requirement, rather than no longer satisfying the one or more requirements of claim 4. *Id.* Similarly, Patent Owner argues that such a determination would not be in response to a “subsequent access request” because there was no preceding request in connection with the newly changed programming tier. *Id.* at 46.

Patent Owner argues that Petitioner's reliance on Block is erroneous because the portions of Block cited in the Petition were not properly incorporated by reference by Gammie. PO Resp. 47–49. In particular, Patent Owner argues that Petitioner relies upon narrow aspects of Block, whereas Gammie's incorporation by reference of Block supports only an incorporation of the high level discussion of pay-per-view programming in Block. *Id.* at 47–48 (citing Ex. 1011, 16:12–14; Ex. 2024 ¶¶ 105–106).

Furthermore, Patent Owner argues Petitioner fails to show that a POSITA would have been motivated to modify Gammie with Block. PO Resp. 49–50.

Finally, Patent Owner argues Block's disclosure that preventing a subscriber from viewing a program (because they have insufficient funds) does not teach preventing secret information from being provided to the governed application. PO Resp. 50–51 (citing Ex. 1011, 4:33–37, 16:12–14; Ex. 2024 ¶¶ 109–110).

Based on a review of the cited evidence, we are persuaded by Petitioner's arguments that Gammie teaches the limitations of claim 7. Gammie provides several examples of requirements, include programming and service tiers, and pay-per-view event authorization, that must be met in order for a subscriber's decoder to descramble a program. Petitioner identified some of these requirements in its allegations for claim 4. Pet. 36 (citing Ex. 1010, 12:55–63, 14:19–24, 17:11–16). Petitioner relies on these same requirements here in claim 7, arguing that Gammie's secure control application checks to see if there has been a change in the subscriber's programming tier or if sufficient credits exist to watch a pay-per-view program (tracking credits by subtracting the appropriate number of credits from the subscriber's remaining credits). Pet. 39–40 (citing Ex. 1010, 4:2–7,

12:59-63, 14:19-24, 19:26-39; Ex. 1011, 4:33-37, 16:12-14; Ex. 1002 ¶¶ 73-76, 132-133). Dr. Madisetti provides credible testimony supporting Petitioner's allegations, testifying that a POSITA would have understood that Gammie would confirm whether enough credits exist or that the subscriber's decoder continues to meet the programming tier requirements in order to authorize and continue authorizing descrambling a particular program. Ex. 1002 ¶ 133. If the requirements are not met, Dr. Madisetti testifies that it would have been obvious to cease decrypting the seed or transmitting the decrypted seed. *Id.* We agree with Petitioner that these disclosures and Dr. Madisetti's supporting testimony show that, when a decoder no longer satisfies the requirements of claim 4 (i.e. no longer has the required programming tier, or no longer has enough credits), the seed would no longer be sent to the governed application in response to a subsequent request and the desired program would not be able to be descrambled.

We first address Patent Owner's argument that the programming tier and pay-per-view credit requirements do not meet, what Patent Owner characterizes as the "temporal relationship" (PO Resp. 42) between claims 1, 4 and 7. As we explained above, Patent Owner argues that, when a subscriber's programming tier is changed, for example by lowering the subscriber's tier, this results in a new programming tier requirement, rather than referring back to the "one or more requirements" that Petitioner identified in claim 4. PO Resp. 45. We disagree. Patent Owner takes too narrow a view of the "requirements" of claim 4 and the subsequent recitation of the "requirements" in claim 7. The requirement Petitioner identified for claim 4 was the requirement that a subscriber's programming tier match the tier of the program being requested. Pet. 36 (arguing that "'tier information, pay-per-view information,' and other 'decoder specific data,' is a

requirement that must be satisfied.”) This is the same requirement cited for claim 7. When a subscriber’s programming tier is lowered but a program with a higher tier is requested, the programming tier of the subscriber does not match the tier of the program and the seed is not released to the descrambler. The request for a program after the subscriber’s programming tier is changed is a subsequent request as compared to a request for a program before the change in programming tiers.

Similarly we disagree that Petitioner’s reliance of tracking pay-per-view credits fails to satisfy the “subsequent access request” limitation of claim 7. Again Patent Owner takes too narrow a view, arguing that the subsequent request needs to be for the same pay-per-view event as the initial request. Instead, we agree with Petitioner that a requirement that the subscriber have sufficient credits to view a pay-per-view event satisfies both the “requirements” limitations of claim 4 and claim 7. We also agree with Petitioner that the “subsequent access request” is a request that is subsequent in time as compared to the “request” of claim 1. Petitioner relies on this interpretation consistently for claims 1, 4 and 7. Pet. 36, 39–40 (citing Ex. 1010, 12:55–63, 14:19–24, 17:11–16, 4:2–7, 12:59–63, 14:19–24, 19:26–39; Ex. 1011, 4:33–37, 16:12–14; Ex. 1002 ¶¶ 73–76, 132–133). Nothing in claim 7 requires that “subsequent access request” be for the same pay-per-view event as that requested for claim 1. Thus, we agree with Petitioner that a later request for a pay-per-view event which the subscriber no longer has enough credits to view, satisfies the “subsequent access request” limitation of claim 7.

Next we address Patent Owner’s argument that “implementing a control action” requires an active operation rather than merely not providing secret information to the governed application. PO Resp. 44. As we

explained above, we disagree with Petitioner’s construction that implementing a control action requires an active operation. Under a proper construction, implementing a control action encompasses a decision made by Gammie’s secure control application to not send the seed to the descrambler for viewing a requested program, as Petitioner alleges. *See* Pet. 39–40 (citing Ex. 1002 ¶¶ 73–76, 132–133).

We next address Patent Owner’s arguments regarding Block, including Patent Owner’s argument that relied upon passages of Block were not properly incorporated by reference. PO Resp. 47–49. Whether material is incorporated by reference into a host document is a question of law. *Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1283 (Fed. Cir. 2000). The standard is whether a skilled artisan would have understood the host document to describe the material to be incorporated with sufficient particularity. *Harari v. Lee*, 656 F.3d 1331, 1334 (Fed. Cir. 2011). To incorporate matter by reference, a document must contain language “clearly identifying the subject matter which is incorporated and where it is to be found”; a “mere reference to another application, or patent, or publication is not an incorporation of anything therein.” *In re De Seversky*, 474 F.2d 671, 674 (CCPA 1973). Put differently, “the host document must identify with detailed particularity what specific material it incorporates and clearly indicate where that material is found in the various documents.” *Adv. Display Sys.*, 212 F.3d at 1282.

Reproduced below is the relevant portion of Gammie including its reference to Block. Gammie states:

Impulse pay-per-view (IPPV) programming is defined here as any programming where the subscriber has a pre-authorized number of “credits” saved in his individual decoder. If a subscriber wishes to view a particular program, the

subscriber merely actuates the decoder, the appropriate number of credits are subtracted from the subscriber's remaining credits, and the subscriber is immediately able to view the program. ***Pay television systems are disclosed, for example, in U.S. Pat. No. 4,484,217, issued Nov. 20, 1989 and 4,163,254 issued Jul. 31, 1979 to Block, incorporated herein by reference.***

Ex. 1010, 19:19–30 (emphasis added). The U.S. Court of Appeals for the Federal Circuit has previously held that language nearly identical to that used in Gammie (“incorporated herein by reference”) can be sufficient to indicate to a POSITA that the referenced material is fully incorporated in the host document. *Harari*, 656 F.3d at 1335–36. Gammie introduces Block in the context of a discussion regarding preventing impulse pay-per-view programming and in keeping track of the amount of credits a subscriber has when requesting to view a particular program. The passages that Petitioner relies upon from Block discuss exactly that same subject matter. For example, Block states that “[t]he system operator may limit the potential for non-payment by preventing the subscriber from viewing any impulse purchase programs if the cost of the program is greater than the existing credit balance.” Ex. 1011, 4:33–37; *see also id.* at 16:12–16 (“If, however, the credit is less than the accumulated cost, the decode control 98 is disabled or otherwise inhibited and a display of this condition is effected, for example, by energizing an indicator on the display or ‘flashing’ the payment due indicator.”). A POSITA would have understood from Gammie’s discussion of impulse pay-per-view programming purchases and pay-per-view credits and the subsequent language indicating that the relied upon “pay television systems are disclosed” in Block, that, at the very least, discussions of impulse pay-per-view programming, credit balances, and

preventing viewing of programs when there are insufficient funds would have been incorporated by reference.

Patent Owner further argues that a POSITA would not have been motivated to combine Gammie with Block. PO Resp. 49–51. Specifically, Patent Owner argues that Petitioner relies on two passages from Block related to equipment that is unique to Block and that Gammie’s system lacks features described in Block. *Id.* at 49 (citing Ex. 1011, 11:48–59, 13:62–65, 16:1–16). Patent Owner argues that Petitioner does not explain why a POSITA would have been motivated to modify Gammie with Block’s features such as the decoder control circuit mentioned in one of the relied upon passages of Block. *Id.* at 49–50 (citing Pet. 39–40). We disagree with Patent Owner. As Petitioner explains in its Reply, Petitioner is not relying on Block’s device or decoder, only its teaching of preventing access based on insufficient credits. Pet. Reply 16 (citing Pet. 39–40). As we explained above, a POSITA would have understood that Gammie incorporates the teachings from Block related to pay-per-view programming and tracking the subscriber’s credits given the context of Gammie’s statement incorporating Block by reference. Thus, the motivation to combine Gammie with the cited passages of Block comes directly from Gammie itself. Ex. 1010, 19:26–30.

We also disagree with Patent Owner’s argument that the inherent ambiguities in identifying authorization and control data as the claimed “request” also lead to exacerbated ambiguities in claim 7 which requires a “subsequent access request.” As we explained in our analysis of claim 1, we find no ambiguities in Petitioner’s contentions regarding what it identifies as the claimed “request to access protected content” of claim 1 and what it identifies as the recited “subsequent access request” of claim 7. Petitioner identifies the communication of the authentication and control data as the

request of claim 1. Pet. 28. Petitioner also refers to the communication of authorization and control data as the subsequent access request in its contentions for claim 7. *Id.* at 39–40 (“preventing decryption of keys and/or seeds present in the authorization and control data for subsequent access request to all or certain programming”). To the extent Patent Owner is arguing that there are ambiguities because the subsequent access request of claim 7 needs to request the same program as the request of claim 1, we disagree for the reasons explained above.

Finally, we disagree with Patent Owner’s argument that Petitioner has improperly combined Gammie’s Figure 2 embodiment with the embodiment that includes the CA/PA software and security modules. It is clear from Gammie’s disclosure that the later embodiments are building upon the prior art embodiments of Figure 2. For example, Gammie describes the embodiment of Figure 5, which does include the relied upon security module, as building upon the Figure 2 embodiment, including the secret serial number database. Ex. 1010, 6:3–33 (“As in FIG 2, . . . [t]he key is encrypted in key encryptor 510 using a secret serial number (SSN) from secret serial number database 511 which contains a list of secret serial numbers.”). We determine a POSITA would have understood that the feature of deauthorizing a decoder in the next key cycle by deleting the SSN from the database would be included in the later embodiments that include the security modules.

5. *Claim 8*

Claim 8 depends from claim 1 and further recites “wherein the secret information comprises one or more access keys.” Ex. 1001, 12:60–61. Petitioner identifies Gammie’s seed or key number as the claimed “secret information” and argues that a POSITA would have understood that the seed

or key number is an access key because it is used to access scrambled content. Pet. 41 (citing Ex. 1010, 2:49–52, 7:33–35, 23:68–24:3, 23:13–16, 24:3–8, 23:47–59, 24:33–35; Ex. 1002 ¶¶ 73–76, 134–135). Patent Owner does not separately dispute Petitioner’s contentions regarding claim 8. We are persuaded by Petitioner’s arguments, which we determine are supported by the cited evidence.

In particular we are persuaded that Gammie’s seed and/or key number teaches the recited “secret information [that] comprises one more access keys.” For example, Gammie discloses that “[t]he key can be a signal or code number used in the scrambling process which is also required to ‘unlock’ or descramble the program in program descrambler 108 in decoder 106.” Ex. 1010, 2:49–52. Gammie discloses that “[t]he ‘seed’ can also be a data code or a signal similar to the key described above.” *Id.* at 7:33–35. These disclosures support Petitioner’s argument that the seed/key number are secret information that are used as access keys to descramble protected content.

6. *Objective Indicia of NonObviousness*

In its Response, Patent Owner contends that there is evidence of long-felt need, failure of others, industry praise, commercial success, and copying which should be considered as objective indicia of nonobviousness. PO Resp. 63–66.

For us to give substantial weight to objective indicia of obviousness or nonobviousness, a proponent must establish a nexus between the evidence and the merits of the claimed invention. *ClassCo, Inc., v. Apple, Inc.*, 838 F.3d 1214, 1220 (Fed. Cir. 2016). “[T]here is no nexus unless the evidence presented is ‘reasonably commensurate with the scope of the claims.’” *Id.* (quoting *Rambus Inc. v. Rea*, 731 F.3d 1248, 1257 (Fed. Cir. 2013)).

A patentee is entitled to a presumption of nexus “when the patentee shows that the asserted objective evidence is tied to a specific product and that product ‘embodies the claimed features, and is coextensive with them.’” *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) (quoting *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018)). But as Petitioner correctly argues (Pet. Reply 23–25), a presumption of nexus is inappropriate here because Patent Owner does not provide an analysis demonstrating that its products are coextensive (or nearly coextensive) with the challenged claim. *See Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-01129, Paper 33 at 33 (PTAB Jan. 24, 2020).

But even without the presumption, Patent Owner “is still afforded an opportunity to prove nexus by showing that the evidence of secondary considerations is the ‘direct result of the unique characteristics of the claimed invention.’” *Fox Factory*, 944 F.3d at 1373–74 (quoting *In re Huang*, 100 F.3d 135, 140 (Fed. Cir. 1996)). Also, the nexus must be “to some aspect of the claim *not already in the prior art.*” *In re Kao*, 639 F.3d 1057, 1069 (Fed. Cir. 2011) (emphasis added). “Ultimately, the fact finder must weigh the [objective indicia] evidence presented in the context of whether the claimed invention as a whole would have been obvious to a skilled artisan.” *Lectrosonics*, IPR2018-01129, Paper 33 at 33 (citing *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1331–32 (Fed. Cir. 2016)).

As we discuss below, we find that Patent Owner has not shown a nexus between the claimed invention and long-felt need, failure of others, industry praise, commercial success, or copying.

Moreover, in addition to this proceeding, Patent Owner presents nearly the same arguments and evidence with respect to objective indicia of nonobviousness in at least four other proceedings involving different

patents. *See Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-00661, Paper 17 at 63–68 (PTAB Jan. 21, 2021) (Patent Owner Response); *Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-00662, Paper 17 at 60–65 (PTAB Jan. 21, 2021) (Patent Owner Response); *Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-00665, Paper 19 at 62–66 (PTAB June 16, 2021) (Patent Owner Response); *Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-01123, Paper 18 at 42–45 (PTAB Apr. 20, 2021) (Patent Owner Response). Patent Owner, however, does not explain adequately how the same evidence of objective indicia of nonobviousness can be attributable to each particular claimed invention. *See Fox Factory*, 944 F.3d at 1378 (“The same evidence of secondary considerations cannot be presumed to be attributable to two different combinations of features. In such situations, the patentee retains the burden of proving the degree to which evidence of secondary considerations tied to a product is attributable to a particular claimed invention.” (citation omitted)).

a) Long-Felt Need and Failure of Others

In order to show a long-felt but unmet need for the claimed invention, the objective evidence must show that the need was a persistent one that was recognized by those of ordinary skill in the art at the time of the invention. *In re Gershon*, 372 F.2d 535, 538 (CCPA 1967). As evidence of long-felt need and failure of others, Patent Owner submits three articles from the *Wall Street Journal* which, according to Patent Owner, suggest a need for a way to distribute digital content in a secure manner that would “(1) ensure the digital content would only be used in an authorized manner, (2) ensure that the digital content creator would be compensated for use of the digital content, and (3) allow for such distribution to client devices that were not

under the control of the distributor.” PO Resp. 63–64 (citing Ex. 2028, 1; Ex. 2029, 1; Ex. 2030, 1). Patent Owner also submits another article from the *Wall Street Journal*, and an article from the *New York Times*, describing work by Xerox PARC, IBM, Microsoft, and other companies in the area of digital rights management. *Id.* at 64 (citing Ex. 2031, 3; Ex. 2032, 1).

Patent Owner contends that “most, if not all, systems developed by others were either not commercially successful, were not adopted by digital content industries, copied the claimed invention or have been licensed under the claimed invention.” PO Resp. 64. But Patent Owner does not cite any evidence supporting this argument.

We assign this evidence little weight, because Patent Owner has not identified anything in the cited articles that ascribes any long-felt need to the merits of the claimed invention of the ’627 patent, and has not pointed to any evidence that others had failed to achieve a solution to any technical problem for which the invention of ’627 patent is also a solution.

b) Significance Recognized by the Industry

As evidence of industry recognition, Patent Owner submits an article published in *Fortune*. PO Resp. 64–65 (citing Ex. 2033). Patent Owner argues that the article praises Patent Owner’s technology for “wrap[ping] the file in a secure digital container and tag[g]ing it with rules describing how it could be used,” and where, “[t]o pay or read the . . . file, recipients would need special software or hardware that could be trusted by the content originator to enforce the rules.” PO Resp. 66 (alterations and omission in original) (emphasis omitted) (quoting Ex. 2033, 2). According to Patent Owner, “the use of special software or hardware to govern access to digital content is the thrust of the subject claims of the ’627 patent.” PO Resp. 65 (citing Ex. 1001, 2:13–3:39).

In its Reply, Petitioner contends the *Fortune* article merely provides a high level summary of Patent Owner’s technology. Pet. Reply 24. Petitioner argues that the mention of a “secure digital container” in the article does not signify industry recognition because the secure digital container was known in the prior art. Pet. Reply 24.

We determine that the *Fortune* article fails to provide a nexus to the claimed invention. We agree with Petitioner that the *Fortune* article provides a high level summary of Patent Owner’s technology that is insufficient by itself to show a nexus to the claimed invention. Although the article mentions a “secure digital container” which purportedly refers to the claimed “secure electronic container,” Patent Owner does not contest Petitioner’s argument that Gammie or Shamoan discloses a secure electronic container. See PO Resp. 24–34; 51–57. “Where the offered secondary consideration actually results from something other than what is both claimed and *novel* in the claim, there is no nexus to the merits of the claimed invention.” *In re Huai-Hung Kao*, 639 F.3d 1057, 1068 (Fed. Cir. 2011) (citing cases) (emphasis in original).

Thus, we find that Patent Owner has not shown that there is a nexus between the evidence of industry recognition and the merits of the claimed invention. Absent a nexus, we assign little weight to the evidence of industry praise.

c) Commercial Success and Copying

As evidence of commercial success and copying, Patent Owner argues that over two dozen companies have licensed the claimed invention, and that “Intertrust has received more than \$1 billion in licensing revenue in return for granting licensees the right to practice the claimed invention and Intertrust’s remaining patent portfolio.” PO Resp. 66.

But Patent Owner does not cite any evidence to support its contention, such as the mentioned licenses themselves, or any testimony by someone who was familiar with the circumstances of the licenses to Patent Owner's portfolio. Absent such evidence, we cannot assess whether the licenses have any nexus to the limitations of the challenged claims. Thus, we assign little weight to Patent Owner unsupported arguments on commercial success and copying.

7. Conclusion as to Obviousness over Gammie

For the reasons explained above, we give little weight to Patent Owner's evidence of nonobviousness. On the other hand, based on the arguments and evidence presented in the Petition, we determine that Petitioner has shown that Gammie teaches each limitation of claims 1 and 4–8 of the '627 patent. Weighing all of the evidence of obviousness and nonobviousness, we conclude that Petitioner has shown the unpatentability of claims 1 and 4–8 as obvious over Gammie by a preponderance of the evidence.

D. Obviousness over Shamoon

Petitioner contends claims 1 and 4–8 are obvious over Shamoon. Pet. 41–60. Below we provide a brief overview of Shamoon and then analyze Petitioner's contentions as they relate to “the scope and content of the prior art” and “any differences between the claimed subject matter and the prior art.” *Graham*, 383 U.S. at 17–18.

1. Overview of Shamoon

Shamoon, titled “Methods and Apparatus for Continuous Control and Protection of Media Content,” is directed to systems and methods for performing content protection and DRM. Ex. 1009, codes (54), (57), 2:1–2. More specifically, Shamoon describes a media player for streaming

encrypted digital content, a secure container including a key for decrypting the content, and a control arrangement in the media player for opening the secure container, extracting the key, and decrypting the encrypted content.

Id. at 2:2–9.

Figure 17 of Shamoon is reproduced below.

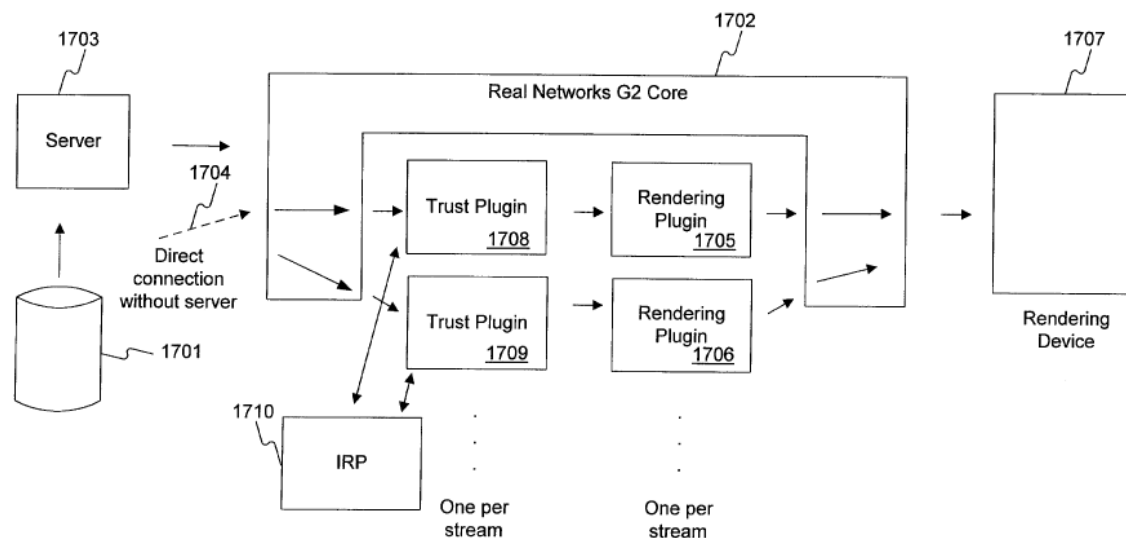


Fig. 17

Figure 17 of Shamoon depicts an exemplary architecture in which a trust plugin operates within an overall Real Networks architecture. Ex. 1009, 2:34–35, 31:18–19. As shown in Figure 17, File 1701 may be provided to Real Networks G2 Client Core 1702 (“Client Core”) through Server 1703 or Direct Connection 1704. *Id.* at 31:20–21. Client Core 1702 may include Trust Plugins 1708, 1709 and Rendering Plugins 1705, 1706. *Id.* at 31:22–24. The architecture may also include Inter-Rights Point (“IRP”) 1710, which is a software process running on the same computer as Client Core 1702. *Id.* at 31:24–25, 32:8–12.

In operation, when File 1701 is a protected stream of content, Client Core 1702 may create an instance of a trust plugin (for example, Trust

Plugin 1708) and pass the stream thereto for processing. Ex. 1009, 31:27–29. The protected content may be encrypted by a cryptographic key stored in a secure container called a DigiBox. *Id.* at 17:24–27, 17:33–18:4.

Figure 12 of Shamoon is reproduced below.

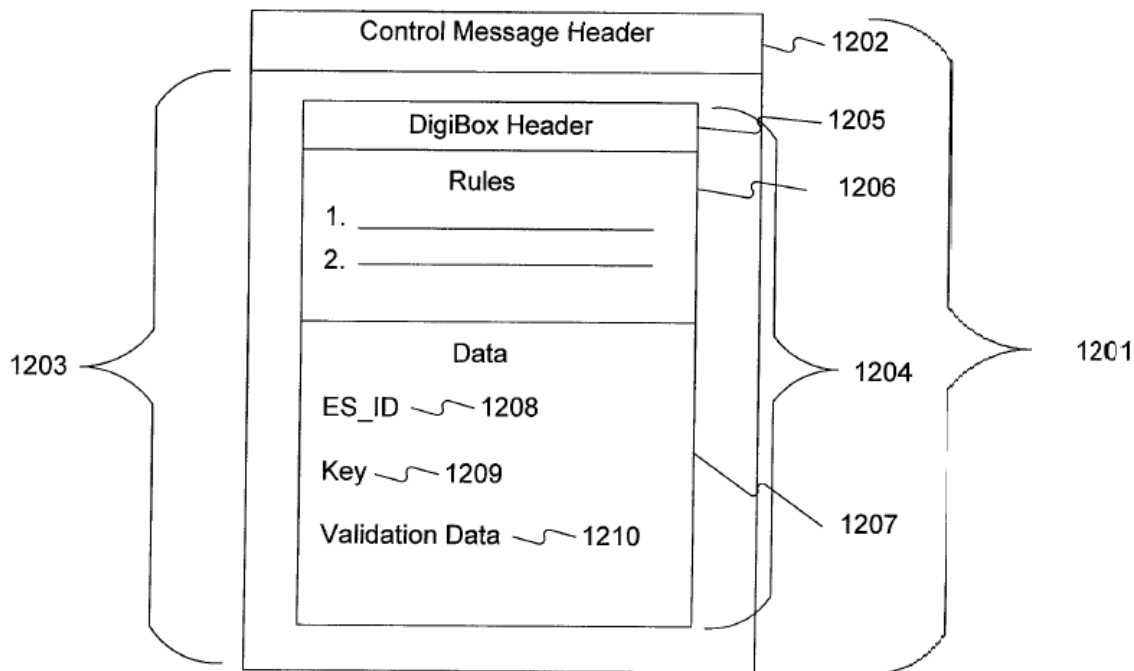


Figure 12 of Shamoon depicts one embodiment of the DigiBox format and how it is incorporated into a control message. *Id.* at 17:28–29. As shown in Figure 12, DigiBox 1204 may contain DigiBox Header 1205, Rules 1206, and Data 1207, which includes, *inter alia*, Cryptographic Key 1209. *Id.* at 17:34–18:2.

Returning to Figure 17, Trust Plugin 1708 may pass a DigiBox to IRP 1710, which may decrypt the DigiBox and extract its cryptographic key and an initialization vector (IV), which then may be passed to Trust Plugin 1708. Ex. 1009, 32:9–15. Trust Plugin 1708 may use this information to decrypt Encrypted Contents 1406 of the stream. *Id.* at 32:14–15. Trust Plugin 1708 may then create an instance of a rendering plugin (for example, Rendering

Plugin 1705) and pass the decrypted contents thereto for further processing. *Id.* at 32:16–24. The rendering plugin may process the stream further and pass it back to the Client Core, which may then pass the stream to Rendering Device 1707. *See id.* at 31:21–23.

Shamoon further describes that rules and controls that specify whether protected content may be processed by an IRP, which is a protected processing environment (PPE) for processing rules and controls. *Id.* at 12:3–5, 12:27–31. These rules and controls may include security and processing requirements such as a password, payment or personal information, geographic location or particular type of viewer, use constraints, and validation data. *See, e.g., id.* at 14:5–14, 15:28–16:12, 17:35–18:13. For example, a key required to decrypt protected content may be provided only if a rule has been satisfied. *Id.* at 14:10–12, 15:1–10, 18:28–34, 19:1–5. If a rule is not satisfied, access to the protected content may be terminated. *Id.* at 11:12–14, 16:2–5.

2. Analysis of Claim 1

a) Preamble [Ipre]

The preamble of claim 1 recites: “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.” Ex. 1001, 12:6–10.

Petitioner argues that, to the extent the preamble is treated as limiting, Shamoon teaches the features recited therein. Pet. 44–45 n.5. In particular, Petitioner argues that Shamoon’s IRP software process runs on a system that includes a CPU and secure memory in a protected processing environment. *Id.* at 44–45 (citing Ex. 1009, 32:9–12 (“IRP 1710 may be a software process running on the same computer as Real Networks G2 Client Core and

Trust Plugin 1708. IRP1710 may run in a protected environment or may incorporate tamper resistance techniques designed to render IRP 1710 resistant to attack.”), 12:3–10, 13:26–28; Ex. 1002 ¶ 144). Patent Owner does not separately dispute Petitioner’s allegations regarding the preamble of claim 1.

We are persuaded by Petitioner’s arguments for the reasons outlined above.

b) Limitation 1a

Limitation 1a recites “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.” Ex. 1001, 12:11–16.

Petitioner identifies Shamoon’s IRP as the claimed “secure control application” and argues the IRP executes in a protected processing environment. Pet 45–46 (citing Ex. 1009, 12:3–10, 13:26–28, 18:21–23, 32:8–12, Fig. 17; Ex. 1005, 87:36–39; Ex. 1002 ¶ 146). Petitioner further identifies Client Core 1702, including its Trust Plugin 1708, as the claimed “governed application.” *Id.* at 47–48 (citing Ex. 1009, 30:6–31, 31:18–29, 32:13–15, 17:24–26, 17:34–18:4; Ex. 1002 ¶ 150). Finally, Petitioner argues that Trust Plugin 1708 passes DigiBox 1404 to IRP 1710 and that this act of passing the DigiBox from Trust Plugin 1708 to IRP 1710 teaches the claimed “receiving . . . a request to access protected content by a governed application.” Pet. 47 (citing Ex. 1009, 2:3–9, 32:8–9, 18:21–25, 32:13–15; Ex. 1002 ¶ 151–152). Petitioner argues that POSITA would have “recognize[d] that receiving a DigiBox, by IPR 1710, from Trust Plugin 1708, is receiving a request to access the stream of protected content because

passing the DigiBox is making a call to the IRP requesting the DigiBox to be decrypted such that a key to access the protected content would be retrieved.” *Id.* at 48 (citing Ex. 1002 ¶ 152). Furthermore, Petitioner argues that Client Core 1702 and its Trust Plugin 1708 operates in an environment separate from the protected processing environment of the IRP. *Id.* at 48–49 (citing Ex. 1009, 32:8–12; Ex. 1002 ¶¶ 153–157).

Patent Owner argues that passing Shamoon’s DigiBox from the Trust Plugin to the IRP is not “receiving . . . a request to access protected content.” PO Resp. 52–57. Here, Patent Owner makes two arguments. We analyze these two arguments in turn.

Patent Owner’s first argument is similar to the one it made regarding the system data packets in Gammie being mapped to both the “request” and “secure electronic container.” Here, Patent Owner argues that Petitioner has mapped Shamoon’s DigiBox as both the claimed “request” and the claimed “secure electronic container.” PO Resp. 53–54 (citing Ex. 2024 ¶ 112). We disagree with Patent Owner for many of the same reasons explained above with respect to the obviousness ground based on Gammie. Specifically, Petitioner has identified the *passing* of the DigiBox from the Trust Plugin to the IRP (by way of a “call” to the IRP) as teaching the claimed “request,” and then separately identifies the DigiBox itself as the “secure electronic container.” Pet. 47–49. Thus, we do not agree that Petitioner has mapped the DigiBox to two separate limitations.

Second, Patent Owner argues the Shamoon’s Trust Plugin is more closely associated with the IRP than the Client Core, and thus passing the DigiBox from the Trust Plugin to the IRP is “an internal communication of the alleged ‘secure control application,’ *not* a request to access protected content ‘receiv[ed] *by* a secure control application.” PO Resp. 54 (citing Ex.

2024 ¶ 114). Patent Owner argues that the Trust Plugin is not subject to any rules or policies imposed by the IRP. *Id.* at 55 (citing Ex. 2024 ¶ 115).

Patent Owner also argues that the Trust Plugin performs functions which show that it is more associated with the IRP or with imposing the rules rather than with being subject to rules by the IRP. *Id.* at 55–56 (citing Ex. 1009, 31:21–35; Ex. 2024 ¶ 116). Therefore, Patent Owner argues, the Trust Plugin is part of the secure control application and not a governed application, and the communication of the DigiBox from the Trust Plugin to the IRP is an internal communication within the secure control application rather than a request that is received by the secure control application.

We disagree with Patent Owner’s argument. As we explained above, Petitioner identifies the IRP as the “secure control application” and the Client Core, along with its trusted plugins, as the “governed application.” Pet. 45–48. Shamoon describes that the Trust Plugins register with the Client Core and that the Client Core creates instances of the Trust Plugins. Ex. 1009, 31:24–29. Thus, the evidence supports Petitioner’s contention that the Trust Plugin is associated with the Client Core. Patent Owner’s argument that the Trust Plugin is not a governed application, fails to address Petitioner’s identification of the Client Core, and not just the Trust Plugins of the Client Core, as the governed application. Pet. 47–48 (citing Ex. 1009, 30:6–31, 31:18–29, 32:13–15, 17:24–26, 17:34–18:4; Ex. 1002 ¶ 150). Shamoon describes that the IRP processes the DigiBox, extracts the cryptographic key and then passes it to the Trust Plugin in order decrypt the content so that the rendering plugin of the Client Core can have access to that content. Ex. 1009, 32:8–31. Thus, the Client Core along with its trusted plugins are, in fact, a governed application because, as Petitioner argues, the IRP controls the decryption key necessary for the Real Networks

player to access the encrypted data packets of the protected content. Pet. 47 (citing Ex. 1009, 30:6–31). For the same reason, the Trust Plugins passing the DigiBox to the IRP for processing is a communication that is received by the IRP (the claimed “secure control application”) rather than a communication internal to the “secure control application.”

For the aforementioned reasons, and based on the evidence of record, we are persuaded by Petitioner’s arguments that Shamoon teaches limitation 1a of claim 1.

c) Limitation 1b

Limitation 1b recites “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.” Ex. 1001, 12:17–24.

Petitioner identifies Shamoon’s cryptographic key as the claimed “secret information” and the DigiBox as the claimed “secure electronic container.” Pet. 49–51 (citing Ex. 1009, 30:8–12, 32:13–15, 17:23–27, 18:14–15, 18:20–21; Ex. 1002 ¶ 158). Petitioner argues that the IRP decrypts the DigiBox and that, by decrypting the DigiBox, a stored key is extracted from the DigiBox in order to decrypt the protected content of the stream. *Id.* at 50–51 (citing Ex. 1009, 17:24–26, 17:34–18:4, 18:20–27; Ex. 1002 ¶¶ 69–72, 159).

Patent Owner does not separately dispute Petitioner’s contentions for this limitation. We are persuaded by Petitioner’s arguments. Shamoon explicitly discloses that the “DigiBox is a secure container” (Ex. 1009, 17:24–26) and that the DigiBox contains the cryptographic key (Ex. 1009,

17:34–18:4). Shamoon further discloses that the IRP processes the DigiBox and extracts the cryptographic key. Ex. 1009, 32:13–15. Thus, we agree with Petitioner that Shamoon teaches extracting, by the IRP, secret information in the form of the cryptographic key from the secure electronic container (i.e. the DigiBox).

d) Limitation 1c

Limitation 1c recites “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.” Ex. 1001, 12:24–28.

Petitioner contends the IRP (“secure control application”) sends the unencrypted cryptographic key (the “secret information”) from the protected processing environment of the IRP to the Client Core including its Trust Plugins. Pet. 52 (Ex. 1002 ¶ 163). Petitioner cites many of the same disclosures from Shamoon to support its argument as it did for the previous limitations of claim 1. Specifically, Petitioner cites Shamoon as disclosing that the IRP passes the cryptographic key to the Trust Plugin after extracting the key from the DigiBox. *Id.* (citing Ex. 1009, 18:20–27; 32:13–15; Ex. 1002 ¶ 164).

Patent Owner does not separately dispute Petitioner’s contentions regarding limitation 1c. We are persuaded by Petitioner’s arguments. Shamoon discloses that “IRP 1708 [sic] may process DigiBox 1404 and extract a cryptographic key and IV, which may then be passed to Trust Plugin 1708.” Ex. 1009, 32:13–15. This disclosure supports Petitioner’s argument that the IRP sends the unencrypted cryptographic key to the Client Core and the Trust Plugin.

e) Conclusion

For the aforementioned reasons, we determine Petitioner has shown that Shamoon teaches all the limitations of claim 1.

3. Claims 4–7

Claim 4 depends from claim 1 and further recites “prior to sending the secret information to the governed application, determining, by the secure control application, that the governed application satisfies one or more requirements.” Ex. 1001, 12:44–47. Claims 5, 6, and 7 directly depend from claim 4.

Petitioner contends that, before sending the secret information to the governed application, Shamoon determines whether the governed application satisfies one or more requirements. Pet. 54 (citing Ex. 1009, 12:27–35, 13:1–28; Ex. 1002 ¶¶ 166–167). Specifically, Petitioner contends that Shamoon’s control block compares a system ID to an authorized system ID, before releasing a key to the authorized system. Pet. 54 (citing Ex. 1009, 12:27–35, 13:1–28; Ex. 1002 ¶¶ 166–167). Petitioner further argues that Shamoon discloses rules requiring that a password has been entered, payment has been made, sufficient budget exists, the computer is in a certain geographic location or release of the key is authorized. Pet. 54–55 (citing Ex. 1009, 14:3–16:5; Ex. 1002 ¶ 168). In addition, Petitioner relies on Shamoon’s disclosure that a DigiBox may deliver rules to the IRP. Pet. 55 (citing Ex. 1009, 17:24–26, 17:34–35). Petitioner argues that, based on these teachings, that it would have been obvious to a POSITA to send a rule, such as those described above, via a DigiBox to the IRP which the IRP would use to control whether Trust Plugin is provided with a key. Pet. 56 (citing Ex. 1002 ¶ 170).

Patent Owner argues that Petitioner “improperly attempt[s] to combine portions of multiple, unrelated embodiments of Shamoon, without any valid rationale for how and why the combinations would be made or whether a [POSITA] would have had a reasonable expectation of success.” PO Resp. 57. Specifically, Patent Owner argues that Petitioner relies on the Real Networks Implementation depicted in Figure 17 of Shamoon to teach the limitations claim 1, but then relies on the governance rules disclosed in separate embodiments depicted in Figures 1, 7, and 20 of Shamoon to teach the “one or more requirements” limitation of claim 4. *Id.* at 57–58 (citing Pet. 45–57). The rules Petitioner relies on, according to Patent Owner, are stored in control block 13 depicted in Figure 1 of Shamoon. *Id.* at 58. The Real Networks implementation, however, does not include control block 13 according to Patent Owner. *Id.* at 59. Similarly, Patent Owner argues that Shamoon does not disclose that DigiBoxes in the Real Networks implementation include any rules. *Id.* (citing Ex. 2024 ¶ 121). Thus, according to Patent Owner, Petitioner’s argument that it would have been obvious to a POSITA to include rules in the DigiBox is conclusory and not sufficiently supported by reasoning showing how this modification would have been made. *Id.* at (citing Ex. 2024 ¶ 122).

Here we agree with Patent Owner. As we explained above, the Petition relies on control block 13 for comparing a system ID to an authorized system ID as a requirement for releasing the key. Pet. 54 (citing Ex. 1009, 12:27–35, 13:1–28; Ex. 1002 ¶¶ 166–167). The Petition further relies on rules, such as those requiring a password, requiring payment, requiring sufficient funds, and checking the geographic location of the computer, as rules that satisfy the “one or more requirements” limitation of claim 4. *Id.* at 54–55 (citing Ex. 1009, 14:3–16:5; Ex. 1002 ¶ 168). Each of

these disclosures is discussed in connection with the “generic system” of Figure 1 and control messages depicted in Figure 7, not in connection with Figure 17 and the Real Network implementation which was relied upon to teach the limitations of claim 1. Ex. 1009, 4:7, 12:11–16:17; Pet. 44–54.

Petitioner argues that Figure 1 of Shamoon is a generic system and that a POSITA would have understood that the other embodiments build on this generic system. Pet. Reply 20–21. As Patent Owner points out, however, at least one other embodiment of Shamoon differs from the generic system because it does not include control block 13. PO Sur-reply 21; *see also* Ex. 1009, 19:30–33 (describing the Pipelined Implementation as an “alternative embodiment” to System 1, and explaining that this alternative system “differs from System 1” in that it “lacks a separate control block, and also lacks a feedback path back from the Composite Block 1110.”).

Accordingly, we agree with Patent Owner that it cannot be presumed that the embodiments of Shamoon, including the Real Networks implementation depicted in Figure 17, incorporate all the features of the generic system. Therefore, in order to appropriately argue that it would have been obvious to a POSITA to use the rules cited in their Petition or to argue that it would have been obvious to a POSITA to send a rule via a DigiBox, Petitioner has the burden of explaining why these features are in fact included in the Real Network embodiment, or why they would be incorporated in the Real Networks embodiment by a POSITA. *In re Stepan Company*, 868 F.3d 1342, 1346 n.1 (Fed. Cir. 2017) (“Whether a rejection is based on combining disclosures from multiple references, combining multiple embodiments from a single reference, or selecting from large lists of elements in a single reference, there must be a motivation to make the combination and a reasonable expectation that such a combination would be successful,

otherwise a skilled artisan would not arrive at the claimed combination.”). We find Petitioner has not adequately identified the possible differences between the Real Network implementation and the generic system of Shamoon or tried to address any such differences if they exist. Dr. Madisetti’s testimony that “it would have been obvious to a POSITA to send IRP 1710 via a DigiBox a rule by which the IRP controls whether the Trust Plugin 1708 is provided with a key,” for example, does not explain whether the DigiBox used in the Real Networks implementation includes rules and if not, why it would have been obvious to a POSITA to include such rules.

Based upon the evidence presented in the Petition and the parties’ arguments, we determine that Petitioner has not provided a valid rationale for how and why a combination between the various embodiments of Shamoon would be made to render the subject matter of claims 4–7 obvious. Accordingly, we are not persuaded that Petitioner has shown Shamoon teaches the limitations of claim 4 or of claims 5–7, which directly depend from claim 4.

4. Claim 8

Claim 8 depends from claim 1 and recites “wherein the secret information comprises one or more access keys.” Ex. 1001, 12:60–61. Petitioner argues Shamoon’s cryptographic key teaches the limitation of claim 8 for the reasons explained by Petitioner with respect to claim 1. Pet. 59–60. Patent Owner does not separately dispute Petitioner’s contentions regarding claim 8. We are persuaded that Shamoon’s cryptographic key, which Petitioner identified as the secret information in claim 1, teaches the secret information comprising one or more access keys. Pet. 49–51 (citing Ex. 1009, 30:8–12, 32:13–15, 17:23–27, 18:14–15, 18:20–21; Ex. 1002 ¶ 158).

5. *Objective Indicia of NonObviousness*

Patent Owner relies on the same evidence of nonobviousness here as they did above for the grounds based on Gammie.

6. *Conclusion*

For the reasons explained above, we give little weight to Patent Owner's evidence of nonobviousness. On the other hand, based on the arguments and evidence presented in the Petition, we determine that Petitioner has shown that Shamoon teaches each limitation of claims 1 and 8, but has not shown that Shamoon teaches the limitations of claims 4–7. Weighing all of the evidence of obviousness and nonobviousness, we conclude that Petitioner only has shown the unpatentability of claims 1 and 8 as obvious over Shamoon by a preponderance of the evidence.

III. CONCLUSION⁸

Weighing all of the evidence of obviousness and nonobviousness together, including the content of the prior art, the differences between the prior art teachings and the claim limitations, and the objective indicia of nonobviousness, we determine that Petitioner has shown by a preponderance of the evidence that claims 1 and 4–8 would have been obvious over Gammie and that claims 1 and 8 would have been obvious over Shamoon.

In summary:

⁸ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. §§ 42.8(a)(3), (b)(2).

Claims	35 U.S.C. §	Reference(s)/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1, 4–8	103(a)	Gammie	1, 4–8	
1, 4–8	103(a)	Shamoon	1, 8	4–7
Overall Outcome			1, 4–8	

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED claims 1 and 4–8 of the '627 patent are held to unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, the parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2020-00664
Patent 9,569,627 B2

FOR PETITIONER:

Scott A. McKeown
scott.mckeown@ropesgray.com
Mark D. Rowland
mark.rowland@ropesgray.com
Keyna Chow
keyna.chow@ropesgray.com
Leslie Spencer
lspencer@desmaraisllp.com

FOR PATENT OWNER:

Christopher A. Mathews
chrismathews@quinnemanuel.com
Razmig Messerian
razmessengerian@quinnemanuel.com
Tigran Guledjian
tigranguledjian@quinnemanuel.com
Scott Florance
scottflorance@quinnemanuel.com