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

INTERTRUST TECHNOLOGIES CORP., *Plaintiff*, v. CINEMARK HOLDINGS, INC., *Defendant*.	§ § § § § § § §	Civil Action No. 2:19-cv-266 (LEAD CASE)
INTERTRUST TECHNOLOGIES CORP., *Plaintiff*, v. AMC ENTERTAINMENT HOLDINGS, INC., *Defendant*.	§ § § § § § § §	Civil Action No. 2:19-cv-265
INTERTRUST TECHNOLOGIES CORP., *Plaintiff*, v. REGAL ENTERTAINMENT GROUP, *Defendant*.	§ § § § § § § §	Civil Action No. 2:19-cv-267

DEFENDANTS' INVALIDITY AND SUBJECT MATTER ELIGIBILITY CONTENTIONS

TABLE OF CONTENTS

I. INTRODUCTION

Pursuant to the Local Patent Rules, the Court's Standing Order Regarding Subject Matter Eligibility Contentions, and the Docket Control Order (ECF No. 33), Defendants Cinemark Holdings, Inc., AMC Entertainment Holdings, Inc., and Regal Entertainment Group ("Defendants") hereby provide their P.R. 3-3 and 3-4 disclosures ("Invalidity Contentions") and Subject Matter Eligibility Contentions. Defendants contend that each of the Asserted Claims (as defined below) is invalid and/or patent-ineligible under at least 35 U.S.C. §§ 101, 102, 103, and/or 112.

A. Asserted Claims

Plaintiff Intertrust Technologies Corporation's ("Intertrust") alleges in its P.R. 3-1 and 3-2 Patent Initial Disclosures ("Infringement Contentions") that Defendants infringe following patents and claims (collectively, the "Asserted Patents" and "Asserted Claims"):

- U.S. Patent No. 6,157,721 ("the '721 Patent"): Claims 9 and 29
- U.S. Patent No. 6,640,304 ("the '304 Patent"): Claim 24
- U.S. Patent No. 6,785,815 ("the '815 Patent"): Claims 42 and 43
- U.S. Patent No. 7,340,602 ("the '602 Patent"): Claims 25 and 26
- U.S. Patent No. 7,406,603 ("the '603 Patent"): Claims 1 and 2
- U.S. Patent No. 7,694,342 ("the '342 Patent"): Claims 1, 7, 8, and 12
- U.S. Patent No. 8,191,157 ("the '157 Patent"): Claims 53, 54, 56-60, 64-66, 69-75, 80, 81, 84, 86-90, 95, 96, and 99
- U.S. Patent No. 8,191,158 ("the '158 Patent"): Claim 4
- U.S. Patent No. 8,931,106 ("the '106 Patent"): Claim 17
- U.S. Patent No. 9,569,627 ("the '627 Patent"): Claims 1 and 4-8

Defendants' Invalidity Contentions and Subject Matter Eligibility Contentions (collectively, "Contentions") address only the Asserted Claims specifically set forth in Intertrust's Infringement Contentions, which are the only claims asserted against Defendants.

B. Ongoing Discovery and Disclosures

Defendants' Contentions are based on Defendants' current knowledge and understanding of the Asserted Claims and review of prior art items as of the date of service, and are made without the benefit of discovery regarding the parties' claim construction contentions, any expert discovery, any third-party discovery, and any claim construction opinion or order by the Court. Accordingly, Defendants' Contentions are provided without prejudice to Defendants' right to revise, amend, correct, supplement, modify, or clarify the same. Defendants also reserve the right to complete their investigation and discovery of the facts, to produce subsequently discovered information, and to introduce such subsequently discovered information at the time of any hearing or trial in this action.

Defendants' Contentions are also based on Defendants' current understanding of the Asserted Claims in view of Intertrust's Infringement Contentions, which are deficient both facially and substantively. Among other things, the Infringement Contentions lack the specificity required by P. R. 3-1, fail to properly identify accused instrumentalities, and fail to explain adequately Intertrust's infringement theories for numerous limitations. Intertrust has prejudiced Defendants' ability to understand, for purposes of preparing these Contentions, what Intertrust alleges to be the scope of the Asserted Claims. In the event Intertrust amends its Infringement Contentions (either to cure these deficiencies or for any other reason) or otherwise responds to address any deficiency therein, Defendants reserve the right to amend or supplement their Contentions.

Defendants incorporate by reference all other bases for invalidity identified in Defendants' Answers, Initial Disclosures, and interrogatory responses in this matter, and any bases of invalidity

identified during the prosecution of the Asserted Patents, as well as all related patents and/or patent applications. Defendants further incorporate by reference all admissions regarding the Asserted Patents including, but not limited to, admissions in the specification of the Asserted Patents and the prosecution of the Asserted Patents and related patents and/or patent applications. Defendants moreover incorporate contentions previously served or subsequently served in any related litigations, including but not limited to any invalidity contentions served by Microsoft Corporation in *Intertrust Technologies Corporation v. Microsoft Corporation*, Nos. 4:01-CV-1640, 4:02-CV-647 (N.D. Cal.), served by Apple, Inc. in *Intertrust Technologies Corporation v. Apple, Inc.*, No. 4:13-CV-1235 (N.D. Cal.), or served in any prior litigations involving the Asserted Patents and related patents (collectively, the "Prior Actions").

C. Claim Construction

The Court has not construed the Asserted Claims. Defendants map the prior art references to the Asserted Claims based on Intertrust's apparent constructions, to the extent understood, of the Asserted Claims as advanced in Intertrust's Infringement Contentions. However, nothing stated in this document or the accompanying claim charts should be treated as an admission or suggestion that Intertrust's apparent claim constructions are correct, or that any claim terms of the Asserted Claims are not invalid under 35 U.S.C. § 112 for being indefinite, failing to satisfy the written description requirement, or failing to satisfy the enablement requirement. In fact, Defendants specifically deny that Intertrust's apparent claim constructions are proper.

Depending on the Court's construction of the Asserted Claims of the Asserted Patents, and/or positions that Intertrust or its expert witness(es) may take concerning claim interpretation, infringement, invalidity issues, and/or subject matter eligibility issues, the asserted prior art references may be of greater or lesser relevance. Given this uncertainty, the charts may reflect alternative applications of the prior art against the Asserted Claims. Thus, no chart or position

taken by Defendants should be construed as an admission or a waiver of any particular construction of any claim term. Defendants also reserve the right to challenge any of the claim terms under 35 U.S.C. § 112, including by arguing that they are indefinite, not supported by the written description, and/or not enabled.

D. Effective Date

Intertrust asserted under P.R. 3-1(e) that the Asserted Claims are entitled to the following priority dates:

- '721 Patent: August 12, 1996
- '304 Patent: February 13, 1995
- '815 Patent: June 8, 1999
- '602 Patent: December 14, 1999
- '603 Patent: August 31, 1999
- '342 Patent: June 9, 2000
- '157 Patent: February 13, 1995
- '158 Patent: February 13, 1995
- '106 Patent: June 9, 2000
- '627 Patent: June 4, 2000

Defendants do not agree that Intertrust is entitled to the above-listed priority dates for each of the Asserted Claims, as Intertrust has failed to prove it is entitled to these priority dates. Nonetheless, Defendants have used Intertrust's claimed priority dates for purposes of these Contentions. Defendants use of Intertrust's asserted priority dates for purposes of these Contentions should not be interpreted as a concession that any Asserted Claim is entitled to Intertrust's asserted priority date. To the extent Intertrust in the future seeks and is granted leave

to amend its disclosures in an attempt to establish an earlier effective date, Defendants reserve the right to amend these Contentions in response, including by disclosing additional prior art or earlier versions or evidence of the prior art disclosed herein.

E. Prior Art Identification and Citation

The accompanying invalidity claim charts (Appendices A-J) cite to particular teachings and disclosures of the prior art references as applied to features of the Asserted Claims. However, persons having ordinary skill in the art may view an item of prior art generally in the context of other publications, literature, products, and understanding. Accordingly, the cited portions are only exemplary and are intended to put Intertrust on notice of the basis for Defendants' contentions. Defendants have endeavored to identify the most relevant portions of the references, but the references may contain additional support for particular claim limitations. Defendants reserve the right to rely on uncited portions of the prior art references, other documents, and/or operational systems, as well as fact and expert testimony, to provide context or to aid in understanding the cited portions of the references and interpreting the teachings of the prior art and to establish bases for combinations of certain cited references that render the Asserted Claims obvious. Defendants also reserve the right to rely on any prior art system referenced, embodied, or described in any of the prior art references identified herein, or which embodies any of the prior art references identified herein.

Moreover, Defendants reserve the right to rely on inventor admissions concerning the scope of the prior art relevant to the Asserted Patents found in, *inter alia*, the prosecution histories of the Asserted Patents or related patents and/or patent applications, any testimony or declarations of the named inventors concerning the Asserted Patents or related patents, and any papers or evidence submitted by Intertrust in connection with this litigation, any other pending or future litigation brought by Intertrust involving the Asserted Patents or related patents, or *inter partes*

review proceedings involving the Asserted Patents or related patents. Defendants also may establish what was known to a person having ordinary skill in the art through treatises, published industry standards other publications, products, and/or testimony.

Where the invalidity claim charts (Appendices A-J) cite to a particular figure in a reference, the citation should be understood to encompass the caption of the figure and other text relating to and/or describing the figure. Similarly, where the invalidity claim charts cite to particular text referring to a figure, the citation should be understood to include the figure and related figures as well.

The prior art references listed herein and in the accompanying invalidity claim charts may disclose the elements of the Asserted Claims explicitly and/or inherently. The prior art references are also relevant for their showing of the state of the art and reasons and motivations for making improvements, additions, and combinations. The suggested obviousness combinations are provided in the alternative to Defendants' anticipation contentions and are not to be construed to suggest that any reference is not itself anticipatory.

Further, the combinations of prior art references contained herein demonstrating the obviousness of the Asserted Patents under 35 U.S.C. § 103 are merely exemplary and are not intended to be exhaustive. All such combinations are intended to include and be in view of the knowledge of a person of ordinary skill in the art. Additional obviousness combinations of the identified prior art references are possible, and Defendants reserve the right to use any such combination(s) in this Action. In particular, Defendants are currently unaware of the extent, if any, to which Intertrust will contend that limitations of any particular claim(s) are not disclosed in the art that Defendants have identified as anticipatory. To the extent that Intertrust does so,

Defendants reserve the right to identify other evidence or references that anticipate or render obvious the particular claim(s).

Nothing in these Contentions should be treated as an admission that any of Defendants' accused instrumentalities meet any limitation of the Asserted Claims. Defendants deny infringing the Asserted Claims. To the extent that any prior art references identified by Defendants contains a claim element that is the same as or similar to an element in an accused instrumentality, based on a claim construction inferred from Intertrust's Infringement Contentions, inclusion of that reference in Defendants' Contentions is not a waiver by Defendants of any claim construction or non-infringement position, nor is it an admission or suggestion by Defendants that any accused instrumentality satisfies the limitations of the Asserted Claims under a proper construction of those claims.

F. Additional Reservation of Rights

Defendants reserve all rights to further supplement or modify these Contentions, including the prior art disclosed and stated grounds of invalidity. In addition, Defendants reserve the right to prove invalidity of the Asserted Claims on bases other than those required to be disclosed in these disclosures and contentions pursuant to P.R. 3-3 and/or the Court's Standing Order Regarding Subject Matter Eligibility Contentions.

Defendants' identification in the prior art of claim elements recited in the preamble of any claims is not intended to indicate that any such preamble is limiting. All such disclosures are made only to the extent the preamble is determined to be limiting.

Defendants also intend to diligently seek discovery from third parties to demonstrate the alleged inventions were known or used by others under 35 U.S.C. § 102(a), in public use and/or on-sale under 35 U.S.C. § 102(b), derivation under 35 U.S.C. § 102(f), and/or earlier invention of

the alleged inventions under 35 U.S.C. § 102(g). Defendants may therefore modify, amend, and/or supplement these Contentions if and when further information becomes available.

Additionally, Defendants incorporate by reference into these Contentions every claim element cross-referenced in Intertrust's Infringement Contentions. For any element in Intertrust's Infringement Contentions for which Intertrust refers to the information from one or more other elements (whether in the same or a different patent), Defendants incorporate by reference the same cross-reference for these contentions.

Subject to the foregoing statements and qualifications, Defendants provide the following:

II. P.R. 3-3 DISCLOSURES AND CONTENTIONS

The following appendices include claim charts of prior art references that, alone and/or in combination with other references, render the Asserted Claims of the Asserted Patents invalid under §§ 102 or 103, and further include (directly and/or in combination with the corresponding subparts of Section II.B, below) secondary references that would have been obvious to combine with the charted prior art references and motivations for making such combinations.

Appendix A	U.S. Patent No. 6,157,721 ("the '721 Patent")
Appendix B	U.S. Patent No. 6,640,304 ("the '304 Patent")
Appendix C	U.S. Patent No. 6,785,815 ("the '815 Patent")
Appendix D	U.S. Patent No. 7,340,602 ("the '602 Patent")
Appendix E	U.S. Patent No. 7,406,603 ("the '603 Patent")
Appendix F	U.S. Patent No. 7,694,342 ("the '342 Patent")
Appendix G	U.S. Patent No. 8,191,157 ("the '157 Patent")
Appendix H	U.S. Patent No. 8,191,158 ("the '158 Patent")
Appendix I	U.S. Patent No. 8,931,106 ("the '106 Patent")
Appendix J	U.S. Patent No. 9,569,627 ("the '627 Patent")

A. P.R. 3-3(a) Disclosures: Identification of Items of Prior Art That Anticipate or Render Obvious Asserted Claims

Defendants contend that the following prior art patents, printed publications, and systems, alone and/or in combination, anticipate and/or render obvious the Asserted Claims of the Asserted

Patents. As noted above, however, discovery is ongoing, and Defendants' prior art investigation and third party discovery are therefore not yet complete. Accordingly, Defendants reserve the right to present additional items of prior art under 35 U.S.C. § 102(a), (b), (e), (f) and/or (g), and/or § 103 that are located during the course of discovery or further investigation. For example, Defendants expect to issue subpoenas to third parties believed to have knowledge, documentation, and/or corroborating evidence concerning some of the prior art listed in these Contentions and/or additional prior art. These third parties include, without limitation, the authors, inventors, or assignees of the references listed in these Contentions. In addition, Defendants reserve the right to assert invalidity under 35 U.S.C. §§ 102(c) or (d) to the extent that discovery or further investigation yields information forming the basis thereof.

1. Prior Art Patents and Published Patent Applications

Defendants disclose the following prior art patents and patent application publications:

a. '721 Patent

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
A-01	5,956,408	US	Arnold	Filed Sep. 1994	Arnold '408
A-02	6,067,575	US	McManis	Filed Dec. 1995 Published May 2000	McManis '575
A-03	5,200,999	US	Matyas	Filed Sep. 1991 Published April 1993	Matyas
A-04	5,757,918	US	Hopkins	Filed Jan. 1995 Published May 1998	Hopkins

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
A-05	5,724,425	US	Chang	Filed Jun. 1994 Published Mar. 1998	Chang
A-06	4,634,807	US	Chorley	Filed August 1985 Published January 1987	Chorley
A-07	5,768,389	US	Ishii	Filed June 1996 Published June 1998	Ishii
A-08	5,557,518	US	Rosen	File Apr. 1994 Published Sep. 1996	Rosen ‘518
A-09	4,351,982	US	Miller	Published Sep. 1982	Miller
A-10	5,388,211	US	Hornbuckle	Filed Apr. 1989 Published Feb. 1995	Hornbuckle
A-11	5,412,717	US	Fischer	Filed May 1992 Published May 1995	Fischer ’717
A-12	1995019672	WO	Sudia	Filed January 1995 Published July 1995	Sudia
A-13	4,817,140	US	Chandra	Published Mar. 1989	Chandra
A-14	5,910,987	US	Ginter	Filed Feb. 1995	Ginter ‘987

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	5,933,503	US	Schell	Filed Mar. 1996 Published Aug. 1999	Schell
	5,625,693	US	Rohatgi	Filed Jul. 1995 Published Apr. 1997	Rohatgi
	5,740,441	US	Yellin	Filed Dec. 1995 Published Apr. 1998	Yellin ’441
	5712,914	US	Aucsmith	Filed Sep. 1995 Published Jan. 1998	Aucsmith ’914
	5,757,915	US	Aucsmith	Filed August 1995 Published May 1998	Aucsmith ’915
	7,095,854	US	Ginter	Filed Oct. 2000 Published Aug. 2006	Ginter ‘854
	5,218,605	US	Low	Filed Jan. 1990 Published Jun. 1993	Low
	5,689,565	US	Spelman	Published 1997	Spelman
	6,075,863	US	Krishnan	Filed Aug. 1996 Published Jun. 2000	Krishnan

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	5,475,839	US	Watson	Filed Nov. 1994 Published Dec. 1995	Watson
	5,812,763	US	Teng	Filed Jan. 1993 Published Sept. 1998	Teng
	6,151,643	US	Cheng	Filed Jun. 1996 Published Nov. 2000	Cheng
	5,889,943	US	Ji	Filed Mar. 1996 Published Mar. 1999	Ji
	5,745,678	US	Herzberg	Filed Aug. 1997 Published Apr. 1998	Herzberg
	5,291,598	US	Grundy	Filed Apr. 1992 Published Mar. 1994	Grundy
	5,696,822	US	Nachenberg	Filed Sept. 1995 Published Dec. 1997	Nachenberg
	5,452,442	US	Kephart	Filed Apr. 1995 Published Sept. 1995	Kephart
	5,440,723	US	Arnold	Filed Jan. 1993 Published Aug. 1995	Arnold ’723

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	5,787,172	US	Arnold	Filed Feb. 1994 Published Jul. 1998	Arnold ’172
	5,898,154	US	Rosen	Filed Jan. 1995 Published Apr. 1999	Rosen ‘154
	5,812,666	US	Baker	Filed Oct. 1995 Published Sept. 1998	Baker
	5,371,692	US	Draeger	Filed Mar. 1991 Published Dec. 1994	Draeger
	5,768,288	US	Jones	Filed Mar. 1996 Published Jun. 1998	Jones
	5,666,416	US	Micali	Filed Nov. 1995 Published Sept. 1997	Micali ’416
	5,604,804	US	Micali	Filed April 1996 Published February 1997	Micali ’804
	5,634,012	US	Stefik	Filed: November 1994 Published: May 1997	Stefik ’012
	5,715,403	US	Stefik	Filed November 1994	Stefik ’403

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
				Published February 1998	
	5,629,980	US	Stefik	Filed November 1994 Published May 1997	Stefik ’980
	5,311,591	US	Fischer	Filed May 1992 Published May 1994	Fischer ’591
	5,978,484	US	Apperson	Filed April 1996 Published November 1999	Apperson
	6,266,416	US	Sigbjornsen	Filed July 1996 Published July 2001	Sigbjornsen
	5,768,389	US	Ishii	Filed June 1996 Published June 1998	Ishii
	6,263,442	US	Mueller	Filed May 1996 Published July 2001	Mueller
	5,421,006	US	Jablon	Filed April 1994 Published May 1995	Jablon
	5,355,479	US	Torii	Filed January 1992	Torii

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
				Published October 1994	
	4,860,203	US	Corrigan	Filed September 1986 Published August 1989	Corrigan

b. <u>'304 Patent</u>

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
B-01	0,268,139	EP	Comerford	Filed: 11/05/1986	Comerford
B-02	5,237,610	US	Gammie	Filed: 03/29/1991 Issued: 08/17/1993	Gammie
B-03	5,388,211	US	Hornbuckle	Filed: 04/20/1993 Issued: 02/07/1995	Hornbuckle
B-04	5,010,571	US	Katznelson	Filed: 09/10/1986 Issued: 04/23/1991	Katznelson
B-05	4,918,728	US	Matyas	Filed: 08/30/1989 Issued: 04/17/1990	Matyas
B-06	5,504,933	US	Saito	Filed: 10/26/1993 Issued: 04/02/1996	Saito

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
B-07	4,866,770	US	Seth-Smith	Filed: 08/14/1986 Issued: 09/12/1989	Smith
B-08	2,095,723	CA	Waite	Filed: 11/06/1991 Issued/Published: 05/29/1992	Waite
B-12	4,634,807	US	Chorley	Filed: 08/23/1985 Issued: 01/06/1987	Chorley
B-13	5,499,298	US	Narasimhalu	Filed: 03/17/1994 Issued: 03/12/1996	Narasimhalu
	4,558,176	US	Arnold	Filed: 09/20/1982 Issued: 12/10/1985	
	4,817,140	US	Chandra	Filed: 11/05/1986 Issued: 03/28/1989	
	4,868,736	US	Walker	Filed: 08/10/1987 Issued: 09/19/1989	
	4,977,594	US	Shear	Filed: 02/16/1989 Issued: 12/11/1990	
	5,155,680	US	Wiedemer	Filed: 04/27/1989 Issued: 10/13/1992	

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	5,666,411	US	McCarty	Filed: 01/13/1994 Issued: 09/09/1997	
	5,796,824	US	Hasebe	Filed: 02/20/1996 Priority: 03/15/1993	
	5,986,690	US	Hendricks	Filed: 11/07/1994 Issued: 11/16/1999	
	0,585,833	EP	Heikkinen	Priority: 09/04/1992 Published: 03/09/1994	
	4,829,569	US	Seth-Smith	Filed: 07/08/1986 Issued: 05/09/1989	
	4,916,738	US	Chandra	Filed: 11/05/1986 Issued: 04/10/1990	
	0,132,007	EP	Crowther	Filed: 07/11/1984 Published: 09/30/1987	
	4,817,142	US	Van Rassel	Filed: 05/21/1985 Issued: 03/28/1989	
	4,907,273	US	Wiedemer	Filed: 09/22/1987 Issued: 03/06/1990	

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	5,202,920	US	Takahashi	Filed: 10/29/1991 Issued: 04/13/1993	
	5,319,705	US	Halter	Filed: 10/21/1992 Issued: 06/07/1994	
	5,416,842	US	Aziz	Filed: 06/10/1994 Issued: 05/16/1995	
	5,506,904	US	Sheldrick	Filed: 12/03/1993 Issued: 04/09/1996	
	5,519,780	US	Woo	Filed: 12/03/1993 Issued: 05/21/1996	
	5,715,403	US	Stefik	Filed: 11/23/1994 Issued: 02/03/1998	
	5,539,828	US	Davis	Filed: 05/31/1994 Issued: 07/23/1996	
	5,473,692	US	Davis	Filed: 09/07/1994 Issued: 12/05/1995	
	5,568,552	US	Davis	Filed: 06/07/1995 Issued: 10/22/1996	

c. **’815 Patent**

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
C-01	5,907,619	US	Davis	May 25, 1999	Davis
C-02	6,697,948	US	Rabin	February 24, 2004	Rabin
C-03	WO199904 0702A1	WIPO	Hanna	August 12, 1999	Hanna
C-04	6,009,176	US	Gennaro	December 28, 1999	Gennaro
C-05	5,625,693	US	Rohatgi	April 29, 1997	Rohatgi
C-06	5,958,051	US	Renaud	September 28, 1999	Renaud
C-07	5,629,980	US	Stefik	May 13, 1997	Stefik ’980
C-08	5,499,294	US	Friedman	March 12, 1996	Friedman
C-09	5,754,659	US	Sprunk	May 19, 1998	Sprunk
C-10	5,892,900	US	Ginter	April 6, 1999	Ginter
C-11	6,668,246	US	Yeung	December 23, 2003	Yeung
C-12	5,968,175	US	Morishita	October 19, 1999	Morishita
C-13	6,230,268	US	Miwa	May 8, 2001	Miwa
	4,881,264	US	Merkle	November 4, 1989	Merkle
	6,061,449	US	Sprunk	May 9, 2000	Sprunk
	5,664,016	US	Preneel	September 2, 1997	Preneel
	5,646,997	US	Barton	July 8, 1997	Barton
	6,311,271	US	Gennaro	October 30, 2001	Gennaro ‘271

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	WO/1996/025814	WIPO	Chaum	August 22, 1996	Chaum
	6,587,563	US	Crandall	July 1, 2003	Crandall
	6,292,919	US	Fries	September 18, 2001	Fries
	5,321,704	US	Erickson	June 14, 1994	Erickson
	4,074,066	US	Ehrsam	February 14, 1978	Ehrsam
	5,991,399	US	Graunke	November 23, 1999	Graunke
	6,418,421	US	Hurtado	September 7, 2002	Hurtado
	6,480,961	US	Rajasekharan	December 11, 2002	Rajasekharan
	5,014,234	US	Gordon	July 5, 1991	Gordon
	6,272,634	US	Tewfik	August 7, 2001	Tewfik
	6,952,774	US	Malvar	October 4, 2005	Malvar
	6,668,246	US	Yeo	December 23, 2003	Yeo
	6,226,618	US	Downs	May 01, 2001	Downs
	7,346,580	US	Lisanke	March 18, 2008	Lisanke
	US 2002/0164026A1	US	Huima	November 7, 2002	Huima
	RE37,178 E	US	Kingdon	May 15, 2001	Kingdon
	WO9724675	WIPO	Eldridge	July 10, 1997	Eldridge
	5,666,415	US	Kaufman	September 9, 1997	Kaufman

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	7,194,092	US	England	March 20, 2007	England
	7,319,759	US	Peinado	January 15, 2008	Peinado
	5,313,471	US	Otaka	May 17,1994	Otaka
	6,049,612	US	Fielder	April 11, 2000	Fielder
	6,209,111	US	Kadyk	March 27, 2001	Kadyk

d. <u>'602 Patent</u>

App.	Patent or App. Publ. No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
D-01	4,881,264	US	Merkle	November 4, 1989	Merkle
D-02	6,061,449	US	Sprunk	May 9, 2000	Sprunk
D-03	5,664,016	US	Preneel	September 2, 1997	Preneel
D-04	5,646,997	US	Barton	July 8, 1997	Barton
D-05	6,311,271	US	Gennaro	October 30, 2001	Gennaro '271
D-06	WO/1996/025814	WIPO	Chaum	August 22, 1996	Chaum
D-07	6,587,563	US	Crandall	July 1, 2003	Crandall
D-08	6,292,919	US	Fries	September 18, 2001	Fries
D-09	6,230,268	US	Miwa	May 8, 2001	Miwa
D-10	5,321,704	US	Erickson	June 14, 1994	Erickson
D-11	4,074,066	US	Ehrsam	February 14, 1978	Ehrsam

App.	Patent or App. Publ. No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
D-19	5,313,471	US	Otaka	May 17,1994	Otaka
D-20	6,049,612	US	Fielder	April 11, 2000	Fielder
D-21	6,209,111	US	Kadyk	March 27, 2001	Kadyk
D-22	RE37,178 E	US	Kingdon	May 15, 2001	Kingdon
D-23	7,194,092	US	England	March 20, 2007	England
D-24	5,666,415	US	Kaufman	September 9, 1997	Kaufman
	5,907,619	US	Davis	May 25, 1999	Davis
	6,697,948	US	Rabin	February 24, 2004	Rabin
	WO199904 0702A1	WIPO	Hanna	August 12, 1999	Hanna
	6,009,176	US	Gennaro	December 28, 1999	Gennaro
	5,625,693	US	Rohatgi	April 29, 1997	Rohatgi
	5,958,051	US	Renaud	September 28, 1999	Renaud
	5,629,980	US	Stefik	May 13, 1997	Stefik ’980
	5,499,294	US	Friedman	March 12, 1996	Friedman
	5,754,659	US	Sprunk	May 19, 1998	Sprunk
	5,892,900	US	Ginter	April 6, 1999	Ginter
	6,668,246	US	Yeung	December 23, 2003	Yeung

App.	Patent or App. Publ. No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	5,991,399	US	Graunke	November 23, 1999	Graunke
	6,418,421	US	Hurtado	September 7, 2002	Hurtado
	6,480,961	US	Rajasekharan	December 11, 2002	Rajasekharan
	5,014,234	US	Gordon	July 5, 1991	Gordon
	6,272,634	US	Tewfik	August 7, 2001	Tewfik
	6,952,774	US	Malvar	October 4, 2005	Malvar
	6,668,246	US	Yeo	December 23, 2003	Yeo
	6,226,618	US	Downs	May 01, 2001	Downs
	7,346,580	US	Lisanke	March 18, 2008	Lisanke
	US 2002/0164026A1	US	Huima	November 7, 2002	Huima
	WO9724675	WIPO	Eldridge	July 10, 1997	Eldridge
	7,319,759	US	Peinado	January 15, 2008	Peinado

e. ’603 Patent

App.	Patent or App. Publ. No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
E-01	6,505,300	US	Chan	January 7, 2003	Chan
E-02	5,870,467	US	Imai	February 9, 1999	Imai

App.	Patent or App. Publ. No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
E-03	6,314,409	US	Schneck	November 6, 2001	Schneck
E-04	5,673,315	US	Wolf	September 30, 1997	Wolf
E-05	5,737,416	US	Cooper	April 7, 1998	Cooper
E-06	2007/0211891	US	Shamoon	September 13, 2007	Shamoon
E-07	4,558,176	US	Arnold	December 10, 1985	Arnold
E-08	8,370,956	US	Stefik	February 5, 2013	Stefik
E-09	5,940,504	US	Griswold	August 17, 1999	Griswold
E-10	5,388,211	US	Hornbuckle	February 7, 1995	Hornbuckle
E-11	6,510,516	US	Benson	January 21, 2003	Benson
E-14	7,319,759	US	Peinado	January 15, 2008	Peinado
E-15	6,820,063	US	England	November 16, 2004	England ’063
E-16	7,346,580	US	Lisanke	March 18, 2008	Lisanke
	5,991,399	US	Graunke	November 23, 1999	Graunke
	6,418,421	US	Hurtado	September 7, 2002	Hurtado
	6,480,961	US	Rajasekharan	December 11, 2002	Rajasekharan
	5,014,234	US	Edwards	July 5, 1991	Edwards
	6,510,516	US	Franklin	January 21, 2003	Franklin
	5,815,571	US	Finley	September 29, 1998	Finley
	5,421,006	US	Jablon	May 30, 1995	Jablon

App.	Patent or App. Publ. No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	6,775,779	US	England	August 10, 2004	England ’779
	5,745,678	US	Herzberg	April 28, 1998	Herzberg
	7,103,574	US	Peinado	September 5, 2006	Peinado
	6,253,374	US	Dresevic	June 26, 2001	Dresevic
	6,073,239	US	Dotan	June 6, 2000	Dotan
	6,226,618	US	Downs	Filed: 08/03/98	Downs
	6,920,657	US	Doherty	Filed: 04/07/2000 Priority: 04/07/1999	Doherty
	6,772,340	US	Peinado	Filed: 03/15/00 Priority: 01/14/00	Peinado
	6,996,720	US	DeMello	Priority: 12/17/99	DeMello
	5,629,980	US	Stefik	Issued: 05/13/97	Stefik ’980
	6,233,684	US	Stefik	Filed: 10/10/97	Stefik ’684
	7,047,241	US	Erickson	Filed: 10/11/96	Erickson
	6,944,776	US	Lockhart	Filed: 04/12/00 Priority: 04/12/99	Lockhart
	2002/ 0012432	US	England	Priority 03/27/99	England ’432
	6,792,113	US	Ansell	Filed: 12/20/99	Ansell

App.	Patent or App. Publ. No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	5,010,571	US	Katznelson	Issued: 04/23/1991	Katznelson
	5,388,211	US	Hornbuckle	Issued: 02/07/1995	Hornbuckle
	5,892,900	US	Ginter	Issued: 04/06/1999	Ginter ’900
	6,157,721	US	Shear	Filed: 08/12/1996	Shear
	5,634,012	US	Stefik	Issued: 05/27/1997	Stefik ’012
	6,236,971	US	Stefik	Filed: 11/10/1997	Stefik ’971
	5,757,907	US	Cooper	Issued: 05/26/1998	
	5,638,443	US	Stefik	Issued: 06/10/1997	
	5,715,403	US	Stefik	Issued: 02/03/1998	
	5,657,390	US	Elgamal et al.	Issued: 09/12/1997	Elgamal ’390
	5,671,279	US	Elgamal	Issued: 09/23/1997	Elgamal ’279
	5,825,877	US	Asti	Issued: 10/20/1998	
	5,910,987	US	Ginter	Issued: 06/08/1999	
	5,925,127	US	Ahmad	Issued: 07/20/1999	
	5,991,399	US	Graunke	Issued: 11/23/1999	
	6,073,124	US	Krishnan	Issued: 06/06/2000	
	6,094,485	US	Weinstein et al.	Filed: 09/18/1997	Weinstein

App.	Patent or App. Publ. No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	6,135,646	US	Kahn	Filed: 02/28/1997	
	6,138,107	US	Elgamal	Filed: 01/04/1996	Elgamal 107
	6,170,060	US	Mott	Filed: 10/3/1997	
	6,189,097	US	Tycksen	Filed: 03/24/1997	
	6,223,291	US	Puhl	Filed: 03/26/1999	
	6,233,684	US	Stefik	Filed 10/10/1997	Stefik ’684
	6,260,043	US	Puri	Filed: 11/06/1998	
	6,301,660	US	Benson	Filed: 03/23/1998	
	6,367,019	US	Ansell	Filed: 03/26/1999	
	6,389,538	US	Gruse	Filed: 08/22/1998	Gruse ’538
	6,398,245	US	Gruse	Filed: 12/01/1998	Gruse ’245
	6,412,070	US	Van Dyke	Filed: 09/21/1998	
	6,418,421	US	Hurtado	Filed: 12/10/1998	
	6,438,235	US	Sims	Filed: 08/05/1998	
	6,463,534	US	Geiger	Filed: 03/26/1999	
	6,513,121	US	Serkowski	Filed: 07/20/1999	
	6,519,700	US	Ram	Filed: 10/23/1998	

App.	Patent or App. Publ. No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	6,532,542	US	Thomlinson	Filed: 11/25/1997	
	6,574,609	US	Downs	Filed: 09/14/1998	Downs 609
	6,582,310	US	Walker	Filed: 12/17/1999	
	6,587,837	US	Spagna	Filed: 12/01/1998	Spagna
	6,697,944	US	Jones	Filed: 10/1/1999	
	6,775,655	US	Peinado	Filed: 11/24/1999	
	6,873,975	US	Hatakeyama	Filed: 3/8/2000	
	6,885,748	US	Wang	Filed: 3/24/2000	
	6,904,523	US	Bialick	Priority: 03/08/1999	
	6,944,669	US	Saccocio	Priority: 10/22/1999	Saccocio
	6,959,288	US	Medina	Filed: 02/01/1999	Medina
	7,013,390	US	Elgamal et al.	Priority: 06/30/1997	Elgamal 390
	7,020,704	US	Lipscomb	Priority: 10/5/1999	
	7,068,787	US	Ta	Filed: 03/24/2000	
	7,155,415	US	Russell	Priority: 04/07/2000	
	7,206,748	US	Gruse	Filed: 12/10/1998	Gruse 748
	7,209,892	US	Galuten	Filed: 12/23/1999	

App.	Patent or App. Publ. No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	7,225,165	US	Kyojima	Priority: 02/01/2000	
	7,353,209	US	Peinado	Filed: 03/15/2000	
	7,424,543	US	Rice	Priority: 09/08/1999	
	7,523,072	US	Stefik	Priority: 11/23/1994	Stefik ’072
	7,626,691	US	Maari	Priority: 03/24/1998	
	8,370,956	US	Stefik	Priority: 11/23/1994	Stefik ’956
	7,861,312	US	Lee	Priority: 01/06/2000	
	8,091,025	US	Ramos	Priority: 03/24/2000	
	8,175,977	US	Story	Filed: 12/28/1998	
	2002/ 0003886	US	Hillegass	Priority: 04/28/2000	
	2002/ 0059364	US	Coulthard	Filed: 02/08/1999	
	2004/ 0125957	US	Rauber	Priority: 04/11/2000	
	1998/ 010381	WO	Shear	Published: 03/12/1998	
	1999/ 045491	WO	Eberhard	Published: 09/10/1999	
	6,088,801	US	Grecsek	Filed: 01/10/1997	

f. ’342 and ’106 Patents

App.	Patent or App. Publ. No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
F-01, I-01	6,226,618	US	Downs	Filed: 08/03/98	Downs
F-02, I-02	6,920,657	US	Doherty	Filed: 04/07/2000 Priority: 04/07/1999	Doherty
F-03, I-03	6,772,340	US	Peinado	Filed: 03/15/00 Priority: 01/14/00	Peinado
F-04, I-04	6,996,720	US	DeMello	Priority: 12/17/99	DeMello
F-05, I-05	5,629,980	US	Stefik	Issued: 05/13/97	Stefik ’980
F-06, I-06	6,233,684	US	Stefik	Filed: 10/10/97	Stefik ’684
F-07, I-07	7,047,241	US	Erickson	Filed: 10/11/96	Erickson
F-08, I-08	6,944,776	US	Lockhart	Filed: 04/12/00 Priority: 04/12/99	Lockhart
F-09, I-09	2002/ 0012432	US	England	Priority 03/27/99	England ’432
F-10, I-10	6,820,063	US	England	Filed: 01/08/99 Priority: 10/26/98	England ’063
F-11, I-11	6,792,113	US	Ansell	Filed: 12/20/99	Ansell
I-12	5,010,571	US	Katznelson	Issued: 04/23/1991	Katznelson

App.	Patent or App. Publ. No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
I-13	5,388,211	US	Hornbuckle	Issued: 02/07/1995	Hornbuckle
F-18 I-14	5,892,900	US	Ginter	Issued: 04/06/1999	Ginter ’900
F-19, I-21	6,157,721	US	Shear	Filed: 08/12/1996	Shear
F-20, I-22	5,634,012	US	Stefik	Issued: 05/27/1997	Stefik ’012
F-21, I-23	6,236,971	US	Stefik	Filed: 11/10/1997	Stefik ’971
F-22, I-24	5,991,399	US	Graunke	Issued: 11/23/1999	Graunke
F-23, I-25	6,611,812	US	Hurtado	Filed: 08/17/1999	Hurtado
	5,757,907	US	Cooper	Issued: 05/26/1998	
	5,638,443	US	Stefik	Issued: 06/10/1997	
	5,715,403	US	Stefik	Issued: 02/03/1998	
	5,657,390	US	Elgamal et al.	Issued: 09/12/1997	Elgamal ’390
	5,671,279	US	Elgamal	Issued: 09/23/1997	Elgamal ’279
	5,825,877	US	Asti	Issued: 10/20/1998	
	5,910,987	US	Ginter	Issued: 06/08/1999	
	5,925,127	US	Ahmad	Issued: 07/20/1999	
	5,991,399	US	Graunke	Issued: 11/23/1999	
	6,073,124	US	Krishnan	Issued: 06/06/2000	

App.	Patent or App. Publ. No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	6,094,485	US	Weinstein et al.	Filed: 09/18/1997	Weinstein
	6,135,646	US	Kahn	Filed: 02/28/1997	
	6,138,107	US	Elgamal	Filed: 01/04/1996	Elgamal 107
	6,170,060	US	Mott	Filed: 10/3/1997	
	6,189,097	US	Tycksen	Filed: 03/24/1997	
	6,223,291	US	Puhl	Filed: 03/26/1999	
	6,233,684	US	Stefik	Filed 10/10/1997	Stefik ’684
	6,260,043	US	Puri	Filed: 11/06/1998	
	6,301,660	US	Benson	Filed: 03/23/1998	
	6,367,019	US	Ansell	Filed: 03/26/1999	
	6,389,538	US	Gruse	Filed: 08/22/1998	Gruse ’538
	6,398,245	US	Gruse	Filed: 12/01/1998	Gruse ’245
	6,412,070	US	Van Dyke	Filed: 09/21/1998	
	6,418,421	US	Hurtado	Filed: 12/10/1998	
	6,438,235	US	Sims	Filed: 08/05/1998	
	6,463,534	US	Geiger	Filed: 03/26/1999	
	6,513,121	US	Serkowski	Filed: 07/20/1999	

App.	Patent or App. Publ. No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	6,519,700	US	Ram	Filed: 10/23/1998	
	6,532,542	US	Thomlinson	Filed: 11/25/1997	
	6,574,609	US	Downs	Filed: 09/14/1998	Downs 609
	6,582,310	US	Walker	Filed: 12/17/1999	
	6,587,837	US	Spagna	Filed: 12/01/1998	Spagna
	6,697,944	US	Jones	Filed: 10/1/1999	
	6,775,655	US	Peinado	Filed: 11/24/1999	
	6,873,975	US	Hatakeyama	Filed: 3/8/2000	
	6,885,748	US	Wang	Filed: 3/24/2000	
	6,904,523	US	Bialick	Priority: 03/08/1999	
	6,944,669	US	Saccocio	Priority: 10/22/1999	Saccocio
	6,959,288	US	Medina	Filed: 02/01/1999	Medina
	7,013,390	US	Elgamal et al.	Priority: 06/30/1997	Elgamal 390
	7,020,704	US	Lipscomb	Priority: 10/5/1999	
	7,068,787	US	Ta	Filed: 03/24/2000	
	7,155,415	US	Russell	Priority: 04/07/2000	
	7,206,748	US	Gruse	Filed: 12/10/1998	Gruse 748

App.	Patent or App. Publ. No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	7,209,892	US	Galuten	Filed: 12/23/1999	
	7,225,165	US	Kyojima	Priority: 02/01/2000	
	7,353,209	US	Peinado	Filed: 03/15/2000	
	7,424,543	US	Rice	Priority: 09/08/1999	
	7,523,072	US	Stefik	Priority: 11/23/1994	Stefik ’072
	7,626,691	US	Maari	Priority: 03/24/1998	
	8,370,956	US	Stefik	Priority: 11/23/1994	Stefik ’956
	7,861,312	US	Lee	Priority: 01/06/2000	
	8,091,025	US	Ramos	Priority: 03/24/2000	
	8,175,977	US	Story	Filed: 12/28/1998	
	2002/ 0003886	US	Hillegass	Priority: 04/28/2000	
	2002/ 0059364	US	Coulthard	Filed: 02/08/1999	
	2004/ 0125957	US	Rauber	Priority: 04/11/2000	
	1998/ 010381	WO	Shear	Published: 03/12/1998	
	1999/ 045491	WO	Eberhard	Published: 09/10/1999	

g. ’157 Patent

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
G-01	0,268,139	EP	Comerford	Filed: 11/05/1986	Comerford
G-02	5,237,610	US	Gammie	Filed: 03/29/1991 Issued: 08/17/1993	Gammie
G-03	5,388,211	US	Hornbuckle	Filed: 04/20/1993 Issued: 02/07/1995	Hornbuckle
G-04	5,010,571	US	Katznelson	Filed: 09/10/1986 Issued: 04/23/1991	Katznelson
G-05	4,918,728	US	Matyas	Filed: 08/30/1989 Issued: 04/17/1990	Matyas
G-06	5,504,933	US	Saito	Filed: 10/26/1993 Issued: 04/02/1996	Saito
G-07	4,866,770	US	Seth-Smith	Filed: 08/14/1986 Issued: 09/12/1989	Smith
G-08	2,095,723	CA	Waite	Filed: 11/06/1991 Issued/Published: 05/29/1992	Waite
G-12	4,634,807	US	Chorley	Filed: 08/23/1985 Issued: 01/06/1987	Chorley

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
G-13	5,499,298	US	Narasimhalu	Filed: 03/17/1994 Issued: 03/12/1996	Narasimhalu
	4,558,176	US	Arnold	Filed: 09/20/1982 Issued: 12/10/1985	
	4,817,140	US	Chandra	Filed: 11/05/1986 Issued: 03/28/1989	
	4,868,736	US	Walker	Filed: 08/10/1987 Issued: 09/19/1989	
	4,977,594	US	Shear	Filed: 02/16/1989 Issued: 12/11/1990	
	5,155,680	US	Wiedemer	Filed: 04/27/1989 Issued: 10/13/1992	
	5,666,411	US	McCarty	Filed: 01/13/1994 Issued: 09/09/1997	
	5,796,824	US	Hasebe	Filed: 02/20/1996 Priority: 03/15/1993	
	5,986,690	US	Hendricks	Filed: 11/07/1994 Issued: 11/16/1999	
	0,585,833	EP	Heikkinen	Priority: 09/04/1992	

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
				Published: 03/09/1994	
	4,829,569	US	Seth-Smith	Filed: 07/08/1986 Issued: 05/09/1989	
	4,916,738	US	Chandra	Filed: 11/05/1986 Issued: 04/10/1990	
	0,132,007	EP	Crowther	Filed: 07/11/1984 Published: 09/30/1987	
	4,817,142	US	Van Rassel	Filed: 05/21/1985 Issued: 03/28/1989	
	4,907,273	US	Wiedemer	Filed: 09/22/1987 Issued: 03/06/1990	
	5,202,920	US	Takahashi	Filed: 10/29/1991 Issued: 04/13/1993	
	5,319,705	US	Halter	Filed: 10/21/1992 Issued: 06/07/1994	
	5,416,842	US	Aziz	Filed: 06/10/1994 Issued: 05/16/1995	
	5,506,904	US	Sheldrick	Filed: 12/03/1993 Issued: 04/09/1996	

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	5,519,780	US	Woo	Filed: 12/03/1993 Issued: 05/21/1996	
	5,715,403	US	Stefik	Filed: 11/23/1994 Issued: 02/03/1998	
	5,539,828	US	Davis	Filed: 05/31/1994 Issued: 07/23/1996	
	5,473,692	US	Davis	Filed: 09/07/1994 Issued: 12/05/1995	
	5,568,552	US	Davis	Filed: 06/07/1995 Issued: 10/22/1996	

h. ’158 Patent

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
H-01	0,268,139	EP	Comerford	Filed: 11/05/1986	Comerford
H-02	5,237,610	US	Gammie	Filed: 03/29/1991 Issued: 08/17/1993	Gammie
H-03	5,388,211	US	Hornbuckle	Filed: 04/20/1993 Issued: 02/07/1995	Hornbuckle

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
H-04	5,010,571	US	Katznelson	Filed: 09/10/1986 Issued: 04/23/1991	Katznelson
H-05	4,918,728	US	Matyas	Filed: 08/30/1989 Issued: 04/17/1990	Matyas
H-06	5,504,933	US	Saito	Filed: 10/26/1993 Issued: 04/02/1996	Saito
H-07	4,866,770	US	Seth-Smith	Filed: 08/14/1986 Issued: 09/12/1989	Smith
H-08	2,095,723	CA	Waite	Filed: 11/06/1991 Issued/Published: 05/29/1992	Waite
H-12	4,634,807	US	Chorley	Filed: 08/23/1985 Issued: 01/06/1987	Chorley
H-13	5,499,298	US	Narasimhalu	Filed: 03/17/1994 Issued: 03/12/1996	Narasimhalu
	4,558,176	US	Arnold	Filed: 09/20/1982 Issued: 12/10/1985	
	4,817,140	US	Chandra	Filed: 11/05/1986 Issued: 03/28/1989	

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	4,868,736	US	Walker	Filed: 08/10/1987 Issued: 09/19/1989	
	4,977,594	US	Shear	Filed: 02/16/1989 Issued: 12/11/1990	
	5,155,680	US	Wiedemer	Filed: 04/27/1989 Issued: 10/13/1992	
	5,666,411	US	McCarty	Filed: 01/13/1994 Issued: 09/09/1997	
	5,796,824	US	Hasebe	Filed: 02/20/1996 Priority: 03/15/1993	
	5,986,690	US	Hendricks	Filed: 11/07/1994 Issued: 11/16/1999	
	0,585,833	EP	Heikkinen	Priority: 09/04/1992 Published: 03/09/1994	
	4,829,569	US	Seth-Smith	Filed: 07/08/1986 Issued: 05/09/1989	
	4,916,738	US	Chandra	Filed: 11/05/1986 Issued: 04/10/1990	
	0,132,007	EP	Crowther	Filed: 07/11/1984	

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
				Published: 09/30/1987	
	4,817,142	US	Van Rassel	Filed: 05/21/1985 Issued: 03/28/1989	
	4,907,273	US	Wiedemer	Filed: 09/22/1987 Issued: 03/06/1990	
	5,202,920	US	Takahashi	Filed: 10/29/1991 Issued: 04/13/1993	
	5,319,705	US	Halter	Filed: 10/21/1992 Issued: 06/07/1994	
	5,416,842	US	Aziz	Filed: 06/10/1994 Issued: 05/16/1995	
	5,506,904	US	Sheldrick	Filed: 12/03/1993 Issued: 04/09/1996	
	5,519,780	US	Woo	Filed: 12/03/1993 Issued: 05/21/1996	
	5,715,403	US	Stefik	Filed: 11/23/1994 Issued: 02/03/1998	
	5,539,828	US	Davis	Filed: 05/31/1994 Issued: 07/23/1996	

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	5,473,692	US	Davis	Filed: 09/07/1994 Issued: 12/05/1995	
	5,568,552	US	Davis	Filed: 06/07/1995 Issued: 10/22/1996	

i. <u>'627 Patent</u>

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
J-01	7,110,542	US	Tripathy	Filed Dec. 1990 Published Sept. 2006	Tripathy
J-02	6,985,589	US	Morley	Filed Dec. 1999	Morley '589
J-03	1999059335	WO	Morley	Published Nov. 1999	Morley '335
J-04	5,818,936	US	Mashayekhi	Filed Mar. 1996 Published Oct. 1998	Mashayekhi
J-05	20070192252	US	Shear	Filed May 15, 1997	Shear
J-06	5,237,610	US	Gammie	Published Aug. 1993	Gammie
J-07	7,111,172	US	Duane	Filed July 1999 Published Sept. 2006	Duane
J-08	98/042101	WO	Smith	Filed Mar. 1998	Smith

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
				Published Sept. 1998	
J-09	5,910,987	US	Ginter	Filed Feb. 1995	Ginter '987
J-10	0 887 723	EP	Ciacelli	Filed May 1998 Published Dec. 1998	Ciacelli
J-11	6,697,489	US	Candelore	Filed Feb. 2000 Published Feb. 2004	Candelore
J-13	6,236,971	US	Stefik	Filed Nov. 1997 Published May 2001	Stefik '971
J-18	99/48296	WO	Shamoon	Published Sep. 1999	Shamoon '296
	6,170,058	US	Kausik	Filed Dec. 1997 Published Jan. 2001	Kausik
	5,473,687	US	Lipscomb	Filed Dec. 1993 Published Dec. 1995	Lipscomb
	6,141,754	US	Choy	Filed Nov. 1997 Published Oct. 2000	Choy
	6,055,314	US	Spies	Filed Mar. 1996 Published Apr. 2000	Spies

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	6,973,444	US	Blinn	Filed Jan. 2000 Published Dec. 2005	Blinn
	5,649,187	US	Hornbuckle	Filed Sept. 1995 Published Jul. 1997	Hornbuckle
	6,064,993	US	Ryan	Filed Dec. 1997 Published May 2000	Ryan
	6,289,450	US	Pensak	Filed May 1999 Published Sept. 2001	Pensak
	6,230,272	US	R. Lockhart	Filed Oct. 1997 Published May 2001	Lockhart ’272
	6,944,776	US	M. Lockhart	Filed Apr. 2000 Published Sept. 2005	Lockhart ’776
	6,741,853	US	Lee	Filed Nov. 2000 Published May 2004	Lee
	2002/0078253	US	Szondy	Filed Dec. 2000 Published June 2002	Szondy
	2002/0042831	US	Capone	Filed Apr. 2001 Published Apr. 2002	Capone

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	1 047 240	EP	Huang	Filed Mar. 2000 Published Nov. 2004	Huang
	2002/0071559	US	Christensen	Filed Dec. 2000 Published June 2002	Christensen
	2002/0071561	US	Kurn	Filed Dec. 2000 Published June 2002	Kurn
	7,398,556	US	Erickson	Filed Feb. 2004 Published Jul. 2008	Erickson
	6,792,113	US	Ansell	Filed Dec. 1999 Published Sept. 2004	Ansell
	5,999,629	US	Heer	Filed Oct. 1995 Published Dec. 1999	Heer
	6,398,245	US	Gruse	Filed Dec. 1998 Published June 2002	Gruse
	6,457,125	US	Matthews	Filed Dec. 1998 Published Sept. 2002	Matthews
	6,687,683	US	Harada	Filed Oct. 1999 Published Feb. 2004	Harada

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	6,550,011	US	Sims	Filed Oct. 1999 Published Apr. 2003	Sims
	6,160,891	US	Al-Salqan	Filed Oct. 1997 Published Dec. 2000	Al-Salqan
	6,367,011	US	Lee	Filed Oct. 1998 Published Apr. 2002	Lee
	5,619,574	US	Johnson	Filed Feb. 1995 Published Apr. 1997	Johnson
	5,048,085	US	Abraham	Filed Oct. 1989 Published Sept. 1991	Abraham
	6,976,165	US	Carpenter	Filed Sept. 1999 Published Dec. 2005	Carpenter
	6,449,720	US	Sprague	Filed May 1999 Published Sept. 2002	Sprague
	6,052,468	US	Hillhouse	Filed Jan. 1998 Published Apr. 2000	Hillhouse
	6,898,706	US	Venkatesan	Filed May 1999 Published May 2005	Venkatesan

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	6,668,246	US	Yeung	Filed Mar. 1999 Published Dec. 2003	Yeung
	6,801,999	US	Venkatesan	Filed May 1999 Published Oct. 2004	Venkatesan
	6,061,451	US	Muratani	Filed Sept. 1997 Published May 2000	Muratani
	6,850,252	US	Hoffberg	Filed Oct. 2000 Published Feb. 2005	Hoffberg
	2002/0059144	US	Meffert	Filed Mar. 2001 Published May 2002	Meffert
	7,685,423	US	Walmsley	Filed Feb. 2000 Published Mar. 2010	Walmsley
	5,852,665	US	Gressel	Filed Jul. 1996 Published Dec. 1998	Gressel ’665
	5,664,017	US	Gressel	Filed May 1995 Published Sept. 1997	Gressel ’017
	6,351,813	US	Mooney	Filed Aug. 1998 Published Feb. 2002	Mooney

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	6,011,874	US	Glueckstad	Filed Dec. 1997 Published Jan. 2000	Glueckstad
	7,055,027	US	Gunter	Filed Mar. 1999 Published May 2006	Gunter
	6,820,203	US	Okaue	Filed Apr. 2000 Published Nov. 2004	Okaue
	2000045539	WO	Medvinsky	Filed Jan. 2000 Published Aug. 2000	Medvinsky
	5,818,939	US	Davis	Filed Dec. 1996 Published Oct. 1998	Davis
	6,560,581	US	Fox	Filed June 1998 Published May 2003	Fox
	5,812,666	US	Baker	Filed Oct. 1995 Published Sept. 1998	Baker
	6,959,288	US	Medina	Filed Feb. 1999 Published Oct. 2005	Medina
	6,996,720	US	Demello	Filed June 2000 Published Feb. 2006	Demello '720

App.	Patent No.	Country of Origin	First Named Inventor	Relevant Date	Short Title
	6,970,849	US	Demello	Filed June 2000 Published Nov. 2005	Demello' 849
	6,044,155	US	Thomlinson	Filed Dec. 1997 Published Mar. 2000	Thomlinson

2. Prior Art Non-Patent Publications

In addition to the patents and patent and patent application publications identified above, Defendants disclose the following prior art publications:

a. <u>'721 Patent</u>

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
	Secure Software Distribution	Rozenblit, IEEE Network Operations and Management Symposium, Feb. 14-17, 1994	February 1994	Rozenblit
	Trusted distribution of software over the Internet	Rubin, Proceedings of the IEEE Symposium on Network and Distributed System Security, February 16-17, 1995	February 1995	Rubin

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
	A cryptographic key generation scheme for multilevel data security, Computers & Security, Volume 9, Issue 6	Harn	October 1990	Harn
	A Secure Environment for Untrusted Helper Applications	Goldberg, Proceedings of the Sixth USENIX UNIX Security Symposium, July 1996	July 1996	Goldberg
	Practical authentication for distributed computing	J. Linn, IEEE Computer Society Symposium on Research in Security and Privacy, May 7-9, 1990	May 1990	Linn
	Security for the Digital Library-Protecting Documents Rather Than Channels	Kohl, Proceedings of the Ninth International Workshop on Database and Expert System Applications	1998	Kohl
	Persistent Access Control To Prevent Piracy Of Digital Information	Schneck, Proceedings of the IEEE	July 1999	Schneck
	Body Language, Security and E-Commerce	Desmaris	Mar. 2000	Desmaris
	Encapsulated Key Escrow	Bellare, MIT Laboratory for Computer Science Technical Report	Nov. 1996	Bellare

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
	Internet Security Association and Key Management Protocol (ISAKMP)	Maughan, Internet Engineering Task Force, Network Working Group	Nov. 1998	Maughan
	Enhanced Security Services for S/MIME	Hoffman, Internet Engineering Task Force, Network Working Group	June 1999	Hoffman
	Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)	Adams, Internet Engineering Task Force, Network Working Group	Dec. 1998	Adams
	Internet Security Glossary	Shirey, Internet Engineering Task Force, Network Working Group	May 2000	Shirey
	Secure Container Technology as a Basis for Cryptographically Secured Multimedia Communication	Kohl, Multimedia and Security Workshop at ACM Multimedia	Oct. 1998	Kohl
	Commercialization of Electronic Information	Morin, Journal of End User Computing (Hershey) Vol.12, Issue 2	Apr.-June 2000	Morin

b. <u>'304 Patent</u>

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
B-09	*ABYSS: A Trusted Architecture for Software Protection*	Steve R. White/IEEE	1987	ABYSS 1987

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
	ABYSS: An Architecture for Software Protection	Steve R. White/IEEE	1990	
	Processing and Transmission of Video, Audio and Control Signals for DBS Services	P.L. Chiu/IEEE	1984	
	Using Secure Coprocessors	Bennet Yee/Carnegie Mellon University	May 1994	
	Introduction to the Citadel Architecture: Security in Physically Exposed Environments	Steve R. White/IBM	July 10, 1991	Citadel
	Scientific Atlanta Could Have a Winner in SA B-MAC	Robert Snowden Jones	1984	Jones
	It Runs in the Family	Scientific Atlanta	1986	HOMESAT

c. <u>'815 Patent</u>

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
C-14	Applied Cryptography – Protocols, Algorithms, and Source Code in C	Bruce Schneier / John Wiley & Sons, Inc.	1996	Schneier

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
C-15	Federal Information Processing Standards Publication 180 "Secure Hash Standard" ("FIPS PUB 180") and Publication 186 "Digital Signature Standard (DSS)" ("FIPS PUB 186")	National Institute of Standards and Technology	1994	FIPS PUB
	Computer Networks (3d ed.)	Tanenbaum	1996	Tanenbaum
	Keying Hash Functions for Message Authentication	Bellare/ Springer-Verlag	1996	Bellare
	MacDES: MAC algorithm based on DES	Knudsen	April 30, 1998	Knudsen
	Hash Functions and the MAC Using All-or-Nothing Property	Shin	March 1-3, 1999	Shin
	How to sign digital streams	Gennaro / CRYPTO '97 Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology	August, 1997	

d. <u>'602 Patent</u>

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
D-12	Computer Networks (3d ed.)	Tanenbaum	1996	Tanenbaum

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
D-13	Keying Hash Functions for Message Authentication	Bellare/ Springer-Verlag	1996	Bellare
D-14	MacDES: MAC algorithm based on DES	Knudsen	April 30, 1998	Knudsen
D-15	Hash Functions and the MAC Using All-or-Nothing Property	Shin	March 1-3, 1999	Shin
D-16	Applied Cryptography – Protocols, Algorithms, and Source Code in C	Bruce Schneier / John Wiley & Sons, Inc.	1996	Schneier
D-25	How to sign digital streams	Gennaro / CRYPTO '97 Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology	August, 1997	

e. <u>'603 Patent</u>

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
	IBM announces electronic copyright solutions	Lunin	May 1995	Lunin
	Detecting digital copyright violations on the internet	Narayanan Shivakumar	August 1999	Narayanan
	MCF: A Malicious Code Filter	Raymond W. Lo	1995	Lo

f. ’342 and ’106 Patents

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
F-12, I-15	SDMI Portable Device Specification	PDWG	07/09/1999	SDMI
	EUROMED-JAVA: Trusted Third Party Services for Securing Medical Java Applets	Varvitsiotis	1999	Varvitsiotis
F-13, I-16	Trusted Third Party Services for Deploying Secure Telemedical Applications Over the WWW	Spinellis	1999	Spinellis
	RFC 2459 – Internet X.509 Public Key Infrastructure Certificate and CRL Profile	Network Working Group	01/1999	X.509
	Authorization and Attribute Certificates for Widely Distributed Access Control	Johnston	06/1998	
	Certificates and Trust in Electronic Commerce	Wilson	1997	
	ABYSS A Basic Yorktown Security System PC Software Asset Protection Concepts	Cina	1986	
	Enabling Access in Digital Libraries	Arms	02/1999	
	Safe Deals Between Strangers	Gladney	1999	
	Safeguarding Digital Library Contents and Users	Gladney	05/1998	

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
	Physical Security for the ABYSS System	Weingart	1987	
	ABYSS: A Trusted Architecture for Software Protection	White	1987	
	ABYSS: An Architecture for Software Protection	White	06/1990	
	A Common Approach to Extending Computer Security Concepts to the Universal Distributed Non-Trusted Environment	Herschaft	12/17/1994	
	Agent-based commercial dissemination of electronic information	Konstantas	05/30/2000	
	Hierarchical Organization of Certification Authorities for Secure Environments	Lopez	02/10/1997	
	Persistent access control to prevent piracy of digital information	Schneck	07/1999	
	A perspective: the role of identifiers in managing and protecting intellectual property in the digital age	Hill	07/1999	
	Flexible control of downloaded executable content	Prakash	05/1999	

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
	Enabling Access In Digital Libraries : A Report On A Workshop On Access Management	Klavans	02/1999	
	Netscape Certificate Management System Installation and Deployment Guide	Netscape Communications Corp.	1999	NCMS Install
	Netscape Certificate Management System Administrator's Guide	Netscape Communications Corp.	1999	NCMS Admin
	Netscape Certificate Management System Agent's Guide	Netscape Communications Corp.	1999	NCMS Agent
	Netscape Certificate Management System Help	Netscape Communications Corp.	1999	NCMS Help
	DOD, Netscape Ready PKI Rollout	Verton	07/18/1999	
	CMS 401 Simplifies Certificates	Barck	09/13/1999	
	Windows Media Rights Manager Overview Webpage	Microsoft Corp	05/19/2000	WMDRM Overview
	Windows Media Rights Manager Technical Features and Benefits Webpage	Microsoft Corp	03/08/1999	WMDRM Features
	Windows Media Rights Manager FAQ Webpage	Microsoft Corp	05/19/2000	WMDRM FAQ
	Windows Media Rights Manager 7 Webpage	Microsoft Corp	06/05/2000	WMDRM 7
	Windows Media Encoder 7 Webpage	Microsoft Corp	05/09/2000	WM Encoder

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
	Windows Media Format 7 Webpage	Microsoft Corp	05/09/2000	WM Format
	Windows Media Tools Webpage	Microsoft Corp	06/01/2000	WM Tools
	Windows Media Player 7 Beta Webpage	Microsoft Corp	05/31/2000	WM Player
	Get Windows Media Player 7 Beta NOW! Webpage	Microsoft Corp	04/13/2000	
	Windows Media Technologies 4.1 Features Webpage	Microsoft Corp	04/03/2000	
	Windows Media Technologies Home Webpage	Microsoft Corp	11/17/1999	
	Windows Media on PressPass Webpage	Microsoft Corp	2000	
	Windows Media Technologies 4 Delivers Cutting-Edge CD-Quality Audio on the Internet	Microsoft Corp	09/17/1999	
	Microsoft and S3's Diamond Multimedia Showcase Rio Player in First Live Demonstration of Windows Media on SDMI-Capable Portable Device	Microsoft Corp	11/15/1999	
	Supertracks and Microsoft Announce Windows Media Digital Rights Technology Integration for New Music Download and Promotion System	Microsoft Corp.	12/07/1999	

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
	Microsoft and Texas Instruments Announce Native Windows Media Support on TI Programmable DSPs	Microsoft Corp.	12/07/1999	
	Microsoft and Preview Systems Announce First Windows Media-Based Digital Audio and Video Distribution Solution for Retail Commerce	Microsoft Corp.	12/07/1999	
	[MS-DRM]: Digital Rights Management License Protocol	Microsoft Corp.	06/01/2017	
	[MS-DRMND]: Windows Digital Rights Management (WMDRM): Network Devices Protocol	Microsoft Corp.	06/01/2017	MS-DRM
	5799 – EMMS Content Mastering	IBM	05/03/2000	EMMS 5799
	EMMS Software Suite	IBM	2001	EMMS Suite
	EMMS Frequently Asked Questions	IBM	Unknown	EMMS FAQ
	IBM Electronic Media Management System, V2.1 – A Digital Rights Management Platform	IBM	01/29/2002	
	BMG Entertainment Plans Adoption of IBM Technology For Commercial Roll-out of Electronic Music Distribution to Consumers	IBM	04/06/2000	

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
	BMG Unveils Comprehensive Online Digital Downloading Plans for the Year 2000 and Beyond	IBM	04/06/2000	
	Five Major Music Companies and IBM Successfully Complete Electronic Music Distribution Trial	IBM	02/02/2000	
	IBM and Liquid Audio Team Up on Digital Music Technologies and Services	IBM	04/06/2000	
	IBM and Reciprocal Establish Strategic Relationship to Expand Digital Music Distribution	IBM	04/06/2000	
	IBM and Sony Show First Results of Collaboration with Electronic Music Distribution	IBM/Sony	11/15/1999	
	Leading Music Mastering Studio to Use IBM's Digital Rights Management Technology	IBM	07/24/2000	
	Toshiba and IBM to Jointly Accelerate Digital Music Distribution Marketplace	IBM	03/13/2000	

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
	Windows Media Technologies 4 Delivers Cutting-Edge CD-Quality Audio on the Internet	IBM	09/17/1999	
	The Media Business; Sony and IBM Create Alliance on Delivering Music Over Net	Richtel	04/16/1999	
	Cryptolope Live! Home Webpage	IBM	01/22/1998	Cryptolope Home
	IBM Introduces Cryptolope Live! Webpage	IBM	09/09/1997	
	Cryptolope Container Technology Webpage	IBM	01/22/1998	Cryptolope News
	IBM infoMarket Saga	Various	Various	
	IBM Make Cryptolope Deal	CNet	12/11/1996	
	IBM Expands Its Digital Rights Management Technology	IBM	04/08/2002	
	DigiBox: A Self-Protecting Container for Information Commerce	Sibert	07/1995	Sibert

g. <u>'157 Patent</u>

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
G-09	*ABYSS: A Trusted Architecture for Software Protection*	Steve R. White/IEEE	1987	ABYSS 1987

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
	Processing and Transmission of Video, Audio and Control Signals for DBS Services	P.L. Chiu/IEEE	1984	
	Using Secure Coprocessors	Bennet Yee/Carnegie Mellon University	May 1994	
	Introduction to the Citadel Architecture: Security in Physically Exposed Environments	Steve R. White/IBM	July 10, 1991	Citadel
	Scientific Atlanta Could Have a Winner in SA B-MAC	Robert Snowden Jones	1984	Jones
	It Runs in the Family	Scientific Atlanta	1986	HOMESAT

h. ’158 Patent

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
H-09	*ABYSS: A Trusted Architecture for Software Protection*	Steve R. White/IEEE	1987	ABYSS 1987
	Processing and Transmission of Video, Audio and Control Signals for DBS Services	P.L. Chiu/IEEE	1984	
	Using Secure Coprocessors	Bennet Yee/Carnegie Mellon University	May 1994	
	Introduction to the Citadel Architecture: Security in Physically	Steve R. White/IBM	July 10, 1991	Citadel

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
	Exposed Environments			
	Scientific Atlanta Could Have a Winner in SA B-MAC	Robert Snowden Jones	1984	Jones
	It Runs in the Family	Scientific Atlanta	1986	HOMESAT

i. ’627 Patent

App.	Title	Primary Author/ Publisher	Publication Date	Short Title
J-12	Piracy: the Dark Side of Electronic Commerce	Sahuguet	May 1998	Sahuguet
	Secure Container Technology as a Basis for Cryptographically Secured Multimedia Communication	Dittmann	Sept. 1998	Dittmann
	ICL Technical Journal	Mailer	Nov. 1997	Mailer
	Cryptographic Containers and the Digital Library	Lotspiech	1997	Lotspiech

3. Prior Art Systems

In addition to the printed publications identified above, Defendants disclose the following prior art systems. The descriptions of the systems and events relating to the systems are stated on information and belief, and are supported by documents that will be produced by Defendants and/or third parties. As discovery is ongoing, Defendants continue to investigate these systems.

Defendants reserve the right to rely upon any system, public knowledge or use embodying or otherwise incorporating any of the prior art disclosed below, alone or in combination. Defendants further reserve the right to rely upon any other documents or references describing any

such system, knowledge, or use. By way of example, and without limitation, Defendants reserve the right to rely upon any system implementing the standards, requirements documents, or specifications disclosed herein or in Intertrust's Infringement Contentions, including but not limited to the standards and specifications of the Digital Cinema Initiative and/or the Society of Motion Picture and Television Engineers (SMPTE), and reserve the right to rely upon the standards, specifications, and other documents describing the system to establish the operation of the system.

a. '721 Patent

Item Sold/Used	Date of Sale/Use[1]
Digibox System	No later than 1995
Abyss System	No later than 1990

(1) Digibox System

The Digibox System is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at Electronic Publishing Resources, Inc. ("EPR"), and Olin Sibert, David Bernstein, David Van Wie, other individuals who presented, published, or demonstrated this system before the alleged invention of the '721 Patent; (2) in public use and/or on sale in this country more than one year before the filing date of the '721 Patent by personnel at EPR, and Olin Sibert, David Bernstein, David Van Wie, other individuals who presented, published, or demonstrated this system before the alleged invention of the '721 Patent. The Digibox System is prior art under 35 U.S.C. § 102(f) as the invention was derived by the alleged inventors during their work at EPR and the individuals who assisted in developing and implementing the Digibox System. The Digibox System is prior art under 35 U.S.C. § 102(g)

[1] These dates are provided upon information and belief. Defendants reserve the right to seek further information regarding these systems during discovery.

because it was invented by EPR, and Olin Sibert, David Bernstein, David Van Wie, and the other individuals who assisted in developing and implementing the Digibox System, who did not abandon, suppress, or conceal, before the alleged invention of the '721 Patent. For each of these reasons, the Digibox System is also prior art under 35 U.S.C. § 103.

Upon information and belief, the Digibox System was first offered as a service in the United States by EPR as early as 1995. Upon information and belief, early versions of the Digibox Systems supported certificates and various encryption protocols.

The following documents are identified in support of the Digibox System, along with any other documents referencing the Digibox System produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
DigiBox: A Self-Protecting Container for Information Commerce	07/1995	Sibert	Sibert

Defendants' contentions regarding where in the Digibox System each element of the Asserted Claims of the '721 Patent is found are provided in Appendix A-15. Defendants reserve the right to seek further information regarding the Digibox System during discovery. Defendants expects to prove its contentions regarding the Digibox System with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the Digibox System.

(2) Abyss System

The Abyss System is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at International Business Machines Corporation ("IBM"), and Steve R. White, Liam Comerford, Steve H. Weingart, Vincent J. Cina Jr., other individuals who

presented, published, or demonstrated this system before the alleged invention of the '721 Patent; (2) in public use and/or on sale in this country more than one year before the filing date of the '721 Patent; (2) in public use and/or on sale in this country more than one year before the filing date of the '721 Patent by personnel at IBM, and Steve R. White, Liam Comerford, Steve H. Weingart, Vincent J. Cina Jr., other individuals who presented, published, or demonstrated this system before the alleged invention of the '721 Patent. The Abyss System is prior art under 35 U.S.C. § 102(f) as the invention was derived by the alleged inventors during their work at IBM and the individuals who assisted in developing and implementing the Abyss System. The Abyss System is prior art under 35 U.S.C. § 102(g) because it was invented by IBM, and Steve R. White, Liam Comerford, Steve H. Weingart, Vincent J. Cina Jr., and the other individuals who assisted in developing and implementing the Abyss System, who did not abandon, suppress, or conceal, before the alleged invention of the '721 Patent. For each of these reasons, the Abyss System is also prior art under 35 U.S.C. § 103.

Upon information and belief, the Abyss System was first offered as a service in the United States by Abyss as early as 1987. Upon information and belief, early versions of the Abyss System supported trusted software execution and tamper resistant storage.

The following documents are identified in support of the Abyss System, along with any other documents referencing the Abyss System produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
ABYSS A Basic Yorktown Security System PC Software Asset Protection Concepts	12/1986	Cina	ABYSS 1986
Physical Security for the ABYSS System	1987	Weingart	ABYSS-Weingart

Publication	Pub. Date	Author	Short Name
ABYSS: A Trusted Architecture for Software Protection	1987	White	ABYSS 1987
ABYSS: An Architecture for Software Protection	1990	White	ABYSS 1990

Defendants' contentions regarding where in the Abyss System each element of the Asserted Claims of the '721 Patent is found are provided in Appendix A-16. Defendants reserve the right to seek further information regarding the Abyss System during discovery. Defendants expects to prove its contentions regarding the Abyss System with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the Abyss System.

(3) Other Prior Art Systems

On information and belief, AT&T Inc., Citibank Systems, Xerox/Contentguard Systems, Viatech Systems, DigReg Systems, Adobe Systems, Symantec Systems, and Digimarc Systems are additional systems that constitute prior art under 35 U.S.C. §§ 102(a) and/or (b) because: (1) they were known or used in this country by the developers of each respective system and other individuals who presented, published, or demonstrated these systems before the alleged invention of the '721 Patent; and/or (2) in public use and/or on sale in this country more than one year before the filing date of the '721 Patent by the developers of each respective system and other individuals who presented, published, or demonstrated these systems before the alleged invention of the '721 Patent. For each of the above reasons, each of these systems are also prior art under 35 U.S.C. § 103.

Upon information and belief, and subject to Defendants' present understanding of the Asserted Claims, its current construction of the claims, and/or Intertrust's apparent construction of the claims in its Infringement Contentions, each of the systems identified above, alone or in combination, satisfies each and every element of the Asserted Claims of the '721 Patent. Defendants reserve the right to seek further information regarding the systems identified above during discovery and supplement these Contentions accordingly. Defendants expect to prove with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the systems, that the above-identified systems satisfy each and every element of the Asserted Claims of the '721 Patent.

b. '304 , '157, and '158 Patents

Item Sold/Used	Date of Sale/Use[2]
ABYSS	No later than 1987
Scientific-Atlantic System	No later than 1991

(1) ABYSS

The ABYSS system is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at International Business Machines Corporation ("IBM"), its successors-in-interest, and other individuals who presented, published, or demonstrated this system before the alleged invention of the '304, '157, and '158 Patents; (2) in public use and/or on sale in this country more than one year before the filing date of the '304, '157, and '158 Patents by IBM, its successors-in-interest, and other individuals who presented, published, or

[2] These dates are provided upon information and belief. Defendants reserve the right to seek further information regarding these systems during discovery.

demonstrated this system before the alleged invention of the '304, '157, and '158 Patents. For each of these reasons, ABYSS is also prior art under 35 U.S.C. § 103.

Upon information and belief, ABYSS was first offered as a service in the United States by IBM as early as 1987 and no later than 1990. Upon information and belief, early versions of ABYSS supported cryptographic systems such as DES, including symmetric cryptosystems and cryptographic keys.

The following documents are identified in support of the ABYSS System, along with any other documents referencing the ABYSS System produced with these disclosures or produced in Prior Actions:

Date	Short Name
12/1986	ABYSS 1986
1987	ABYSS-Weingart
1987	ABYSS 1987
1990	ABYSS 1990
Nov. 5, 1986	Comerford
Aug. 30, 1989	Matyas
Mar. 22, 1991	Citadel

Defendants' contentions regarding where in the ABYSS System each element of the Asserted Claims of the '304, '157, and '158 Patents is found are provided in Appendices B-10, G-10, and H-10. Defendants reserve the right to seek further information regarding the ABYSS System during discovery. Defendants expects to prove its contentions regarding the ABYSS System with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the ABYSS System.

(2) Scientific-Atlantic Systems

The Scientific Atlanta system is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at Scientific-Atlanta Inc. ("Scientific Atlanta"), its successors-in-interest, and other individuals who presented, published, or demonstrated this system before the alleged invention of the '304, '157, and '158 Patents; (2) in public use and/or on sale in this country more than one year before the filing date of the '304, '157, and '158 Patents by Scientific Atlanta, its successors-in-interest, and other individuals who presented, published, or demonstrated this system before the alleged invention of the '304, '157, and '158 Patents. For each of these reasons, Scientific Atlanta is also prior art under 35 U.S.C. § 103.

Upon information and belief, Scientific Atlanta was first offered as a service in the United States by Scientific Atlanta as early as 1990 and no later than 1991. Upon information and belief, early versions of Scientific Atlanta supported scrambling of data, video, and audio signals for transmission of entertainment content.

The following documents are identified in support of the Scientific Atlanta System, along with any other documents referencing the Scientific Atlanta System produced with these disclosures or produced in Prior Actions:

Date	Short Name
Mar. 29, 1991	Gammie
1984	Jones
1986	HOMESAT

Defendants' contentions regarding where in the Scientific Atlantic Systems each element of the Asserted Claims of the '304, '157, and '158 Patents is found are provided in Appendices B-11, G-11, and H-11. Defendants reserve the right to seek further information regarding the Scientific Atlantic Systems during discovery. Defendants expects to prove its contentions

regarding the Scientific Atlantic Systems with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the Scientific Atlantic Systems.

c. ’815 Patent

Item Sold/Used	Date of Sale/Use[3]
DigiBox System	July, 1995
IBM Cryptolope	January 22, 1998
Sun Microsystems HotJava	1997

(1) DigiBox System

The Digibox System is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at Electronic Publishing Resources, Inc. (“EPR”), and Olin Sibert, David Bernstein, David Van Wie, other individuals who presented, published, or demonstrated this system before the alleged invention of the ’815 Patent; (2) in public use and/or on sale in this country more than one year before the filing date of the ’815 Patent by personnel at EPR, and Olin Sibert, David Bernstein, David Van Wie, other individuals who presented, published, or demonstrated this system before the alleged invention of the ’815 Patent. The Digibox System is prior art under 35 U.S.C. § 102(f) as the invention was derived by the alleged inventors during their work at EPR and the individuals who assisted in developing and implementing the Digibox System. The Digibox System is prior art under 35 U.S.C. § 102(g) because it was invented by EPR, and Olin Sibert, David Bernstein, David Van Wie, and the other individuals who assisted in developing and implementing the Digibox System, who did not

[3] These dates are provided upon information and belief. Defendants reserve the right to seek further information regarding these systems during discovery.

abandon, suppress, or conceal, before the alleged invention of the '815 Patent. For each of these reasons, the Digibox System is also prior art under 35 U.S.C. § 103.

Upon information and belief, the Digibox System was first offered as a service in the United States by EPR as early as 1995. Upon information and belief, early versions of the Digibox Systems supported certificates and various encryption protocols.

The following documents are identified in support of the DigiBox system, along with any other documents referencing the DigiBox system produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
US 2007/0211891 A1	September 13, 2007	Shamoon et al.	Shamoon
DigiBox: A Self-Protecting Container for Information Commerce	July, 1995	Sibert et al.	DigiBox

Defendants' contentions regarding where in the DigiBox system each element of the Asserted Claims of the '815 Patent is found are provided in Appendix C-16. Defendants reserve the right to seek further information regarding DigiBox during discovery. Defendants expect to prove its contentions regarding DigiBox with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of DigiBox.

(2) IBM Cryptolope

The IBM Cryptolope system is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at IBM, its successors-in-interest, and other individuals who presented, published, or demonstrated this system before the alleged invention of

the ’815 Patent; (2) in public use and/or on sale in this country more than one year before the filing date of the ’815 Patent by IBM, its successors-in-interest, and other individuals who presented, published, or demonstrated this system before the alleged invention of the ’815 Patent. For each of these reasons, Cryptolope is also prior art under 35 U.S.C. § 103.

Upon information and belief, Cryptolope was first offered in the United States by IBM as early as 1998 and satisfies the Asserted Claims of the ’815 Patent.

The following documents are identified in support of the Cryptolope system, along with any other documents referencing the Cryptolope system produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
Cryptolope Container Technology	1998	IBM	Cryptolope

Defendants’ contentions regarding where in the Cryptolope system each element of the Asserted Claims of the ’815 Patent is found are provided in Appendix C-17. Defendants reserve the right to seek further information regarding Cryptolope during discovery. Defendants expect to prove its contentions regarding Cryptolope with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of Cryptolope.

(3) Sun Microsystems HotJava

The Sun Microsystems HotJava system is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at Sun Microsystems, its successors-in-interest, and other individuals who presented, published, or demonstrated this system before the alleged invention of the ’815 Patent; (2) in public use and/or on sale in this country more than one

year before the filing date of the '815 Patent by Sun Microsystems, its successors-in-interest, and other individuals who presented, published, or demonstrated this system before the alleged invention of the '815 Patent. For each of these reasons, HotJava is also prior art under 35 U.S.C. § 103.

Upon information and belief, HotJava was first offered in the United States by Sun Microsystems as early as 1997 and satisfies the Asserted Claims of the '815 Patent.

The following documents are identified in support of the HotJava system, along with any other documents referencing the HotJava system produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
U.S. Patent No. 5,958,051	1999	Renaud	Renaud

Defendants' contentions regarding where in the HotJava system each element of the Asserted Claims of the '815 Patent is found are provided in Appendix C-18. Defendants reserve the right to seek further information regarding HotJava during discovery. Defendants expect to prove its contentions regarding HotJava with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of HotJava.

(4) Other Prior Art Systems

On information and belief, Sun Microsystems' Java Platform, Xerox's VPR, Xerox/ContentGuard systems, Thomson Consumer Electronics TV systems, and General Instrument's VideoCipher and DigiCipher are additional systems that constitute prior art under 35 U.S.C. §§ 102(a) and/or (b) because: (1) they were known or used in this country by the developers of each respective system and other individuals who presented, published, or demonstrated these

systems before the alleged invention of the '815 Patent; and/or (2) in public use and/or on sale in this country more than one year before the filing date of the '815 Patent by the developers of each respective system and other individuals who presented, published, or demonstrated these systems before the alleged invention of the '815 Patent. For each of the above reasons, each of these systems are also prior art under 35 U.S.C. § 103.

Upon information and belief, and subject to Defendants' present understanding of the Asserted Claims, its current construction of the claims, and/or Intertrust's apparent construction of the claims in its Infringement Contentions, each of the systems identified above, alone or in combination, satisfies each and every element of the Asserted Claims of the '815 Patent. Defendants reserve the right to seek further information regarding the systems identified above during discovery and supplement these Contentions accordingly. Defendants expect to prove with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the systems, that the above-identified systems satisfy each and every element of the Asserted Claims of the '815 Patent.

d. '602 Patent

Item Sold/Used	**Date of Sale/Use[4]**
DigiBox System	July, 1995
IBM Cryptolope	January 22, 1998

[4] These dates are provided upon information and belief. Defendants reserve the right to seek further information regarding these systems during discovery.

(1) DigiBox System

The Digibox System is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at Electronic Publishing Resources, Inc. ("EPR"), and Olin Sibert, David Bernstein, David Van Wie, other individuals who presented, published, or demonstrated this system before the alleged invention of the '602 Patent; (2) in public use and/or on sale in this country more than one year before the filing date of the '602 Patent by personnel at EPR, and Olin Sibert, David Bernstein, David Van Wie, other individuals who presented, published, or demonstrated this system before the alleged invention of the '602 Patent. The Digibox System is prior art under 35 U.S.C. § 102(f) as the invention was derived by the alleged inventors during their work at EPR and the individuals who assisted in developing and implementing the Digibox System. The Digibox System is prior art under 35 U.S.C. § 102(g) because it was invented by EPR, and Olin Sibert, David Bernstein, David Van Wie, and the other individuals who assisted in developing and implementing the Digibox System, who did not abandon, suppress, or conceal, before the alleged invention of the '602 Patent. For each of these reasons, the Digibox System is also prior art under 35 U.S.C. § 103.

Upon information and belief, the Digibox System was first offered as a service in the United States by EPR as early as 1995. Upon information and belief, early versions of the Digibox Systems supported certificates and various encryption protocols.

The following documents are identified in support of the DigiBox system, along with any other documents referencing the DigiBox system produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
US 2007/0211891 A1	September 13, 2007	Shamoon et al.	Shamoon

Publication	Pub. Date	Author	Short Name
DigiBox: A Self-Protecting Container for Information Commerce	July, 1995	Sibert et al.	DigiBox

Defendants' contentions regarding where in the DigiBox system each element of the Asserted Claims of the '602 Patent is found are provided in Appendix D-17. Defendants reserve the right to seek further information regarding DigiBox during discovery. Defendants expect to prove its contentions regarding DigiBox with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of DigiBox.

(2) IBM Cryptolope

The IBM Cryptolope system is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at IBM, its successors-in-interest, and other individuals who presented, published, or demonstrated this system before the alleged invention of the '602 Patent; (2) in public use and/or on sale in this country more than one year before the filing date of the '602 Patent by IBM, its successors-in-interest, and other individuals who presented, published, or demonstrated this system before the alleged invention of the '602 Patent. For each of these reasons, Cryptolope is also prior art under 35 U.S.C. § 103.

Upon information and belief, Cryptolope was first offered in the United States by IBM as early as 1998 and satisfies the Asserted Claims of the '602 Patent.

The following documents are identified in support of the Cryptolope system, along with any other documents referencing the Cryptolope system produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
Cryptolope Container Technology	1998	IBM	Cryptolope

Defendants' contentions regarding where in the Cryptolope system each element of the Asserted Claims of the '602 Patent is found are provided in Appendix D-18. Defendants reserve the right to seek further information regarding Cryptolope during discovery. Defendants expect to prove its contentions regarding Cryptolope with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of Cryptolope.

(3) Other Prior Art Systems

On information and belief, Sun Microsystems' Java Platform, Xerox's VPR, Xerox/ContentGuard systems, Thomson Consumer Electronics TV systems, and General Instrument's VideoCipher and DigiCipher are additional systems that constitute prior art under 35 U.S.C. §§ 102(a) and/or (b) because: (1) they were known or used in this country by the developers of each respective system and other individuals who presented, published, or demonstrated these systems before the alleged invention of the '602 Patent; and/or (2) in public use and/or on sale in this country more than one year before the filing date of the '602 Patent by the developers of each respective system and other individuals who presented, published, or demonstrated these systems before the alleged invention of the '602 Patent. For each of the above reasons, each of these systems are also prior art under 35 U.S.C. § 103.

Upon information and belief, and subject to Defendants' present understanding of the Asserted Claims, its current construction of the claims, and/or Intertrust's apparent construction of the claims in its Infringement Contentions, each of the systems identified above, alone or in

combination, satisfies each and every element of the Asserted Claims of the '602 Patent. Defendants reserve the right to seek further information regarding the systems identified above during discovery and supplement these Contentions accordingly. Defendants expect to prove with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the systems, that the above-identified systems satisfy each and every element of the Asserted Claims of the '602 Patent.

e. '603 Patent

Item Sold/Used	Date of Sale/Use[5]
DigiBox System	July, 1995
IBM Cryptolope	January 22, 1998

(1) DigiBox System

The Digibox System is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at Electronic Publishing Resources, Inc. ("EPR"), and Olin Sibert, David Bernstein, David Van Wie, other individuals who presented, published, or demonstrated this system before the alleged invention of the '603 Patent; (2) in public use and/or on sale in this country more than one year before the filing date of the '603 Patent by personnel at EPR, and Olin Sibert, David Bernstein, David Van Wie, other individuals who presented, published, or demonstrated this system before the alleged invention of the '603 Patent. The Digibox System is prior art under 35 U.S.C. § 102(f) as the invention was derived by the alleged inventors during their work at EPR and the individuals who assisted in developing and

[5] These dates are provided upon information and belief. Defendants reserve the right to seek further information regarding these systems during discovery.

implementing the Digibox System. The Digibox System is prior art under 35 U.S.C. § 102(g) because it was invented by EPR, and Olin Sibert, David Bernstein, David Van Wie, and the other individuals who assisted in developing and implementing the Digibox System, who did not abandon, suppress, or conceal, before the alleged invention of the '603 Patent. For each of these reasons, the Digibox System is also prior art under 35 U.S.C. § 103.

Upon information and belief, the Digibox System was first offered as a service in the United States by EPR as early as 1995. Upon information and belief, early versions of the Digibox Systems supported certificates and various encryption protocols.

The following documents are identified in support of the DigiBox system, along with any other documents referencing the DigiBox system produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
US 2007/0211891 A1	September 13, 2007	Shamoon et al.	Shamoon
DigiBox: A Self-Protecting Container for Information Commerce	July, 1995	Sibert et al.	DigiBox

Defendants' contentions regarding where in the DigiBox system each element of the Asserted Claims of the '603 Patent is found are provided in Appendix E-12. Defendants reserve the right to seek further information regarding DigiBox during discovery. Defendants expect to prove its contentions regarding DigiBox with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of DigiBox.

(2) IBM Cryptolope

The IBM Cryptolope system is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at IBM, its successors-in-interest, and other individuals who presented, published, or demonstrated this system before the alleged invention of the '603 Patent; (2) in public use and/or on sale in this country more than one year before the filing date of the '603 Patent by IBM, its successors-in-interest, and other individuals who presented, published, or demonstrated this system before the alleged invention of the '603 Patent. For each of these reasons, Cryptolope is also prior art under 35 U.S.C. § 103.

Upon information and belief, Cryptolope was first offered in the United States by IBM as early as 1998 and satisfies the Asserted Claims of the '603 Patent.

The following documents are identified in support of the Cryptolope system, along with any other documents referencing the Cryptolope system produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
Cryptolope Container Technology	1998	IBM	Cryptolope

Defendants' contentions regarding where in the Cryptolope system each element of the Asserted Claims of the '603 Patent is found are provided in Appendix E-13. Defendants reserve the right to seek further information regarding Cryptolope during discovery. Defendants expect to prove its contentions regarding Cryptolope with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of Cryptolope.

(3) Other Prior Art Systems

On information and belief, Sun Microsystems' Java Platform, Xerox's VPR, Xerox/ContentGuard systems, Thomson Consumer Electronics TV systems, and General Instrument's VideoCipher and DigiCipher are additional systems that constitute prior art under 35 U.S.C. §§ 102(a) and/or (b) because: (1) they were known or used in this country by the developers of each respective system and other individuals who presented, published, or demonstrated these systems before the alleged invention of the '603 Patent; and/or (2) in public use and/or on sale in this country more than one year before the filing date of the '603 Patent by the developers of each respective system and other individuals who presented, published, or demonstrated these systems before the alleged invention of the '603 Patent. For each of the above reasons, each of these systems are also prior art under 35 U.S.C. § 103.

Upon information and belief, and subject to Defendants' present understanding of the Asserted Claims, its current construction of the claims, and/or Intertrust's apparent construction of the claims in its Infringement Contentions, each of the systems identified above, alone or in combination, satisfies each and every element of the Asserted Claims of the '603 Patent. Defendants reserve the right to seek further information regarding the systems identified above during discovery and supplement these Contentions accordingly. Defendants expect to prove with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the systems, that the above-identified systems satisfy each and every element of the Asserted Claims of the '603 Patent.

f. ’342 and ’106 Patents

Item Sold/Used	Date of Sale/Use[6]
Netscape System	No later than 1999
WMDRM System	No later than 1999
IBM DRM Systems	No later than 1999
Digibox System	No later than 1995

(1) Netscape System

The Netscape System is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at Netscape Communications, its successors-in-interest, including American Online, and Taher Elgamal, Jeff Weinstein, other individuals who presented, published, or demonstrated this system before the alleged invention of the ’342 and ’106 Patents; (2) in public use and/or on sale in this country more than one year before the filing date of the ’342 and ’106 Patents by personnel at Netscape Communications, its successors-in-interest, including American Online, and Taher Elgamal, Jeff Weinstein, other individuals who presented, published, or demonstrated this system before the alleged invention of the ’342 and ’106 Patents. For each of these reasons, the Netscape System is also prior art under 35 U.S.C. § 103.

Upon information and belief, the Netscape System was first offered as a service in the United States by Netscape Communications as early as 1999. Upon information and belief, early versions of the Netscape Systems supported certificates and various encryption protocols.

[6] These dates are provided upon information and belief. Defendants reserve the right to seek further information regarding these systems during discovery.

The following documents are identified in support of the Netscape System, along with any other documents referencing the Netscape System produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
Netscape Certificate Management System Installation and Deployment Guide	1999	Netscape Communications Corp.	NCMS Install
Netscape Certificate Management System Administrator's Guide	1999	Netscape Communications Corp.	NCMS Admin
Netscape Certificate Management System Agent's Guide	1999	Netscape Communications Corp.	NCMS Agent
Netscape Certificate Management System Help	1999	Netscape Communications Corp.	NCMS Help
U.S. Pat. 5,657,390	Issued: 09/12/1997	Elgamal et al.	Elgamal 390
U.S. Pat. 5,671,279	Issued: 09/23/1997	Elgamal	Elgamal 279
U.S. Pat. 6,094,485	Filed: 09/18/1997	Weinstein et al.	Weinstein
U.S. Pat. 6,138,107	Filed: 01/04/1996	Elgamal	Elgamal 107
U.S. Pat. 6,944,669	Priority: 10/22/1999	Saccocio	Saccocio
U.S. Pat. 7,013,390	Priority: 06/30/1997	Elgamal et al.	Elgamal 390
DOD, Netscape Ready PKI Rollout	07/18/1999	Verton	
CMS 401 Simplifies Certificates	09/13/1999	Barck	

Defendants' contentions regarding where in the Netscape System each element of the Asserted Claims of the '342 and '106 Patents is found are provided in Appendices F-14 and I-17, respectively. Defendants reserve the right to seek further information regarding the Netscape System during discovery. Defendants expects to prove its contentions regarding the Netscape System with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the Netscape System.

(2) Windows Media Digital Rights Management (WMDRM) System

The WMDRM System is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at Microsoft Corporation, its successors-in-interest, and Peter Biddle, Bryan Willman, Paul England, Marcus Peinado, other individuals who presented, published, or demonstrated this system before the alleged invention of the '342 and '106 Patents; (2) in public use and/or on sale in this country more than one year before the filing date of the '342 and '106 Patents by personnel at Microsoft Corporation, its successors-in-interest, and Peter Biddle, Bryan Willman, Paul England, Marcus Peinado, other individuals who presented,, published, or demonstrated this system before the alleged invention of the '342 and '106 Patents. For each of these reasons, the WMDRM System is also prior art under 35 U.S.C. § 103.

Upon information and belief, the WMDRM System was first offered as a service in the United States by Microsoft Corporation as early as 1999. Upon information and belief, early versions of the WMDRM Systems supported certificates and various encryption protocols.

The following documents are identified in support of the WMDRM System, along with any other documents referencing the WMDRM System produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
Windows Media Rights Manager Overview Webpage	05/19/2000	Microsoft Corp	WMDRM Overview
Windows Media Rights Manager Technical Features and Benefits Webpage	03/08/1999	Microsoft Corp	WMDRM Features
Windows Media Rights Manager FAQ Webpage	05/19/2000	Microsoft Corp	WMDRM FAQ
Windows Media Rights Manager 7 Webpage	06/05/2000	Microsoft Corp	WMDRM 7
Windows Media Encoder 7 Webpage	05/09/2000	Microsoft Corp	WM Encoder
Windows Media Format 7 Webpage	05/09/2000	Microsoft Corp	WM Format
Windows Media Tools Webpage	06/01/2000	Microsoft Corp	WM Tools
Windows Media Player 7 Beta Webpage	05/31/2000	Microsoft Corp	WM Player
Get Windows Media Player 7 Beta NOW! Webpage	04/13/2000	Microsoft Corp	
Windows Media Technologies 4.1 Features Webpage	04/03/2000	Microsoft Corp	
Windows Media Technologies Home Webpage	11/17/1999	Microsoft Corp	
Windows Media on PressPass Webpage	2000	Microsoft Corp	
Windows Media Technologies 4 Delivers Cutting-Edge CD-Quality Audio on the Internet	09/17/1999	Microsoft Corp	
Microsoft and S3's Diamond Multimedia Showcase Rio Player in First Live Demonstration	11/15/1999	Microsoft Corp	

Publication	Pub. Date	Author	Short Name
of Windows Media on SDMI-Capable Portable Device			
Supertracks and Microsoft Announce Windows Media Digital Rights Technology Integration for New Music Download and Promotion System	12/07/1999	Microsoft Corp.	
Microsoft and Texas Instruments Announce Native Windows Media Support on TI Programmable DSPs	12/07/1999	Microsoft Corp.	
Microsoft and Preview Systems Announce First Windows Media-Based Digital Audio and Video Distribution Solution for Retail Commerce	12/07/1999	Microsoft Corp.	
[MS-DRM]: Digital Rights Management License Protocol	06/01/2017	Microsoft Corp.	
[MS-DRMND]: Windows Digital Rights Management (WMDRM): Network Devices Protocol	06/01/2017	Microsoft Corp.	MS-DRM

Defendants' contentions regarding where in the WMDRM System each element of the Asserted Claims of the '342 and '106 Patents is found are provided in Appendices F-15 and I-18, respectively. Defendants reserve the right to seek further information regarding the WMDRM System during discovery. Defendants expects to prove its contentions regarding the WMDRM System with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the WMDRM System.

(3) IBM Digital Rights Management (DRM) Systems

The IBM DRM Systems, including Cryptolope Container Technology ("Cryptolope") and/or Electronic Media Management System (EMMS"), are prior art under 35 U.S.C. §§ 102(a) and (b) because they were (1) known or used in this country by personnel at International Business Machines ("IBM"), its successors-in-interest, and Jeff Crigler, Tim Byars, other individuals who presented, published, or demonstrated these systems before the alleged invention of the '342 and '106 Patents; (2) in public use and/or on sale in this country more than one year before the filing date of the '342 and '106 Patents by personnel at IBM, its successors-in-interest, and Jeff Crigler, Tim Byars, other individuals who presented,, published, or demonstrated these systems before the alleged invention of the '342 and '106 Patents. For each of these reasons, the IBM DRM Systems are also prior art under 35 U.S.C. § 103.

Upon information and belief, the IBM DRM Systems were first offered as a service in the United States by IBM as early as 1999. Upon information and belief, early versions of the IBM DRM Systems supported certificates and various encryption protocols.

The following documents are identified in support of the IBM DRM Systems, along with any other documents referencing the IBM DRM Systems produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
5799 – EMMS Content Mastering	05/03/2000	IBM	EMMS 5799
EMMS Software Suite	2001	IBM	EMMS Suite
EMMS Frequently Asked Questions	Unknown	IBM	EMMS FAQ
IBM Electronic Media Management System, V2.1 – A Digital Rights Management Platform	01/29/2002	IBM	

Publication	Pub. Date	Author	Short Name
BMG Entertainment Plans Adoption of IBM Technology For Commercial Roll-out of Electronic Music Distribution to Consumers	04/06/2000	IBM	
BMG Unveils Comprehensive Online Digital Downloading Plans for the Year 2000 and Beyond	04/06/2000	IBM	
Five Major Music Companies and IBM Successfully Complete Electronic Music Distribution Trial	02/02/2000	IBM	
IBM and Liquid Audio Team Up on Digital Music Technologies and Services	04/06/2000	IBM	
IBM and Reciprocal Establish Strategic Relationship to Expand Digital Music Distribution	04/06/2000	IBM	
IBM and Sony Show First Results of Collaboration with Electronic Music Distribution	11/15/1999	IBM/Sony	
Leading Music Mastering Studio to Use IBM's Digital Rights Management Technology	07/24/2000	IBM	
Toshiba and IBM to Jointly Accelerate Digital Music Distribution Marketplace	03/13/2000	IBM	
Windows Media Technologies 4 Delivers Cutting-Edge CD-Quality Audio on the Internet	09/17/1999	IBM	

Publication	Pub. Date	Author	Short Name
The Media Business; Sony and IBM Create Alliance on Delivering Music Over Net	04/16/1999	Richtel	
Cryptolope Live! Home Webpage	01/22/1998	IBM	Cryptolope Home
IBM Introduces Cryptolope Live! Webpage	09/09/1997	IBM	
Cryptolope Container Technology Webpage	01/22/1998	IBM	Cryptolope News
IBM infoMarket Saga	Various	Various	
IBM Make Cryptolope Deal	12/11/1996	CNet	
IBM Expands Its Digital Rights Management Technology	04/08/2002	IBM	
U.S. Pat. 6,389,538	Filed: 08/22/1998	Gruse	Gruse 538
U.S. Pat. 6,398,245	Filed: 12/01/1998	Gruse	Gruse 245
U.S. Pat. 6,418,421	Filed: 12/10/1998	Hurtado	Hurtado
U.S. Pat. 6,574,609	Filed: 09/14/1998	Downs	Downs 609
U.S. Pat. 6,226,618	Priority: 08/03/1998	Downs	Downs
U.S. Pat. 6,587,837	Filed: 12/01/1998	Spagna	Spagna
U.S. Pat. 6,959,288	Filed: 02/01/1999	Medina	Medina
U.S. Pat. 7,206,748	Filed: 12/10/1998	Gruse	Gruse 748

Defendants' contentions regarding where in the IBM DRM Systems each element of the Asserted Claims of the '342 and '106 Patents is found are provided in Appendices F-16 and I-19,

respectively. Defendants reserve the right to seek further information regarding the IBM DRM Systems during discovery. Defendants expects to prove its contentions regarding the IBM DRM Systems with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the IBM DRM Systems.

(4) Digibox System

The Digibox System is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at Electronic Publishing Resources, Inc. ("EPR"), and Olin Sibert, David Bernstein, David Van Wie, other individuals who presented, published, or demonstrated this system before the alleged invention of the '342 and '106 Patents; (2) in public use and/or on sale in this country more than one year before the filing date of the '342 and '106 Patents by personnel at EPR, and Olin Sibert, David Bernstein, David Van Wie, other individuals who presented, published, or demonstrated this system before the alleged invention of the '342 and '106 Patents. The Digibox System is prior art under 35 U.S.C. § 102(f) as the invention was derived by the alleged inventors during their work at EPR and the individuals who assisted in developing and implementing the Digibox System. The Digibox System is prior art under 35 U.S.C. § 102(g) because it was invented by EPR, and Olin Sibert, David Bernstein, David Van Wie, and the other individuals who assisted in developing and implementing the Digibox System, who did not abandon, suppress, or conceal, before the alleged invention of the '342 and '106 Patents. For each of these reasons, the Digibox System is also prior art under 35 U.S.C. § 103.

Upon information and belief, the Digibox System was first offered as a service in the United States by EPR as early as 1995. Upon information and belief, early versions of the Digibox Systems supported certificates and various encryption protocols.

The following documents are identified in support of the Digibox System, along with any other documents referencing the Digibox System produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
DigiBox: A Self-Protecting Container for Information Commerce	07/1995	Sibert	Sibert

Defendants' contentions regarding where in the Digibox System each element of the Asserted Claims of the '342 and '106 Patents is found are provided in Appendices F-17 and I-20, respectively. Defendants reserve the right to seek further information regarding the Digibox System during discovery. Defendants expects to prove its contentions regarding the Digibox System with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the Digibox System.

(5) Other Prior Art Systems

On information and belief, Citibank Systems, Xerox/Contentguard Systems, Viatech Systems, DigReg Systems, Adobe Systems, Symantec Systems, and Digimarc Systems are additional systems that constitute prior art under 35 U.S.C. §§ 102(a) and/or (b) because: (1) they were known or used in this country by the developers of each respective system and other individuals who presented, published, or demonstrated these systems before the alleged invention of the '342 and '106 Patents; and/or (2) in public use and/or on sale in this country more than one year before the filing date of the '342 and '106 Patents by the developers of each respective system and other individuals who presented, published, or demonstrated these systems before the alleged

invention of the '342 and '106 Patents. For each of the above reasons, each of these systems are also prior art under 35 U.S.C. § 103.

Upon information and belief, and subject to Defendants' present understanding of the Asserted Claims, its current construction of the claims, and/or Intertrust's apparent construction of the claims in its Infringement Contentions, each of the systems identified above, alone or in combination, satisfies each and every element of the Asserted Claims of the '342 and '106 Patents. Defendants reserve the right to seek further information regarding the systems identified above during discovery and supplement these Contentions accordingly. Defendants expect to prove with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the systems, that the above-identified systems satisfy each and every element of the Asserted Claims of the '342 and '106 Patents.

g. '627 Patent

Item Sold/Used	Date of Sale/Use[7]
Netscape System	No later than 1999
WMDRM System	No later than 1999
IBM DRM Systems	No later than 1999
Digibox System	No later than 1995

(1) Netscape System

The Netscape System is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at Netscape Communications, its successors-in-interest, including American Online, and Taher Elgamal, Jeff Weinstein, other individuals who

[7] These dates are provided upon information and belief. Defendants reserve the right to seek further information regarding these systems during discovery.

presented, published, or demonstrated this system before the alleged invention of the '627 Patent; (2) in public use and/or on sale in this country more than one year before the filing date of the '627 Patent by personnel at Netscape Communications, its successors-in-interest, including American Online, and Taher Elgamal, Jeff Weinstein, other individuals who presented, published, or demonstrated this system before the alleged invention of the '627 Patent. For each of these reasons, the Netscape System is also prior art under 35 U.S.C. § 103.

Upon information and belief, the Netscape System was first offered as a service in the United States by Netscape Communications as early as 1999. Upon information and belief, early versions of the Netscape Systems supported certificates and various encryption protocols.

The following documents are identified in support of the Netscape System, along with any other documents referencing the Netscape System produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
Netscape Certificate Management System Installation and Deployment Guide	1999	Netscape Communications Corp.	NCMS Install
Netscape Certificate Management System Administrator's Guide	1999	Netscape Communications Corp.	NCMS Admin
Netscape Certificate Management System Agent's Guide	1999	Netscape Communications Corp.	NCMS Agent
Netscape Certificate Management System Help	1999	Netscape Communications Corp.	NCMS Help
U.S. Pat. 5,657,390	Issued: 09/12/1997	Elgamal et al.	Elgamal 390
U.S. Pat. 5,671,279	Issued: 09/23/1997	Elgamal	Elgamal 279

Publication	Pub. Date	Author	Short Name
U.S. Pat. 6,094,485	Filed: 09/18/1997	Weinstein et al.	Weinstein
U.S. Pat. 6,138,107	Filed: 01/04/1996	Elgamal	Elgamal 107
U.S. Pat. 6,944,669	Priority: 10/22/1999	Saccocio	Saccocio
U.S. Pat. 7,013,390	Priority: 06/30/1997	Elgamal et al.	Elgamal 390
DOD, Netscape Ready PKI Rollout	07/18/1999	Verton	
CMS 401 Simplifies Certificates	09/13/1999	Barck	

Defendants' contentions regarding where in the Netscape System each element of the Asserted Claims of the '627 Patent is found are provided in Appendix J-14. Defendants reserve the right to seek further information regarding the Netscape System during discovery. Defendants expects to prove its contentions regarding the Netscape System with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the Netscape System.

(2) Windows Media Digital Rights Management (WMDRM) System

The WMDRM System is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at Microsoft Corporation, its successors-in-interest, and Peter Biddle, Bryan Willman, Paul England, Marcus Peinado, other individuals who presented, published, or demonstrated this system before the alleged invention of the '627 Patent; (2) in public use and/or on sale in this country more than one year before the filing date of the '627 Patent by personnel at Microsoft Corporation, its successors-in-interest, and Peter Biddle, Bryan Willman,

Paul England, Marcus Peinado, other individuals who presented,, published, or demonstrated this system before the alleged invention of the '627 Patent. For each of these reasons, the WMDRM System is also prior art under 35 U.S.C. § 103.

Upon information and belief, the WMDRM System was first offered as a service in the United States by Microsoft Corporation as early as 1999. Upon information and belief, early versions of the WMDRM Systems supported certificates and various encryption protocols.

The following documents are identified in support of the WMDRM System, along with any other documents referencing the WMDRM System produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
Windows Media Rights Manager Overview Webpage	05/19/2000	Microsoft Corp	WMDRM Overview
Windows Media Rights Manager Technical Features and Benefits Webpage	03/08/1999	Microsoft Corp	WMDRM Features
Windows Media Rights Manager FAQ Webpage	05/19/2000	Microsoft Corp	WMDRM FAQ
Windows Media Rights Manager 7 Webpage	06/05/2000	Microsoft Corp	WMDRM 7
Windows Media Encoder 7 Webpage	05/09/2000	Microsoft Corp	WM Encoder
Windows Media Format 7 Webpage	05/09/2000	Microsoft Corp	WM Format
Windows Media Tools Webpage	06/01/2000	Microsoft Corp	WM Tools
Windows Media Player 7 Beta Webpage	05/31/2000	Microsoft Corp	WM Player
Get Windows Media Player 7 Beta NOW! Webpage	04/13/2000	Microsoft Corp	

Publication	Pub. Date	Author	Short Name
Windows Media Technologies 4.1 Features Webpage	04/03/2000	Microsoft Corp	
Windows Media Technologies Home Webpage	11/17/1999	Microsoft Corp	
Windows Media on PressPass Webpage	2000	Microsoft Corp	
Windows Media Technologies 4 Delivers Cutting-Edge CD-Quality Audio on the Internet	09/17/1999	Microsoft Corp	
Microsoft and S3's Diamond Multimedia Showcase Rio Player in First Live Demonstration of Windows Media on SDMI-Capable Portable Device	11/15/1999	Microsoft Corp	
Supertracks and Microsoft Announce Windows Media Digital Rights Technology Integration for New Music Download and Promotion System	12/07/1999	Microsoft Corp.	
Microsoft and Texas Instruments Announce Native Windows Media Support on TI Programmable DSPs	12/07/1999	Microsoft Corp.	
Microsoft and Preview Systems Announce First Windows Media-Based Digital Audio and Video Distribution Solution for Retail Commerce	12/07/1999	Microsoft Corp.	
[MS-DRM]: Digital Rights Management License Protocol	06/01/2017	Microsoft Corp.	

Publication	Pub. Date	Author	Short Name
[MS-DRMND]: Windows Digital Rights Management (WMDRM): Network Devices Protocol	06/01/2017	Microsoft Corp.	

Defendants' contentions regarding where in the WMDRM System each element of the Asserted Claims of the '627 Patent is found are provided in Appendix J-15. Defendants reserve the right to seek further information regarding the WMDRM System during discovery. Defendants expects to prove its contentions regarding the WMDRM System with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the WMDRM System.

(3) IBM Digital Rights Management (DRM) Systems

The IBM DRM Systems, including Cryptolope Container Technology ("Cryptolope") and/or Electronic Media Management System (EMMS"), are prior art under 35 U.S.C. §§ 102(a) and (b) because they were (1) known or used in this country by personnel at International Business Machines ("IBM"), its successors-in-interest, and Jeff Crigler, Tim Byars, other individuals who presented, published, or demonstrated these systems before the alleged invention of the '627 Patent; (2) in public use and/or on sale in this country more than one year before the filing date of the '627 Patent by personnel at IBM, its successors-in-interest, and Jeff Crigler, Tim Byars, other individuals who presented,, published, or demonstrated these systems before the alleged invention of the '627 Patent. For each of these reasons, the IBM DRM Systems are also prior art under 35 U.S.C. § 103.

Upon information and belief, the IBM DRM Systems were first offered as a service in the United States by IBM as early as 1999. Upon information and belief, early versions of the IBM DRM Systems supported certificates and various encryption protocols.

The following documents are identified in support of the IBM DRM Systems, along with any other documents referencing the IBM DRM Systems produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
5799 – EMMS Content Mastering	05/03/2000	IBM	EMMS 5799
EMMS Software Suite	2001	IBM	
EMMS Frequently Asked Questions	Unknown	IBM	
IBM Electronic Media Management System, V2.1 – A Digital Rights Management Platform	01/29/2002	IBM	
BMG Entertainment Plans Adoption of IBM Technology For Commercial Roll-out of Electronic Music Distribution to Consumers	04/06/2000	IBM	
BMG Unveils Comprehensive Online Digital Downloading Plans for the Year 2000 and Beyond	04/06/2000	IBM	
Five Major Music Companies and IBM Successfully Complete Electronic Music Distribution Trial	02/02/2000	IBM	
IBM and Liquid Audio Team Up on Digital Music Technologies and Services	04/06/2000	IBM	

Publication	Pub. Date	Author	Short Name
IBM and Reciprocal Establish Strategic Relationship to Expand Digital Music Distribution	04/06/2000	IBM	
IBM and Sony Show First Results of Collaboration with Electronic Music Distribution	11/15/1999	IBM/Sony	
Leading Music Mastering Studio to Use IBM's Digital Rights Management Technology	07/24/2000	IBM	
Toshiba and IBM to Jointly Accelerate Digital Music Distribution Marketplace	03/13/2000	IBM	
Windows Media Technologies 4 Delivers Cutting-Edge CD-Quality Audio on the Internet	09/17/1999	IBM	
The Media Business; Sony and IBM Create Alliance on Delivering Music Over Net	04/16/1999	Richtel	
Cryptolope Live! Home Webpage	01/22/1998	IBM	Cryptolope Live! Webpage
IBM Introduces Cryptolope Live! Webpage	09/09/1997	IBM	
Cryptolope Container Technology Webpage	01/22/1998	IBM	Cryptolope Webpage
IBM infoMarket Saga	Various	Various	
IBM Make Cryptolope Deal	12/11/1996	CNet	
IBM Expands Its Digital Rights Management Technology	04/08/2002	IBM	
U.S. Pat. 6,389,538	Filed: 08/22/1998	Gruse	Gruse 538

Publication	Pub. Date	Author	Short Name
U.S. Pat. 6,398,245	Filed: 12/01/1998	Gruse	Gruse 245
U.S. Pat. 6,418,421	Filed: 12/10/1998	Hurtado	Hurtado
U.S. Pat. 6,574,609	Filed: 09/14/1998	Downs	Downs 609
U.S. Pat. 6,226,618	Priority: 08/03/1998	Downs	Downs
U.S. Pat. 6,587,837	Filed: 12/01/1998	Spagna	Spagna
U.S. Pat. 6,959,288	Filed: 02/01/1999	Medina	Medina
U.S. Pat. 7,206,748	Filed: 12/10/1998	Gruse	Gruse 748

Defendants' contentions regarding where in the IBM DRM Systems each element of the Asserted Claims of the '627 Patent is found are provided in Appendix J-16. Defendants reserve the right to seek further information regarding the IBM DRM Systems during discovery. Defendants expects to prove its contentions regarding the IBM DRM Systems with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the IBM DRM Systems.

(4) Digibox System

The Digibox System is prior art under 35 U.S.C. §§ 102(a) and (b) because (1) it was known or used in this country by personnel at Electronic Publishing Resources, Inc. ("EPR"), and Olin Sibert, David Bernstein, David Van Wie, other individuals who presented, published, or demonstrated this system before the alleged invention of the '627 Patent; (2) in public use and/or on sale in this country more than one year before the filing date of the '627 Patent by personnel at

EPR, and Olin Sibert, David Bernstein, David Van Wie, other individuals who presented, published, or demonstrated this system before the alleged invention of the '627 Patent. The Digibox System is prior art under 35 U.S.C. § 102(f) as the invention was derived by the alleged inventors during their work at EPR and the individuals who assisted in developing and implementing the Digibox System. The Digibox System is prior art under 35 U.S.C. § 102(g) because it was invented by EPR, and Olin Sibert, David Bernstein, David Van Wie, and the other individuals who assisted in developing and implementing the Digibox System, who did not abandon, suppress, or conceal, before the alleged invention of the '627 Patent. For each of these reasons, the Digibox System is also prior art under 35 U.S.C. § 103.

Upon information and belief, the Digibox System was first offered as a service in the United States by EPR as early as 1995. Upon information and belief, early versions of the Digibox Systems supported certificates and various encryption protocols.

The following documents are identified in support of the Digibox System, along with any other documents referencing the Digibox System produced with these disclosures or produced in Prior Actions:

Publication	Pub. Date	Author	Short Name
DigiBox: A Self-Protecting Container for Information Commerce	07/1995	Sibert	Sibert

Defendants' contentions regarding where in the Digibox System each element of the Asserted Claims of the '627 Patent is found are provided in Appendix J-17. Defendants reserve the right to seek further information regarding the Digibox System during discovery. Defendants expects to prove its contentions regarding the Digibox System with additional evidence, such as

source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the Digibox System.

(5) Other Prior Art Systems

On information and belief, Citibank Systems, Xerox/Contentguard Systems, Viatech Systems, DigReg Systems, Adobe Systems, Symantec Systems, and Digimarc Systems are additional systems that constitute prior art under 35 U.S.C. §§ 102(a) and/or (b) because: (1) they were known or used in this country by the developers of each respective system and other individuals who presented, published, or demonstrated these systems before the alleged invention of the '627 Patent; and/or (2) in public use and/or on sale in this country more than one year before the filing date of the '627 Patent by the developers of each respective system and other individuals who presented, published, or demonstrated these systems before the alleged invention of the '627 Patent. For each of the above reasons, each of these systems are also prior art under 35 U.S.C. § 103.

Upon information and belief, and subject to Defendants' present understanding of the Asserted Claims, its current construction of the claims, and/or Intertrust's apparent construction of the claims in its Infringement Contentions, each of the systems identified above, alone or in combination, satisfies each and every element of the Asserted Claims of the '627 Patent. Defendants reserve the right to seek further information regarding the systems identified above during discovery and supplement these Contentions accordingly. Defendants expect to prove with additional evidence, such as source code, testimony of percipient witnesses, and other contemporaneous documents regarding the development and commercialization of the systems, that the above-identified systems satisfy each and every element of the Asserted Claims of the '627 Patent.

B. P.R. 3-3(b) Disclosures: Each Item of Prior Art that Anticipates and/or Renders Obvious the Asserted Claim, and Obviousness Combinations and Motivations

Based on presently known information and the apparent constructions Intertrust is asserting in its Infringement Contentions, the prior art references identified above anticipate the Asserted Claims or, alone or in combination with the knowledge in the art, render the Asserted Claims obvious. To the extent Intertrust asserts that any of the prior art references charted in Appendices A-J fail to explicitly or inherently disclose any element of the Asserted Claims, Defendants contend that it would have been obvious to modify such reference to include the allegedly missing element, in view of the knowledge of one of ordinary skill in the art, the admitted prior art of the Asserted Patents, and/or in combination with any of the other prior art references identified in the Appendices for that respective Asserted Patent. For each element of the Asserted Claims, the following Appendices identify the prior art that discloses that element:

Appendix	Asserted Patent
A-Combination	’721 Patent
B- Combination	’304 Patent
C- Combination	’815 Patent
D- Combination	’602 Patent
E- Combination	’603 Patent
F-Combination	’342 Patent
G- Combination	’157 Patent
H- Combination	’158 Patent
I-Combination	’106 Patent
J- Combination	’627 Patent

1. Motivations to Combine

It would have been obvious to one of ordinary skill in the art to combine one or more of the prior art references listed above with each of the other references and/or nothing more than his

or her own knowledge, education, experience and/or common sense to arrive at the alleged invention of the Asserted Patents. As the Supreme Court emphasized in *KSR Int'l Co. v. Teleflex, Inc.,* inventions arising from ordinary innovation, ordinary skill, or common sense are not patentable. *See* 550 U.S. 398, 406, 420-422 (2007). In addition, "the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *Id*. at 416.

The identified prior art references also use those familiar elements for their primary or well-known purposes in a manner well within the ordinary level of skill in the art. In addition, the identified prior art addresses the same or similar technical issues relating to methods of controlling access to content. Accordingly, common sense and the knowledge of the prior art render the claims of the Asserted Patents invalid under either §§ 102 or 103.

The Supreme Court has held that, "[w]hen a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, § 103 likely bars its patentability. For the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill . . . ." *KSR,* 550 U.S. at 417.

Finally, as further described below, the motivation to combine the teachings of the prior art references disclosed herein is also found in the references themselves and in: (1) the nature of the problem being solved, (2) the express, implied, and inherent teachings of the prior art, including the admitted prior art of the Asserted Patents, (3) the knowledge of persons of ordinary skill in the art, (4) the fact that the prior art is generally directed towards the same subject matter as the

Asserted Patents, and/or (5) the predictable results obtained in combining the different elements of the prior art.

Defendants believe that no showing of a specific motivation to combine the identified prior art references described herein and in the attached charts is required, as each combination of art would have no unexpected results and at most would simply represent a known alternative to one of ordinary skill in the art. *See KSR,* 550 U.S. at 414-18 (rejecting the Federal Circuit's "rigid" application of the teaching, suggestion, or motivation to combine test, instead espousing an "expansive and flexible" approach). Indeed, the Supreme Court held that a person of ordinary skill in the art is "a person of ordinary creativity, not an automaton" and "in many cases a person of ordinary skill in the art will be able to fit the teachings of multiple patents together like pieces of a puzzle." *Id*. at 421. Nevertheless, in addition to the information contained in this section and elsewhere in these contentions, Defendants identify the following motivations and reasons to combine the cited art. In addition, Defendants incorporate by reference any and all motivations to combine set forth in the prosecution history for the Asserted Patents and/or patents and applications related thereto.

a. Motivations to Combine Prior Art for the '721 Patent

Motivations to combine any of the prior art references identified herein for the '721 Patent with one another exists within the references themselves, as well as within the knowledge of those of ordinary skill in the art at the relevant time.

(1) Technical incentives and market forces drove similar solutions in the prior art.

Regarding the '721 Patent, many of the identified prior art references address the same technical issues and suggest similar solutions in the field of computer security using public key cryptography. Indeed, the need for an effective method to preserve a computer processing

environment from harmful or fraudulent content that originates from any source, including the user, and more generally a need to distinguish trusted and untrusted content in such an environment, are problems already recognized in the prior art and the field of the invention and would provide a person of ordinary skill in the art motivation to combine the prior art references identified above.

For example, Arnold '408 recognizes that in order "to maintain data confidentiality, readily determine the authenticity of data, and closely control access to data," a "combination of elements must work together to achieve a more secure environment." Arnold '408 at 1:18-20 and 42-43. Therefore, like the '721 patent, Arnold '408 describes the need of a computer processing environment to distinguish fraudulent content from genuine content that is appropriate for execution, and offers as a motivation for combining the prior art the example of a software distribution system in which both the manufacturer and the end user wish to ensure the integrity of programs, data, and upgrades thereto . *See* Arnold '408 at 3:6-5:30. As noted by Arnold '408:

> It is easy to see why this kind of flexibility is highly desirable, for both the manufacturer and the user. There is a significant impediment to its use, however; security.
>
> Both the manufacturer and user want to be sure they have control over programs that are loaded into the memory. The manufacturer may want to make sure only its programs are used, to ensure the programs meet quality and performance standards. The manufacturer may also want to prevent anyone from learning how the software works, or what the data is that is being sent to the user. The user, on the other hand, wants to make sure the programs in the devices are valid, and prevent any that might malfunction, or which might pose a security threat. An example of a security threat would be a "Trojan horse" program which would normally operate correctly, but which had "secret" features to circumvent the user's security practices, or to divulge the user's secret information.
>
> Typically, there will be one source for all field upgrades to code or configuration data, although other scenarios are possible. For the purposes of discussion, assume that the device manufacturer is the only valid source of code or data updates; and the device is a security adapter card, with a secured area or module where data is protected from disclosure. The problem can then be described with two fundamental requirements:

> First, data sent to the user must be kept secret. It must be impossible for anyone to discover or modify the contents of the data.
>
> Second, the user must be able to verify that: the data came from the valid source (e.g., the manufacturer). This is a form of non-repudiation.

Arnold '408 at 4:65-5:30.

Arnold '408 presents a solution that mirrors that of the '721 patent: a public key based digital signature verification technique that stores a public key behind a tamper resistant area to protect the key and all functions associated with it from manipulation by even the user. As explained by Arnold '408:

> Functions are housed within a tamper-resistant module, or secured area, for protection,…
>
> The user receives this information, and loads the data and signature into the secured area of the adapter card in step 140. In step 150, the adapter decrypts the data using the public key K_{PU}, recovering the clear data D. Following this, in step 160, the digital signature is verified using the same key. If the signature verifies, the data is genuine and it can only have been created by the manufacturer, who holds the private key K_{PR}. Once the data has been decrypted and its validity has been determined, the data is applied to the nonvolatile memory in the adapter card, step 180; otherwise, the information is discarded, step 170….
>
> In step 260, the data is received at the user site where adapter cards are installed. The data is loaded into the secured area of the card, which contains the public key KPU. In step 270, KPU is used to decrypt the symmetric key KS using the public key algorithm. In step 280, the recovered KS is used to decrypt the data using the symmetric key algorithm. In step 290, the digital signature is verified using KPU, in order to verify the origin of the data. If the signature verifies, it means that both the data D and the key KS were valid; in this case, the data is loaded into the nonvolatile memory on the adapter card and enabled for use, step 310. Otherwise, the data is discarded or otherwise rejected. All cryptographic calculations are preferably performed inside the secured area, so there is no threat of data manipulation while the data is recovered and verified.

Arnold '408 at 4:5-6; 7:28-36; 8: 5-20.

As another example, McManis '575 also describes the limitations of the then existing computer security systems in ensuring that content that is to be executed is genuine :

> As a result, there are number of reasons why it is desirable to have a computer system that is designed to primarily execute integrity verifiableANPrograms but also has the capability of executing integrity non-verifiable ASPrograms.
>
> Although compilation of ANPrograms by a third party is possible, such compilations require that the third party be authenticated. That is, it must be possible to verify from the information in the compiled ASProgram that it was compiled by a specific trusted third party. Even better, it should also be possible to authenticate that the compiled ASProgram was generated by a specific trusted compiler. And, since the integrity of the compiled ASProgram with respect to predefined integrity criteria cannot be directly verified, the compiled ASProgram should include information that in a verifiable manner identifies the corresponding ANProgram from which it was compiled and the ASLanguage in which it was compiled.

McManis '575 at 2: 17-34. McManis '575 describes a solution that reflects the public key cryptographic system of the '721 Patent:

> A generally available, trusted repository of public encryption keys, sometimes called a naming service, holds the public keys for the compiler and the trusted compiling party. Using these public encryption keys all recipients of the compiled program can decrypt the digital signatures in the compiled program to verify that the compiled program was compiled by the indicated trusted party and by the indicated compiler, and also to verify the identity of the corresponding architecture neutral program.

Id. at 3:51-59. Additional references provide solutions in the context of computer security achieved through cryptographic techniques including:

- "Care must be taken to ensure that the (secret) public key is never inadvertently exposed…The Verify Application Digital Signature instruction validates a digital signature, called dsig, using an input hash value (called hash-val) and a public key PU in accordance with Section 7 of ISO DIS 9796." Matyas at 11:12-13 and 122:12-15.

- "The network controls user verification through a single public key exponent, e, and modulus, n. The e and n values are available to all terminals in the network. The private (i.e., secret) public key, d, corresponding to e and n is contained in a secure environment only at the card issuer site." Hopkins at 7:24-29.

- "This invention provides a method and apparatus utilizing public key encryption techniques for enhancing software security and for distributing software." Chang at 3:15-17.

- "The corresponding secret key is held securely in the first storage means of an SPD. When the secure module is received by the SPD the secret key is used to decrypt the DES key which is then used to decrypt the secure module and this module is stored in the third storage means. The SPD processor and the host computer may then operate in series or parallel to run the software but the SPD is so arranged that the secret key, the DES key and, usually, the decoded module cannot be obtained from the SPD." Chorley at 2:31-40.

- "According to another aspect of the present invention there is provided a method for generating and managing a secret key of a public key cryptosystem, comprising the steps of: (a) generating a public key and a secret key inside a first tamper resistant device…." Chang at 4:1-5.

- "In this case, for example, the public key is known only to all trusted servers 200 and trusted agents 120 and is sealed within their tamper-proof housings… Concurrently, Public Key A verifies the encrypted electronic object's signature using B's public key (steps 508-510)." Rosen '518 at 10:63-65; 19:17-19.

- "In addition, because the sender of the message and the intended receiver of the message each have a unique n and e, the sender and receiver can each guarantee the authentication of the other by an encrypted 'signature', encrypted using their separate n's and e's and decrypted using their separate d's…. This also requires the same central location which generates and provides the 'secret' public-key decryption key also, at least at some time prior to providing this decryption key to a subscriber, know this key." Miller at 2:59-64; 4:37-41.

- "As described above, decryption of the key module is performed in the data encryption/decryption module 70 of RCM 18. The encryption key used in the decryption process is inaccessible to the user. Thus, in accordance with the present invention, a downloaded rental software package will only run on the particular target computer 14 having an encryption key corresponding to the encryption key employed by the host computer 12 when the key module of the rental software package was encrypted." Hornbuckle at 12:34-37.

- "Thus, if a well-known manufacturer of programs has signed the program with a public key or digital certificate, then, if desired, such a program may be assigned whatever level of authority desired depending upon how much the manufacturer is trusted and the system may permit execution of such program. Such a digital signature from the manufacturer can be used to verify that the associated program had not been infected with a virus since it can be determined whether or not the program is exactly the same as it was when it was generated by the manufacturer. If the check in block 306 indicates that there is a digital signature." Fischer '717 at 16:15-25.

- "In a preferred embodiment of the present invention, the tamper-resistant chip, or a tamper-resistant trusted device containing the chip, that performs the encryption, decryption and digital signature is embedded with a non- modifiable public/private

signature key pair unique to that chip and with a 'manufacturer's certificate.'" Sudia at 22.

- "For the same reason the software vendor's decryption keys (such as AK) are never exposed to the software user, the hardware vendor's encryption keys (CSK) are never exposed to the software vendor… It should be understood that the coprocessor must have at least two levels of privilege so that the memory used to store AKs can be properly secured from the user." Chandra at 4:50-53; 16:5-8

- Depending on the authentication technique chosen, the public key and the private key of a certification key pair may need to be protected…If the certification public key is kept confidential (i.e., only available in plaintext inside the PPE 650), it may make cracking security much more difficult. Ginter '987 at 210: 20-23 and 30-33.

Here, regarding the '721 Patent, market forces demanded that computer processing environments be protected from fraudulent or harmful content originating from any source, including users. Thus, one of skill in the art would have been motivated to combine or modify references using known methods that one of skill in the art would have recognized as offering improvements to solutions of that time. The references identified describe methods that were known to offer improvements, and, accordingly, one of skill in the art would have been motivated to combine or modify combined references to include such improvements.

(2) Combination of known elements yields predictable results.

Because the Asserted Claims of the '721 Patent simply arrange old elements known in the field of computer security, with each performing the same function it had been known to perform, and yields no more than what one would expect from such an arrangement, combinations of the prior art are obvious. At the time of the alleged invention of the '721 Patent, there were a finite number of predictable solutions for computer security, including the use of public key cryptography for the purpose of preserving the integrity of computer processing environments against fraudulent or harmful content, and thus a person of ordinary skill in the art had good reason to pursue and/or combine known options and related applications.

Moreover, the alleged invention of the '721 Patent encompasses nothing more than old technology that significantly pre-dates the alleged priority date. The '721 patent admits that the digital signature of its alleged invention may be implemented by "many well-known processes for creating digital signatures." '721 Patent at 10:60-61. Among the various asymmetric key cryptography algorithms that antedate the priority date, the '721 Patent identifies the Digital Signature Algorithm (DSA), a technique that dates from the early 1990s, and the Rivest–Shamir–Adleman (RSA) algorithm, which was devised even earlier in the 1970s. '721 Patent at 10:60-65 and 13:43-46. Therefore, a person of ordinary skill in the art would have known to use such conventional public key cryptographic techniques to practice the digital signature verification recited in asserted claims 9 and 29.

The asserted claims also relate to securing a public key behind a tamper resistant barrier and therefore having it hidden from the user. Tamper resistant data storage was already old as of the priority date of the '721 patent, as was its use to keep a public key hidden from a user. For instance, Arnold '408 describes a cryptographic device "housed within a tamper-resistant module, or secured area, for protection…." Arnold '408 at 4:5-6. Arnold further teaches that a public key K_{PU} that is used to verify digital signatures is stored in this tamper-resistant secured area. *Id*. at 8:5-20. Likewise, Rosen '518 describes "[a] public key [that] is known only to all trusted servers 200 and trusted agents 120 and is sealed within their tamper-proof housings." Rosen '518 at 10:63-65. Similarly, Chandra recognizes the need to hide keys from users when describing a "coprocessor [that] must have at least two levels of privilege so that the memory used to store AKs can be properly secured from the user. This is needed because the user could be a writer-of-software." *See also, e.g.,* Ginter '987 at 3: 63–4: 7, 20: 31–54, 21:9-25, 47:15-32, and 57:40-51.

See also Hornbuckle at 12:34-37. Therefore, a person of ordinary skill in the art would have been motivated to use tamper resistant means to keep a public key hidden from the user.

A person of ordinary skill in the art having knowledge of this prior art, public key cryptographic algorithms, and tamper resistant storage, among other things, would have been motivated to combine the prior art as identified above. For example, it would have been obvious to a person of ordinary skill in the art to combine Chang with Arnold '408 in order to secure the public key of Chang behind a tamper resistant secured area as taught in Arnold '408 and therefore hide it from the user. Chang discloses the use of a public key to verify a signature associated with a load module in the form of data or software. *See, e.g.,* Chang at 9:34-10:5. Arnold '408 recognizes that a public key that is used for verifying a signature may be vulnerable to manipulation. Arnold '408 at 7:28-36; 8:5-20. Arnold '408 addresses this vulnerability by securing the public key behind a tamper resistant secured area and therefore hiding the key from the user. Arnold '408 at 4:5-8; 11:3-6. At the time of the alleged invention of the '721 Patent, a person of ordinary skill in the art would have known that a public key used to verify a digital signature could be secured behind a tamper resistant barrier and therefore hidden from the user, thereby preserving the key from fraudulent manipulation by anyone, including the user.

Further, motivation exists because the prior art references all are commonly related and are from the same field of art, and a person of ordinary skill in the art would draw equally from the field of art to solve the problem allegedly presented in the '721 Patent. The suggested combinations reflect at least combinations of prior art elements according to known methods to yield predictable results, simple substitutions of known elements to obtain predictable results, and combinations that are obvious to try. Further elaboration and information shall be provided with Defendants' expert reports.

(3) Exemplary prior art combinations

As discussed above, Appendix A-Combination set out the references that disclose each element of the Asserted Claims of the '721 Patent, and Defendants contend that it would have been obvious to modify such references to include any allegedly missing element, in view of the knowledge of one of ordinary skill in the art, the admitted prior art of the '721 Patent, and/or in combination with any of the other prior art references identified in the '721 Patent. By way of example, and without limitation, Defendants provide the following exemplary combinations for particular claim limitations based on teachings of the cited prior art references. Defendants reserve the right to rely upon any combination of prior art references whether listed herein or otherwise.

Claims [721.9a] and [721.29a] – Receiving a Load Module/Executable

To the extent a reference does not expressly or inherently disclose receiving a load module/executable, it would have been obvious to one skilled in the art at the time of the alleged conception of the '721 Patent to do so because doing so was one of a finite number of known ways to send the same content to a recipient. For example, the '721 patent itself recognizes that receiving a load module would have been obvious to one of ordinary skill in the art. '721 Patent at 3:16–23; 8: 34–40.

This limitation is also rendered obvious by the teachings of Arnold '408. Arnold '408 is directed to the "secure distribution of software, software updates, and configuration data," in which a user receives such information protected via cryptographic techniques. Arnold '408 at 1:11-13; 5:36-38. Arnold '408 teaches that, after a manufacturer sends encrypted data and an associated digital signature, "The user receives this information, and loads the data and signature into the secured area of the adapter card in step 140." Arnold '408 at 7:25-27.

McManis '575 also teaches this limitation at 6:42-43, which states "The transmitted ANProgram 200 is then received at the server computer 104." *See also id*. at 8:62-65.

This limitation is also taught by Chang at 8:49-65:

> As shown in FIG. 4, the generated software passport 38, including the application code is then distributed using any desired software distribution model. The passport 38 is received by a user and is executed using an operating system (OS) running on a computer system ("platform") such as the system of FIG. 1. Referring now to FIG. 5, the use of the present invention by platform builders will be described. In the electronic game industry and the interactive television cable set-top box industry, platform producers often desire to allow only authorized code to be executed on their particular platform. To be able to control the accessibility of a platform, the received code must be identifiable and the platform must be able to identify the software when it arrives. As illustrated in FIG. 5, the present invention may be applied in a platform producer licensing scheme with particular application for use in settop box and video game environments.

See also id. at 4:9-43.

Likewise, Ishii at 19:66-20:4 states:

> The contents server 31 provides a service. A user who wish to receive this service inserts the personal portable device 34 into the user terminal 33, and operates this user terminal 33 such that the desired contents are distributed from the contents server 31 through the network 32 to the user terminal 33.

See also id. at 20:41-47.

Hornbuckle also teaches this limitation at 2:54-3:5:

> In the software rental system of the present invention, a control module is installed on or in cooperation with the customer's computer (hereafter also target computer), and the customer pays for services, i.e., the use of the software, received. While operation of the system is as convenient to use, substantially different features, advantages and implementation with respect to the corresponding television system are necessary and desirable. Specifically, the customer in a software rental system may rent any program of an entire library of computer programs at any time, rather than waiting for a particular time slot during which a particular program would be available. Moreover, it is not necessary to install a separate transmission system, such as a TV cable system, to access programs, since they are downloaded over conventional telephone lines. Finally, the software available for rent is not broadcast over the entire system, but rather individual programs are down-loaded to the user's system from the host only after selection by the user.

Similarly, Chandra at 3:22-51 teaches:

> The present invention is based on the recognition that today's software distribution techniques distribute to the user, in addition to the software itself, the right to execute that software. That is, more particularly, when software is sold to the typical user, the user acquires not only the software itself but the right to use it. However, he can, with a typical personal computer, duplicate the software and distribute it along with the (implied) right to use it to others. The invention seeks to separate the software, from the right to use it. Further, it seeks to place the means of creating these Rights-to-Execute in the hands of the software authors or their representatives. It also seeks to do these things with no perturbation to the existing or planned channels of software distribution and minimum change to the means by which software is prepared for distribution. As will be described below, in accordance with the present invention, the typical software purchaser may still duplicate at will the software he has received from the vendor. However, he cannot duplicate the right to use the software; in fact he receives a single right to use the software. To become effective, that right to use must be installed in a suitable coprocessor, and it is only when the right to use is installed on the suitable coprocessor (which is associated with the host computer on which the user intends to run the software) that the software becomes executable. Other copies of the software that the user might make are not executable on any other host computer (even if such other host computer is associated with another suitable coprocessor).

Accordingly, based on at least these prior art references, receiving a load module or executable was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged priority date of the alleged invention of the ’721 Patent to include such functionality in combinations for the reasons discussed above including, for example, that doing so would be applying a known technique to other computer security systems to achieve the same result.

Claims [721.9b] and [721.29b] – Determining a Digital Signature Associated with the Load Module/Executable

To the extent a reference does not expressly or inherently disclose determining whether the load module/executable has an associated digital signature, it would have been obvious to one skilled in the art at the time of the alleged priority date of the alleged invention of the ’721 Patent to do so because doing so was one of a finite number of known ways to send the same content to

multiple recipients. For example, the '721 Patent itself, at 4:31-35, acknowledges that associating a digital signature with a load module or executable was well known as of this date: "Ginter et al. specification discloses… Strictly controlling initiation of load module execution by use of encryption keys, digital signatures and/or tags…."

This limitation is also taught by Arnold '408, which at 7:8-9 states "In step 110, the manufacturer computes a digital signature on the data D using the private key K_{PR}."

Likewise, Rosen '518 at 6:7-11 teaches:

> An Object Signature field 44 contains a digital signature of the electronic object. Digital signatures are well known in the art and are used to detect if a signed electronic object has been altered in any way since the time it was signed.

Similarly, Sudia at 25 discloses:

> The manufacturer's public signature key can be used by the user to verify instructions received from others by checking whether those instructions have attached a valid digital signature created by the manufacturer's private signature key, in order to determine whether those instructions originated with the manufacturer or one trusted by the manufacturer.

Therefore, based on at least these prior art references, determining whether the load module/executable has an associated digital signature was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged priority date of the alleged invention of the '721 Patent to include such functionality in combinations for the reasons discussed above including, for example, that doing so would be applying a known technique to other computer security systems to achieve the same result.

Claim [721.9c] and [721.29c] – Verifying the Digital Signature with a Public Key Secured Behind a Tamper Resistant Barrier and Therefore Hidden from the User

To the extent a reference does not expressly or inherently disclose "if the load module[or executable] has an associated digital signature, authenticating the digital signature using at least

one public key secured behind a tamper resistant barrier and therefore hidden from the user," these limitations are rendered obvious by the teachings of, at least, Arnold '408. Arnold '408 employs a public key K_{PU} and an associated digital signature to preserve the integrity of data D. Specifically, Arnold '408 teaches the verification of a digital signature that is associated with a "load module" like data D at 7:28-33:

> In step 150, the adapter decrypts the data using the public key K_{PU}, recovering the clear data D. Following this, in step 160, the digital signature is verified using the same key. If the signature verifies, the data is genuine and it can only have been created by the manufacturer, who holds the private key K_{PR}.

Similarly, Arnold '408 teaches securing public key K_{PU} behind a tamper resistant barrier at 4:5-6, which states "Functions are housed within a tamper resistant module, or secured area, for protection…," and at 11:5-6, which states "wherein said public key is stored within said secured area…." The tamper resistant secured area protects public key K_{PU} from manipulation, as explained by Arnold '408 at 8:12-20:

> In step 290, the digital signature is verified using KPU, in order to verify the origin of the data. If the signature verifies, it means that both the data D and the key KS were valid; in this case, the data is loaded into the nonvolatile memory on the adapter card and enabled for use, step 310. Otherwise, the data is discarded or otherwise rejected. All cryptographic calculations are preferably performed inside the secured area, so there is no threat of data manipulation while the data is recovered and verified.

Likewise, Chandra, in a content protection system that includes "a physically and logically secure coprocessor [that] is associated with a host computer," "decrypt[s] the software decryption key so it can thereafter decrypt the software, for execution purposes." *Id.* at Abstract. Chandra further teaches that the decryption key AK is to be kept hidden from the user. Specifically, with regard to decryption key AK, Chandra teaches at 16:5-15:

> It should be understood that the coprocessor must have at least two levels of privilege so that the memory used to store AKs can be properly secured from the user. This is needed because the user could be a writer-of-software. If the software executed on behalf of one author could read the AKs of other authors, the user-authors could recover other authors' AKs and decrypt their protected software. Management of installation, use of, and access to AKs should be understood to be important functions of the higher level of privilege to the system.

See also id. at 4:50-58; 16:21-30.

Sudia is directed to a "tamper-resistant chip, or a tamper-resistant trusted device containing the chip, that performs the encryption, decryption and digital signature [and] is embedded with a non-modifiable public/private signature key pair unique to that chip and with a 'manufacturer's certificate.'" Sudia at 22 (insertion added). Similar to the use described by the '721 Patent of a tamper resistant barrier to secure a public key, Sudia employs its tamper-resistant chip to secure public keys intended for use in cryptographic verification operations. Specifically, Sudia teaches at 25-26:

> A chip manufactured for use in an embodiment of the present invention would also include the manufacturer's public signature verification key embedded within the chip in a tamper-resistant manner. The manufacturer's public signature key can be used by the user to verify instructions received from others by checking whether those instructions have attached a valid digital signature created by the manufacturer's private signature key, in order to determine whether those instructions originated with the manufacturer or one trusted by the manufacturer. The chip may also include embedded and tamper-resistant public instructions keys that can be used by the user to verify instructions received from others. The public instructions key could be the public key of some other trusted entity, such as Bankers Trust Co., selected by the manufacturer or could be the public key of a trusted national or global system-wide authority, and may optionally be embedded into the chip by the manufacturer for use as a "short-cut" to avoid having to verify the extra manufacturer-to-trusted-entity certificate. The manufacturer could install several instruction keys of various qualified key escrow houses that the manufacturer selects and believes to be capable and trusted.

Rosen ’518 relates to a “cryptographically secure communication” system that employs a “tamper-proof” “trusted agent” in which public keys are “sealed.” Rosen ’518 at 4:10-20; 10: 64-67. As stated at 10:56-67 of Rosen ’518:

> Each primary trusted server 210 has its own public key and corresponding private key. The primary trusted server public keys are commonly shared by all trusted servers 200 and trusted agents 120 in the system. These public keys are stored in a primary trusted server public key (PTS(PK)) list. The term "public" key as used here and throughout the specification, does not imply that the key is known to the public at large. In this case, for example, the public key is known only to all trusted servers 200 and trusted agents 120 and is sealed within their tamper-proof housings. This limited sense of "public" provides added security to the system as a whole.

Similarly, Ishii at 7:15-18 describes a “key and certification generation mechanism 110 [that] is formed by a container which is physically and electrically protected such that a reading of a generated secret key and a tampering of a generated certification cannot be made by anyone in any way whatsoever.” Ishii teaches at 32:24-39 that this tamper resistant device also secures public keys:

> The method of claim 1, further comprising the steps of: (d) generating a public key of the public key cryptosystem inside the tamper resistant device in correspondence to the secret key generated at the step (a); (e) storing public keys generated at the step (d) in past inside the tamper resistant device; (f) checking whether a new public key generated at the step (d) overlaps with any previously generated public key stored at the step (e) inside the tamper resistant device; and (g) producing a certification by signing the new public key generated at the step (d) inside the tamper resistant device when the step (f) indicates that the new public key is not overlapping with any previously generated public key.

See also id. at 23:34-53; 33:6-21.

Hopkins similarly teaches at 7:24-32:

> The network controls user verification through a single public key exponent, e, and modulus, n. The e and n values are available to all terminals in the network. The private (i.e., secret) public key, d, corresponding to e and n is contained in a secure environment only at the card issuer site. The private public key, d, does play a role

> in the card personalization process, but is not present in the card or in the verification terminal, nor anywhere in the transaction processing network.

See also id. at 8:46-47.

Therefore, based at least on the prior art discussed above, the verification of a digital signature through the use of a public key that is secured behind a tamper resistant barrier and therefore hidden from the user was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged priority date of the alleged invention of the '721 Patent to secure a public key in this manner and include such functionality in combinations for the reasons discussed above including, for example, that doing so would preserve content from unauthorized access and thus would amount to applying a known technique to other computer security systems to achieve the same result.

Claims [721.9d] and [721.29.d] – Conditioning Execution of the Load Module/Executable on the Authentication of the Digital Signature

To the extent a reference does not expressly or inherently disclose "conditionally executing the load module[/executable] based at least in part on the results of authenticating step (c)", these limitations are rendered obvious by the teachings of, at least, Arnold '408. Arnold '408 conditions the use of data on a successful verification of a digital signature, as described at 7:21-35:

> The manufacturer, in step 130, sends the encrypted data pke(D) and the digital signature dsig(D) to the card users through any convenient channel; diskettes, electronic mail, or any other medium is sufficient. The user receives this information, and loads the data and signature into the secured area of the adapter card in step 140. In step 150, the adapter decrypts the data using the public key K_{PU}, recovering the clear data D. Following this, in step 160, the digital signature is verified using the same key. If the signature verifies, the data is genuine and it can only have been created by the manufacturer, who holds the private key K_{PR}. Once the data has been decrypted and its validity has been determined, the data is applied to the nonvolatile memory in the adapter card, step 180; otherwise, the information is discarded, step 170.

See also id. at 8:5-20; 10:58-12:7

Likewise, Chang conditions the execution of binary code on a successful signature verification, as described at 3:38-65:

> A user, upon receipt of the software passport, loads the passport into a computer which determines whether the software passport includes the application writer's license and digital signature. In the event that the software passport does not include the application writer's license, or the application writer's digital signature, then the user's computer system discards the software passport and does not execute the binary code. As an additional security step, the user's computer computes a second message digest for the software passport and compares it to the first message digest, such that if the first and second message digests are not equal, the software passport is also rejected by the user's computer and the code is not executed. If the first and second message digests are equal, the user's computer extracts the application writer's public key from the application writer's license for verification. The application writer's digital signature is decrypted using the application writer's public key. The user's computer then compares a message digest of the binary code to be executed, with the decrypted application writer's digital signature, such that if they are equal, the user's computer executes the binary code. Accordingly, software products distributed with the present invention's software passport permits the user's computer to authenticate the software as created by an authorized application writer who has been issued a valid application writer's license. Any unauthorized changes to the binary code comprising the distributed software is evident through the comparison of the calculated and encrypted message digests.

Similarly, McManis ’575 teaches, at 3:27-31, that “The program executing computer also includes an architecture specific program executer that, when the digital signatures in the architecture specific program have been verified, executes the architecture specific program code of the architecture specific program.” *See also id.* at Abstract and 18:25-67.

Therefore, based at least on the prior art discussed above, conditionally executing the load module based at least in part on the results of a digital signature authenticating step was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged priority date of the ’721 Patent to include such functionality in combinations for the reasons discussed above including, for example, that doing so would be applying a known technique to other computer security systems to achieve the same result.

b. Motivations to Combine Prior Art for the '304, '157, and '158 Patents

Motivations to combine any of the prior art references identified herein for the '304, '157, and '158 Patents with one another exists within the references themselves, as well as within the knowledge of those of ordinary skill in the art at the relevant time.

(1) Technical incentives and market forces drove similar solutions in the prior art.

Regarding the '304, '157, and '158 Patents, which share a specification and similar claims, many of the identified prior art references address the same technical issues and suggest similar solutions in the field of content protection. Indeed, the need for effective methods to monitor and secure types of electronic data to ensure that the proper recipient has authorization and access to use the data is a problem long recognized in the prior art, and methods for content protection were well-known, well-developed, and well-utilized in the distributions of content such as software and cable television. Thus, a person of ordinary skill in the art would be motivated to combine the prior art references identified *supra* to control the use of electronic content in the manner of the claims of the '304, '157, and '158 Patents.

For example, like the '304 Patent, '157 Patent, and '158 Patent, ABYSS 1987 identifies the problem of data protection, and the need for technical solutions thereto as legal remedies were inadequate. ABYSS 1987 at 38. ABYSS 1987 describes the limitations of existing electronic content systems, and the need for optimized control over them:

> These technical methods have not succeeded because of two complementary shortcomings. First, they are not an effective barrier to duplication. Today's low-end computers are both logically and physically open systems. In fact, most commercial computers of any kind are open, at least to those with operator privileges. The user (or operator) is capable of examining every memory location, and every processor cycle, of the system. Once the behavior of the application is understood, it can be changed to subvert the software protection measures. Similarly, distribution

> media are completely open to examination and modification. Second, existing technical methods have imposed unacceptable burdens on the legitimate user. Users are often prevented from making backup copies of their software, and from installing their software on hard disks or file servers.

ABYSS 1987 at 38. Thus, nearly a decade before the priority date of the '304, '157, and '158 Patents, ABYSS 1987 identified a need for data protection that prevented duplication or examination of secured content, and was not burdensome on a user. ABYSS 1987 proceeded to describe such a system, and the technical solutions that would provide for it:

> The trend in the software market today is to abandon technical protection methods, and rely solely upon legal protection. This is difficult at best in the widely distributed and anonymous marketplace often addressed by low end software. It is impossible in countries and cultures which have no history of intellectual property law [Chur86]. So, the need for practical technical protection measures continues, and grows.
>
> A practical software protection system must overcome both of the shortcomings outlined above. It must be extremely secure, and ensure that the effort involved in illicitly duplicating an application is at least as large as that involved in rewriting it from scratch. It must also be extremely convenient for the legitimate user, and flexible enough to support a broad spectrum of computing environments and software distribution systems. A variety of authors have explored ideas which go beyond the more common diskette-based protection schemes, in an attempt to meet the requirements of increased security and convenience.

ABYSS 1987 at 38.

This need to protect electronic data was appreciated by industries active in the distribution and processing of electronic content, which sought solutions to protect the content. Specifically, the prior art references identified ways to protect this data, including the use of encryption.

- "Maintaining security in a conditional-access television network depends on the following requirements:
  (i) The signal scrambling techniques must be sufficiently complex to insure that direct encryptographic attack is not practical.
  (ii) keys distributed to an authorized decoder cannot be read out and transferred to other decoders.

The first condition can be satisfied by practical scrambling algorithms now available such as the DES (Data Encryption Standard) or related algorithms.
The second condition requires the physical security of certain devices within the television signal decoder and is much more difficult to satisfy. Such a device must prevent observation of both the key decryption process and the partially decrypted key signals." Gammie at 2:27-42.

- "It is therefore an object of the invention to provide an improved method of data cryptography.
  It is another object of the invention to provide an improved method of data cryptography which is more flexible than in the prior art.
  It is another object of the invention to provide an improved data cryptography method which controls the authorization of users to encrypt, decrypt or authenticate data in accordance with a security policy established by the system manager.
  It is another object of the invention to provide a data cryptographic method which builds into the storage of a key the authority to use that key in a manner which has been authorized by its originator.
  It is an object of the invention to improve file security by providing the ability to encrypt a data file so that one portion is fully encrypted and another portion can be decrypted by authorized recipients." Matyas at 2:7-24.

- "In some of these satellite television broadcasting systems, unlike conventional type terrestrial television broadcasting, to which anybody is entitled to have access, a scrambled television program is transmitted so that only the subscribed viewers who signed the viewing contract can view the program, and the subscribed viewers receive the program on a pay basis using a tuner/decoder, which can descramble the program." Saito at 1:18-25.

- "It is essentially straightforward to protect services during transmission by encrypting the service keys and by rapidly changing the service keys in a random manner. The main security problem arises in protecting the service keys from compromise during distribution. For that purpose, a device is required with the following characteristics:
  (1) capable of highly sophisticated decryption techniques;
  (2) factory programmable;
  (3) immune to modification or copying; and
  (4) including protected non-volatile memory." Smith at 40:9-21.

The prior art further identified protecting data by means of authorization, registration, or tamper resistance:

- "A process and system for activating various programs are provided in a personal computer (10), The personal computer (10) is initially provided with a registration shell program (11). A data link (30) is established between the personal computer (10) and a registration computer (12). By providing the registration computer (12) with various information, a potential licensee can register to utilize the main program (16). Once the registration process is complete, a tamperproof overlay program is constructed at the registration

computer (12) and transferred to the personal computer (10). The tamperproof overlay includes critical portions of the main program (16), without which the main program (16) would not operate and also contains licensee identification and license control data." Waite at Abstract.

- "The present invention relates to remotely controlling and monitoring the use of computer software. More particularly, this invention relates to a system for renting computer software products while 1) deriving customer use and billing information; 2) preventing unauthorized copying and use; 3) maintaining the integrity of the rented software product (hereafter also "package"); and 4) controlling related voice, program and data communications between the host and user's computers." Hornbuckle at 1:15-23.

- "The present invention is a method and system for controlling and accounting for retrieval of data from a memory containing an encrypted data file from which retrieval must be authorized. The system includes means for authorizing such retrieval by providing an encryption key for enabling retrieval of the data and a credit signal for use in limiting the amount of data to be retrieved from the file; means for limiting the amount of data retrieved from the file in accordance with the credit signal; and means for recording the amount of data retrieved from the file. The system may further include means for reporting the recorded amount of data retrieved from the file; and means for authenticating such report." Katznelson at 1:13-26.
- " The invention is in the field of data processing, especially in connection with a software copy protection mechanism. That mechanism restricts software, distributed on a magnetic disk or other medium, for use on any computer which is associated with an authorized, physically secure coprocessor where the mechanism does not interfere with the user create of 'backup' copies, but the protection is not compromised by any such 'backup' copies." Comerford at 1:4-13.

Here, regarding the '304, '157, and '158 Patent, market forces demanded software and hardware remedies for data protection. Thus, one of skill in the art would have been motivated to combine or modify references using known methods that one of skill in the art would have recognized as offering improvements to solutions of that time. The references identified describe methods that were known to offer improvements, and, accordingly, one of skill in the art would have been motivated to combine or modify combined references to include such improvements.

(2) Combination of Known Elements Yields Predictable Results

Because the Asserted Claims of the '304, '157, and '158 Patents simply arrange old elements known in the field of data protection, with each performing the same function it had been

known to perform, and yields no more than what one would expect from such an arrangement, the claims are obvious. At the time of the alleged invention of the '304, '157, and '158 Patents, there were a finite number of predictable solutions for data protection, including the use of encryption, keys, and authorization, and therefore a person of ordinary skill in the art had good reason to pursue and/or combine known options and related applications.

Moreover, the alleged inventions of the '304, '157, and '158 Patents are built upon technology that significantly pre-dates the alleged conception date. Sending content and information related to its use had been well-known for years. For example, rights-to-execute that control access to content were broadly known. *See* ABYSS 1987, Comerford.

In addition, cryptography and the use of a series of keys to secure content were well-known in the art. Applicant's own Admitted Prior Art includes three patents assigned to Intel[8] that describe cryptographic systems in the "Background of the Invention." *See, e.g.*, U.S. 5,539,828 at 1:26-37. These systems transmit encrypted information that is decrypted at the receiver. *Id.* The '828 Patent discloses a semiconductor device that stores cryptographic keys and digital certificate(s) to ensure the origin of a hardware agent. *See, e.g.*, '828 Patent at Abstract, 6:39-67. The keys and certificate are stored in non-volatile memory on the hardware agent. *Id*. at 5:41-43. Each hardware agent stores a unique, device-specific public/private key pair. '828 Patent at 5:33 37, 6:8-17. The key pair may be generated, for example, based on a random number generator. *Id*. at 6:8-17. The public key is "digitally signed" (i.e., encrypted) with the manufacturer's private key, creating a digital certificate. *Id*. at 6:29-33. A remote device is thereafter able to use the digital certificate to verify that the hardware agent was made by a specific manufacturer, thereby authenticating it. *Id*. at 6:64-67.

[8] U.S. Pat. Nos. 5,539,828, 5,473,692 and 5,568,552. *See* '304 Patent at 1:12-13.

Motivation to combine these known elements exists because the identified patents and articles all are commonly related and are from the same field of art, and a person of ordinary skill in the art would draw equally from the field of art to solve the problem allegedly presented in the '304, '157, and '158 Patents. The suggested combinations reflect at least combinations of prior art elements according to known methods to yield predictable results, simple substitutions of known elements to obtain predictable results, and combinations that are obvious to try. Further elaboration and information shall be provided with Defendants' expert reports.

(3) Exemplary prior art combinations

As discussed above, Appendices B, G, and H set out the references that disclose each element of the Asserted Claims of the '304 Patent, '157 Patent, and '158 Patent, and Defendants contend that it would have been obvious to modify such references to include any allegedly missing element(s), in view of the knowledge of one of ordinary skill in the art, the admitted prior art of the '304, '157, and '158 Patents, and/or in combination with any of the other prior art references identified in the '304, '157, and '158 Patents. By way of example, and without limitation, Defendants provide the following exemplary combinations for particular claim limitations based on teachings of the cited prior art references. Defendants reserve the right to rely upon any combination of prior art references whether listed herein or otherwise.

Claims [304.24b], [158.4c], [157.53e], [157.69b], [157,69e], [157.70], [157.71], [157.72] [157.84a] [157.86b], [157.99a] – Separately Receiving Content and Rule/Control Information/Digital Object

The above-identified claims of the '304, '157, and '158 Patents include elements directed to separately receiving content and information related to the use of that content. Specifically, the above-identified claims recite:

- "receiving a first entity's control information separately from the digital file;" (304.24b);

- "receiving, at the electronic appliance, independently from the electronic content item via separate delivery and protected separately from the electronic content item, a rule specifying one or more permitted uses of the electronic content item;" (158.4c);
- "(b) one or more electronic objects received by the electronic appliance separately from the piece of electronic content and via separate delivery, the one or more electronic objects specifying one or more permitted or prohibited uses of the piece of electronic content; and" (157.53e);
- "receiving, by the electronic appliance, separately from the first piece of electronic content, a first key, the first key being associated with the first piece of electronic content, and the first key being encrypted at least in part;" (157.69b);
- "receiving, by the electronic appliance, separately from the first piece of electronic content, and via separate delivery, a first electronic object, the first electronic object specifying one or more permitted or prohibited uses of the first piece of electronic content;" (157.69e);
- "The method of claim 69, in which the first key is received at a first time and the first piece of electronic content is received at a second time that is different from the first time." (157.70);
- "The method of claim 69, in which the first key is received over a first path and the first piece of electronic content is received over a second path that is different from the first path." (157.71);
- "The method of claim 69, in which the first key is received from a first entity and the first piece of electronic content is received from a second entity that is different from the first entity." (157.72);

- "The method of claim 69, further comprising: receiving, separately from the first piece of electronic content and the first electronic object, a second piece of electronic content;" (157.84a);
- "receiving, by the electronic appliance, separately from the first piece of electronic content, and via separate delivery, a first electronic object, the first electronic object specifying one or more permitted or prohibited uses of the first piece of electronic content;" (157.86b);
- "The method of claim 86, further comprising: receiving, separately from the first piece of electronic content and the first electronic object, a second piece of electronic content;" (157.99a).

These claims all require that content and information related to the use of that content—"control information" ('304 Patent), "rule" ('158 Patent), or "electronic object" ('157 Patent)—are "receiv[ed] . . . separately." The similarity of these elements means a person of ordinary skill in the art would be similarly motivated to combine the prior art identified in Appendices B, G, and H to result in "receiving…separately" the content and the information related to its use, as explained below.

To the extent a reference does not expressly or inherently disclose separately receiving electronic content and a rule/control information/digital object, this limitation is rendered obvious by the teaching of, at least, ABYSS 1987. ABYSS 1987 teaches that:

> Separating the software from its Right-to-Execute permits a large variety of distribution channels to be used for either. Many electronic distribution methods are not employed today because of the difficulty of preventing illicit interception of the applications. ABYSS can protect all of these distribution channels.

ABYSS 1987 at 50.

Likewise, ABYSS 1987 discloses:

> Optical disks and compact disks have been suggested as possible distribution media for software. Ironically, one of their disadvantages is that they are capable of storing so many applications on a single disk, that it is difficult to market the entire set of applications together. With ABYSS, it is possible to sell a disk containing hundreds of protected applications at a very low price, and sell individual Rights-To-Execute separately. Similarly, it is possible to transmit a large collection of applications on FM radio bands, or on a cable television network, and sell their Rights-To-Execute separately. This enables very inexpensive distribution channels, while retaining their protection.

Id.

Additional references also provide separately receiving content and information related to its use in the context of data protection, including:

- "The basic copy protection mechanism is described in copending application [YO985-091]; this mechanism separates the software which is to be protected from the right to execute that software. Comerford at 1:19-24.

- "Preferably however, secure memory 720 and 707 store authorization information (i.e.,-credits) for pay-per-view programming, and the security modules forward actual pay-per-view data via the telephone controller/modem 875 at a later time." Gammie at 19:34-39.

- "When the rental software is transmitted by the host computer 12 over the telephone network 26, the encrypted key module and the associated OSP module are transmitted as well. Alternatively, the encrypted module, the OSP software and the unencrypted remainder of the rental software may be sent to the customer on floppy disks or magnetic tape by mail or other delivery service. When downloaded from the host computer 12 or loaded from media otherwise provided by a software rental service, the entire rental software package (including the encrypted key module and OSP module) is stored in a peripheral storage device (e.g., hard disk or floppy disk) associated with the target computer 14." Hornbuckle at 11:57-12:2.

- "The registration system assembles the tamperproof overlay file and the decryption key into a single shipping file 38 for transmission to the registration shell of the personal computer. Update main program files may also be included into the shipping file which is transmitted to the registration system of the PC by means of file transfer programs and the previously established data link." Waite at 8:20-26.

Accordingly, separately receiving electronic content and information related to the use of that content was well-known in the art, and it would have been obvious to one skilled in the art at

the time of the alleged invention of the ’304, ’157, and ’158 Patents to include such functionality for the reasons discussed above including, for example, that doing so would be applying a known technique to other electronic distribution systems to achieve the same result.

Claims [304.24c], [158.4e], [158.4f], [157,69d], [157.69g], [157.87c], [157.74], [157.81], [157.86d], [157.89], [157.96] [157.84c], [157.99c] – Information to Govern, at Least in Part, a Use/Determining/Decrypting/Selectively Granting the Request

The above-identified claims of the ’304, ’157, and ’158 Patents include elements directed to information to govern, at least in part, a use, determining, decrypting, and selectively granting the request to use content. Specifically, the above-identified claims recite:

- “using the first entity’s control information to govern, at least in part, a use of the digital file at the computing system; and” (304.24c);
- “determining that the requested use of the electronic content item corresponds to a permitted use of the electronic content item specified in the rule; and” (158.4e);
- “using, at least in part, a decryption key to decrypt the electronic content item, the decryption key being stored in a secure processing unit contained in the electronic appliance.” (158.4f);
- “decrypting, by the electronic appliance, the first piece of electronic content using, at least in part, the first key;” (157.69d);
- “selectively granting, by the electronic appliance, the request in accordance with the first electronic object.” (157.69g);
- “wherein selectively granting the request includes decrypting the first piece of electronic content using the first key.” (157.87c);

- "The method of claim 69, in which selectively granting the request in accordance with the first electronic object includes decrypting the first piece of electronic content using, at least in part, the first key." (157.74);
- "The method of claim 80, in which the at least one condition comprises an indication that the permitted use may be made only for a certain time period, and in which selectively granting the request comprises determining the at least one condition is satisfied." (157.81);
- "selectively granting, by the electronic appliance, the request in accordance with the first electronic object;" (157.86d);
- "The method of claim 86, wherein selectively granting the request includes accessing information stored in internal memory of a secure processing unit running on the electronic appliance." (157.89)
- "The method of claim 95, in which the at least one condition comprises an indication that the permitted use may be made only for a certain time period, and in which selectively granting the request comprises determining that the at least one condition is satisfied." (157.96);
- "selectively granting the request in accordance with the first electronic object." (157.84c);
- "selectively granting the request in accordance with the first electronic object." (157.99c).

The claims all require "information to govern, at least in part, a use of the digital file" ('304 Patent), "determining that the requested use of the electronic content item corresponds to a permitted use of the electronic content" ('158 Patent), "decrypting, by the electronic appliance, the first piece of electronic content using" (''157 Patent), and "selectively granting, by the electronic appliance, the request in accordance with the first electronic object" (''157 Patent) related to the use of content. The similarity of these elements means a person of ordinary skill in the art would

be similarly motivated to combine the prior art identified in Appendices B, G, and H to result in allowing viewers to access protected electronic content, as explained below.

To the extent a reference does not expressly or inherently disclose information to govern, at least in part, a use/determining/decrypting/selectively granting the request, this limitation is rendered obvious by the teaching of, at least, Saito. Saito teaches that:

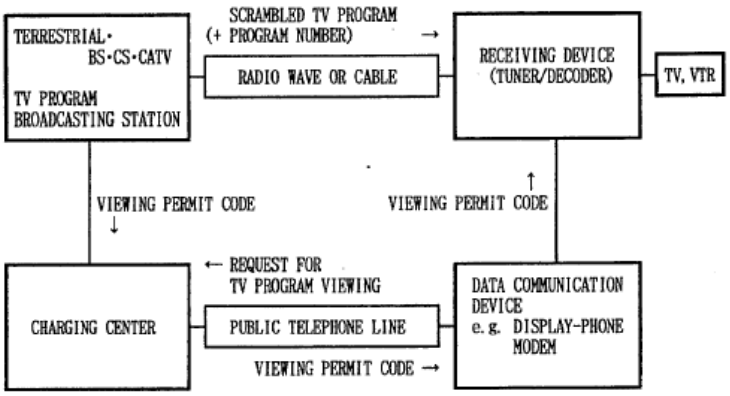
> Upon receipt of the viewing permit code, the satellite broadcasting tuner/decoder 15, CATV adapter/decoder 23 or multiplex teletext adapter 34 descrambles the program, to which an identifying information corresponding to the viewer permit code had been given, and a television signal is sent to a television set 16 or 24 or teletext signal is sent to display devices 35,35,35,....Thus, the viewable picture is displayed on the television set 16 or 24, and the character signal is displayed on the display devices 35, 35, 35, ...

Saito at 3:29-37.

Likewise, Saito discloses:

> When the viewer makes a request for viewing a television program to the charging center via a public telephone line using the data communication device, the charging center sends the viewing permit code, which has been sent from the broadcasting station before the program is broadcast, to the data communication device. The viewing permit code sent to the data communication device is sent to the receiving device. The program is descrambled according to the viewing permit code by the receiving device when the desired broadcasting program is broadcast, and the desired program is displayed or recorded when the receiving device outputs the program to a television set (TV) or to a video tape recorder (VTR). (*see also* FIG.2)

Fig. 2



Id.

Additional references provide solutions in the context data protection including:

- "Once a Right-To-Execute is installed on a protected processor, it may be used at any time to enable the execution of applications associated with it. This is done as follows:

  1. The protected processor obtains reference information, which allows it to locate the Right-To-Execute to be used.

  2. Once found, the protected processor checks that this Right-To-Execute may be used to execute application programs. Assuming that it is, selected parts of the Right-To-Execute may be made available for reading, and modification, by the application to be loaded.

  3. *U* is loaded into the unprotected memory area, and $E_A(P)$ is loaded into the protected memory area and decrypted. If the decryption of $E_A(P)$ yields a valid message authentication or manipulation detection code, execution of *U* and *P* is begun. If not, *P* is purged from protected memory.

  4. At any time during execution, including at the very start, the protected part of the application may be allowed to access (and perhaps modify) selected parts of its own Right-To-Execute. It may use this in conjunction with the real-time clock in the protected processor, for instance, to verify that it is not being executed after its expiration date. Should the protected part of the application find that it is being executed contrary to the terms and conditions specified in its Right-To-Execute, it may effectively terminate its own execution." ABYSS 1987 at 44-45.

- "Thus, incorporating the conditions of the right to execute within the protected software results in securing these conditions against alteration by the user or anyone else unless

authorized by the software vendor. In order to save (for testing) the conditions which are tested against the programmed criteria, we use some storage space in the non volatile memory of the coprocessor; this storage space has already allocated to it the function of storing the decryption key necessary to decrypt the encrypted software. Thus the storage space allocated to a particular protected piece of software is expanded to include the condition which can be measured against the criteria. Because of the non-volatility of the memory, so long as the right to execute is available in the coprocessor, the objective conditions are also available." Comerford at 3:54-4:12.

- "The decrypted and stored data is used by the conditional access software or program authorization software contained within the security module to determine whether a particular program is to be decrypted depending upon a subscriber's tier, pay-per-view account, etc." Gammie at 14:19-24.

- "However, in a manner transparent to the user, when the key module of the software package is retrieved from the peripheral storage device of target computer 14, the OSP software module is activated. The OSP module fetches the encrypted version of the key module from the peripheral storage device (not shown) and sends it to the RCM 18 for decryption by the encryption/decryption module 70. After decryption, the key module is sent back to the target computer 14 and loaded into its internal memory (RAM) for execution. At the latter step the OSP module also initiates a timer controlled by the RTC 56 to begin recording the actual use time of the rental program for computation of rental time charges." Hornbuckle at 12:64-13:9.

- "The addressed packet data supplied to RAM 124 by MATS 122 is supplied at 172 to microprocessor 114. As mentioned above, the user address portion of the addressed packet, which is noted above is transmitted in clear text, is compared by MATS 122 to a decoder identification number, stored therein at manufacture as indicated at 175. If the numbers match, such that the addressed packet is appropriate for processing by the particular decoder, the remainder of the addressed packet is supplied to microprocessor 114 as indicated at 172 and decrypted at 176 using a secret serial number which is stored in the electrically erasable programmable read only memory (EEPROM) 116 at manufacture of the device, as indicated at 180." Smith at 29:19-32.

- "Upon determining that the status of the customer account associated with the customer terminal 11 warrants authorizing retrieval of data from the file identified in the file use request signal 12, the authorization terminal 10 authorizes the customer terminal 11 to retrieve data from said file by providing to the customer terminal 11 both and [sic] encrypted file key 13 and an authenticated credit data signal 14. The credit data signal 14 indicates an amount of credit to be extended to the customer terminal 11 for retrieval of data from the file identified in the file use request signal 12." Katznelson at 2:27-38..

Accordingly, governing, determining, decrypting, and selectively granting access to protected information was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged invention of the alleged invention of the '304 , '157, and '158

Patents to include such functionality in combination for the reasons discussed above including, for example, that doing so would be applying a known technique to other electronic content distribution systems to achieve the same result.

Claim [304.24d] – Reporting Information Relating to the Use of the Digital File to the First Entity

To the extent a reference does not expressly or inherently disclose reporting information relating to the use of the digital file to the first entity, this limitation is rendered obvious by the teaching of at least Hornbuckle. Hornbuckle teaches that "time and billing data are provided to the host computer 12 by RCM 18 on command from the host computer 12." Hornbuckle at 6:27-29. Such usage information is uploaded to the host computer. *Id.* at 3:31-36. As can be seen at *id.* at 3:50-55, this upload occurs via a link between the host computer and the target computer:

> With the features listed above, the proposed system provides for error-free transmission of programs or other data between a host computer and a target computer, and for the secure transmission, reception and usage of programs or other data transferred between the host computer and the target computer.

Such two-way communication links or reporting functionalities are disclosed throughout the prior art. For example:

- "It may be useful to allow other applications to report certain information about the Right-To-Execute. For instance, a utility could summarize information about all Rights-To-Execute owned by a user." ABYSS 1987 at 40.
- "A usage report 60 indicating the usage history recorded in the use history storage unit 23 is generated for communication to the authorization and key distribution terminal 10 in response to either operation of the keyboard 33 or an interrogation signal 61 received from the authorization and key distribution terminal 10." Katznelson at 4:65-5:2.
- "The telephone controller 875 can be programmed to call the headend at a predetermined time or at a predetermined time interval, or upon receiving a signal from the headend preferably when phone usage is at a minimum (i.e.—early morning hours). The telephone controller can call the headend via a toll free 1-800 number, a so-called "watts" lie, or via

a local call to a commercial data link such as TYMNET or TELENET. Once the call is connected and communications established, the decoder 806 uploads to the headend a record of pay-per-view usage encrypted with the secret telephone STN_1." Gammie at 20:1-12.

- "When this key is pressed, the registration file is closed and a registration shell file transfer program 26 establishes a data link with the registration system file transfer program 32. The registration program 40 in the registration computer is protected by a validation means 42 to perform a security check ensuring that the data link has been established with a legitimate registration shell. The registration shell then transmits the registration request file 25 to the registration system which would receive the file, and perform the necessary error checking and hand-shaking operation between linked file transfer programs 26 and 32." Waite at 7:20-31.

Accordingly, reporting information relating to the use of the digital file to the first entity was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged invention of the '304 Patent to include such functionality in combinations for the reasons discussed above.

Claim [304.24p] – Method for Monitoring Use of a Digital File at a Computing System

To the extent a reference does not expressly or inherently disclose claim 304.24p, "[a] method for monitoring use of a digital file at a computing system," this limitation is rendered obvious by the teaching of at least ABYSS 1987. ABYSS 1987 teaches

> [] an environment where a large number of workstations are connected to a network, such as a local area network with a file server, significant economies can be achieved for widely used applications. A single copy of an application can be kept on a file server. The protected processor associated with this server can store a Right-To-Execute which enables up to some fixed number of copies to execute, for instance. When a user requests the application, a single Right-To-Execute is also transferred to the workstation, and the server's count is decremented. The transferred Right-To-Execute may require renewal every minute or so to continue to be valid. The workstation can request renewal of the Right-To-Execute from the server at any time, and thus continue to possess a valid Right-To-Execute as long as is necessary. If the workstation does not check back with the server, the server knows that the workstation's Right-To-Execute has expired, so the server can

> increment its count of Rights-To-Execute for that application. The software lending library is much like a lending library for books, in which the books automatically reappear in the library when they are due.

Id. at 49. As can be seen at *id.* at Abstract,

> ABYSS (A Basic Yorktown Security System) is an architecture for the trusted execution of application software. It supports a uniform security service across the range of computing systems. The use of ABYSS discussed in this paper is oriented towards solving the software protection problem, especially in the lower end of the market. Both current and planned software distribution channels are supportable by the architecture, and the system is nearly transparent to legitimate users. A novel use-once authorization mechanism, called a token, is introduced as a solution to the problem of providing authorizations without direct communication. Software vendors may use the system to obtain technical enforcement of virtually any terms and conditions of the sale of their software, including such things as rental software. Software may be transferred between systems, and backed up to guard against loss in case of failure. We discuss the problem of protecting software on these systems, and offer guidelines to its solution. ABYSS is shown to be a general security base, in which many security applications may execute.

Such monitoring functionalities are disclosed throughout the prior art. For example:

- "The present invention relates to remotely controlling and monitoring the use of computer software. More particularly, this invention relates to a system for renting computer software products while 1) deriving customer use and billing information; 2) preventing unauthorized copying and use; 3) maintaining the integrity of the rented software product (hereafter also "package"); and 4) controlling related voice, program and data communications between the host and user's computers." Hornbuckle at 1:15-23.

- "A system for controlling and accounting for retrieval of data from a CD-ROM memory containing encrypted data files from which retrieval must be authorized." Katznelson at Abstract.

- "A process and system for activating various programs are provided in a personal computer (10), The personal computer (10) is initially provided with a registration shell program (11). A data link (30) is established between the personal computer (10) and a registration computer (12). By providing the registration computer (12) with various information, a potential licensee can register to utilize the main program (16). Once the registration process is complete, a tamperproof overlay program is constructed at the registration

computer (12) and transferred to the personal computer (10). The tamperproof overlay includes critical portions of the main program (16), without which the main program (16) would not operate and also contains licensee identification and license control data." Waite at Abstract.

- "To solve the above problems, the present inventors have filed Japanese Patent Application No. 4-199942, which discloses a charging system, whereby a charging center sends a viewing permit code for viewing a pay program to a data communication device in response to a request for viewing the pay program and a request for distribution of a broadcasting program, which are executed from a pay-per program viewer via a public telephone line using a data communication device. The charging center also collects a fee for such program, and a receiving device displays a pay program according to the viewing permit code when it accepts the viewing permit code." Saito at 2:10-21.

Accordingly, a method for monitoring a digital file was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged invention of the '304 Patent to include such functionality in combinations for the reasons discussed above.

Claims [304.24a], and [157.53d] – Digital File/Electronic Content

The above-identified claims recite:

- "receiving a digital file;" (304.24a);
- "(a) a piece of electronic content;" (157.53d).

To the extent a reference does not expressly or inherently disclose receiving a digital file or electronic content, this limitation is rendered obvious by the teaching of, at least, ABYSS 1987. ABYSS 1987 teaches that "[t]he [software] application package contains documentation (hopefully!), a floppy diskette, and a token card." ABYSS 1987 at 42. ABYSS 1987 discloses that "[t]he user makes the token and distribution diskette available to the protected processor." *Id.* at 44. As can be seen at *id.*,

> **Shipping the Protected Software**
>
> The above components can now be distributed. The unprotected part of the software *U*, the protected part $E_A(P)$, the Right-to-Execute $E_S(RTE_A)$, and the encrypted token data $E_A(T_J)$ can be

> distributed by any means. The token data T_J, which is plaintext, must be kept physically secure, for example in a token.
>
> A typical means of distributing these components would be to package *U*, $E_A(P)$, and $E_S(RTE_A)$ on a floppy diskette. This diskette could be bulk-reproduced, since every such diskette can be identical. Tokens can be designed so that T_J and $E_A(T_J)$ can be placed inside of a token. The diskette and token can be packaged together or separately, and shipped to retailers.

Such functionalities are disclosed throughout the prior art. For example:

- "In the software rental system of the present invention, a control module is installed on or in cooperation with the customer's computer (hereafter also target computer), and the customer pays for services, i.e., the use of the software, received." Hornbuckle at 2:54-58.

- "A system for controlling and accounting for retrieval of data from a CD-ROM memory containing encrypted data files from which retrieval must be authorized." Katznelson at Abstract.

- "In one embodiment, a particular program which is complete except for an operational executive control loop is initially provided in a personal computer or other device on a magnetic disc, firmware, hardware, or other means. Additionally, a registration shell program is also included with the particular program. However, in the case of small or extremely valuable program, the entire program may be missing and only the shell provided. Due to the exclusion of the executive control loop, the program would not operate without the implementation of the proper registration process. As shown in FIGS. I and III, this registration process is initiated utilizing a registration shell program 11 in the personal computer (PC) 10 as well as a registration program 40 provided in a registration computer 12. A registration system program is provided in the registration computer 12 and is accessible to the registration shell program 11 by an electronic data link 30. The electronic data link may be a local area network, a telephone modem link, or any other type." Waite at 6:13-30.

- "In this way, for example, a video message can be sent at night, when transmission time is relatively inexpensive, and stored automatically for viewing when convenient the following day." Smith at 11:59-64.

Accordingly, receiving a digital file or electronic content would have been obvious to one skilled in the art at the time of the alleged invention of the '304 and '157 Patents to include such functionality in combinations for the reasons discussed above.

Claims [304.24e], and [157.86e] – Impede Tampering

The above-identified claims recite:

- "wherein at least one aspect of the computing system is designed to impede the ability of a user of the computing system to tamper with at least one aspect of the computing system's performance of one or more of said using and reporting steps." (304.24e);

- "wherein the electronic appliance comprises hardware and/or software operable to impede the user from tampering with performance of said selectively granting step." (157.86e)

To the extent a reference does not expressly or inherently disclose impeding tampering of the system by users, this limitation is rendered obvious by the teaching of, at least, ABYSS 1987. ABYSS 1987 teaches a "architecture [that] provides the software vendor with tools to enforce the conditions under which the application may be used." ABYSS 1987 at 39. ABYSS 1987 discloses a "[s]oftware run under ABYSS [that] executes exactly as it was written, and cannot be modified arbitrarily by the user." *Id.* at 39. As can be seen at *id.* at 39,

> The protected processor is a logically, physically, and procedurally secure unit. It is logically secure, in that an application cannot directly access the supervisor process, or the protected part of any other application, to violate their protection. It is physically secure (which is indicated by the heavy box in Figure 1), in that it is contained in a tamper-resistant package [Wein86] [Chau84] [Pric86]. It is procedurally secure in that the services which move information, and Rights-To-Execute in particular, into and out of the protected processor cannot be used to subvert the protection.

Such functionalities are disclosed throughout the prior art. For example:

- "The tamperproof overlay is the key device that prevents license abuse after activation because the executive control loop program instructions may not be separated from the unique licensee identification data and license control data without detection, nor may the licensee identification and license control data be changed without detection.
  The tamperproof overlay file is considered to be made tamperproof by initially storing a cyclic redundancy check value within the overlay file when the overlay file is generated. The cyclic redundancy check value is computed for the entire contents of the overlay file including program instruction and licensee data. Since licensee data is unique, each CRC

will be unique. The stored CRC value is compared to the cyclic redundancy check value computed by the loader segment each time the overlay is loaded. If the cyclic redundancy check values do not agree, the loader segment will exit to the operating system. Thus, any change to the overlay file contents renders the overlay file defunct, unless a corresponding change the stored cyclic redundancy check value is also made. Secondly, the entire contents of the tamperproof overlay are encrypted by the registration system in such a manner as to obscure the location of the cyclic redundancy check value, thus making it difficult to locate and change its value." Waite at 10:12-34.

- "In accordance with the present invention, microprocessor 50 in RCM 18 is programmed to destroy an encryption key if: (1) the RCM 18 is physically tampered with; (2) the telephone number of the target computer 14 is changed without notice or the telephone is disconnected for longer than a preselected period of time (in this case, destruction of the protection key takes place only after power is restored). If the encryption key is destroyed by the RCM 18, RCM 18 will attempt to notify the user by using a special alarm, such as a beeping sound or LED display." Hornbuckle at 14:1-11.

- "If the KOM was not twice encrypted with an alternate SSN, then a pirate could alter destination and encryption bits 9b and 9c to transmit a decrypted KOM between security modules, and thus intercept is during transmission. By using the alternate SSN, if tampering of destination and encryption bits occur, the internal security module would believe the encrypted KOM were encrypted using the regular SSN, and thus could not decrypt the KOM. Only partially decrypted KOM's are passed between modules and only in the double encryption state. The present system prohibits the use of exchanging external security modules between decoders since both SSNs must correspond with a twice encrypted KOM." Gammie at 16:55-68.

- "These objectives must be met in a way which is secure against attempts of the user, or anyone else not specifically authorized by the software vendor to either vary the conditions or the objective criteria under which the conditions are met. In accordance with the invention, the criteria are stated in software, and more particularly, in the protected or encrypted portion of the application soft- ware. As is described in our copending application [YO985-091], the only form in which the protected application software is available to the user is in encrypted form; because the user does not have access to the decryption key as a data object, he is unable to modify, or even read the protected software. Thus, incorporating the conditions of the right to execute within the protected software results in securing these conditions against alteration by the user or anyone else unless authorized by the software vendor." Comerford at 3:40-58.

- "In the preferred embodiment, the microprocessor 114 is a "secure" microprocessor, meaning that it cannot be tampered with or its software read out or altered without destroying it, and the EEPROM 116 is comprised therein. As indicated at 120, the decoder then "grabs" the indicated page when the teletext header including the appropriate page number is received by "grabbing" the teletext lines which follow the teletext header thus identified." Smith at 18:49-59.

- "The Controller 48 is coupled to an output channel 29 for outputting re-encrypted controlled information. Preferably, the various channels coupled to the controllers 48 are tamper-proof. This will make it impossible for users to tap into the clear channel 47, to access the controller 48, to alter the value of the memory storage 52, or to change the value of the clock 55." Chorley at 8:51-59.

- "The Controller 48 is coupled to an output channel 29 for outputting re-encrypted controlled information. Preferably, the various channels coupled to the controllers 48 are tamper-proof. This will make it impossible for users to tap into the clear channel 47, to access the controller 48, to alter the value of the memory storage 52, or to change the value of the clock 55." Narasimhalu at 8:51-59.

Accordingly, impeding user tampering at the system would have been obvious to one skilled in the art at the time of the alleged invention of the '304 and '157 Patents to include such functionality in combinations for the reasons discussed above.

Claims [158.4b] and [157.89] – Storing the Electronic Content Item in Memory of the Electronic Appliance

The above-identified claims recite:

- "storing the electronic content item in memory of the electronic appliance;" (158.4b);

- "The method of claim 86, wherein selectively granting the request includes accessing information stored in internal memory of a secure processing unit running on the electronic appliance." (157.89)

To the extent a reference does not expressly or inherently disclose storing the electronic content item in memory of the electronic appliance, this limitation is rendered obvious by the teaching of, at least, ABYSS 1987. ABYSS 1987 teaches that "[f]iles containing the software may be stored on the user's hard disk, on network file servers, or on a mainframe, and may be backed up at will." ABYSS 1987 at 50. ABYSS 1987 discloses a "protected processor [which] constitutes a minimal, but complete, computing system." *Id.* at 39. As can be seen at *id.* at 39, this computing system

> … contains a processor, a real-time clock, a random or pseudo-random number generator, and sufficient memory to store protected

> parts of applications while they execute. It also contains secure memory for storage of Rights-To-Execute. This storage retains its contents even when the system is power off.

Such storage and memory functionalities are disclosed throughout the prior art. For example:

- "It may be useful to allow other applications to report certain information about the Right-To-Execute. For instance, a utility could summarize information about all Rights-To-Execute owned by a user." ABYSS 1987 at 40.

- "With access to the software decryption key AK, the protected application file B can be decrypted and stored in the temporary memory 26 of the coprocessor 20 so that it may be executed by the coprocessor 20. Because of its physical and logical security, the plain text form, in which application file B is stored in temporary memory 26 during the course of execution and is not available to the user or a pirate." Comerford at 23:16-25.

- "When downloaded from the host computer 12 or loaded from media otherwise provided by a software rental service, the entire rental software package (including the encrypted key module and OSP module) is stored in a peripheral storage device (e.g., hard disk or floppy disk) associated with the target computer 14." Hornbuckle at 12:49-53.

- "When downloaded from the host computer 12 or loaded from media otherwise provided by a software rental service, the entire rental software package (including the encrypted key module and OSP module) is stored in a peripheral storage device (e.g., hard disk or floppy disk) associated with the target computer 14." Smith at 11:54-63.

- "A read only memory (ROM) 37 containing the encrypted data files is loaded in the customer data retrieval terminal 11." Katznelson at 3:6-8.

- "When the program is not executing, the protected program remains in its encrypted form, in the mass storage of the computer along with the unprotected program files. The protected program is decrypted only when loaded for execution and may not be changed without access to the authentic encryption key." Waite at 4:19-24.

Accordingly, storing electronic content at a receiving appliance would have been obvious to one skilled in the art at the time of the alleged invention of the '157 and '158 Patents to include such functionality in combinations for the reasons discussed above.

Claims [158.4a], [157.69a], and [157.86a]– Electronic Content Item Being Encrypted at Least in Part

The above-identified claims recite:

- "receiving, at the electronic appliance, an electronic content item, the electronic content item being encrypted at least in part;" (158.4a);
- "receiving, by the electronic appliance, a first piece of electronic content, the first piece of electronic content being encrypted at least in part;" (157.69a)
- "receiving, by the electronic appliance, a first piece of electronic content, the first piece of electronic content being encrypted at least in part;" (157.86a);

To the extent a reference does not expressly or inherently disclose an electronic content item being encrypted at least in part, this limitation is rendered obvious by the teaching of, at least, Smith. Smith describes a system in which an "assembled teletext, video, and audio signal is encrypted" and transmitted as "addressed packets" to a decoder. Smith at 9:56-60. Smith discloses:

> As described above, a primary aspect of the communications system described and claimed in the present application is the transmission of individually addressable, encrypted messages from a transmitter to an individual decoder for display to the subscriber.

Smith at 19:60-64.

Further, that reference shows the system receiving encrypted content at receiving antenna 22:

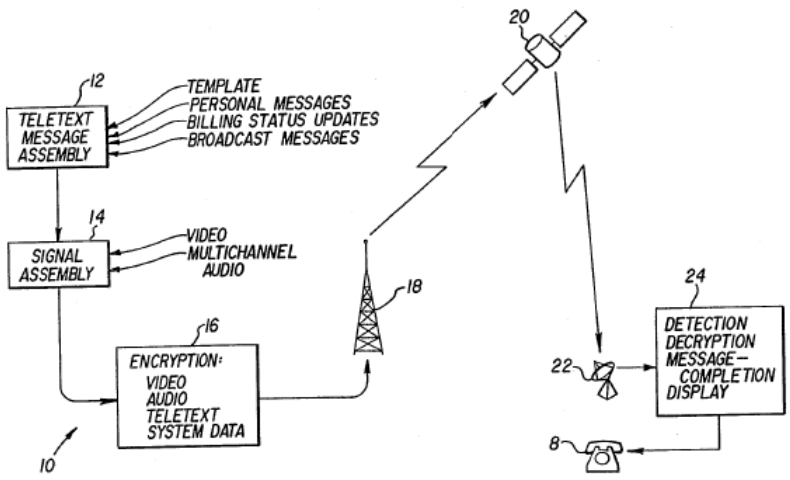


FIG. 1

Smith at Figure 1.

Content being encrypted at least in part is disclosed throughout the prior art. For example:

- "The protected part is encrypted when it is outside the protected processor, and only decrypted when it is loaded into the protected processor. The unprotected part is exposed to view.
  The protected part executes securely on the protected processor, in that it cannot be examined or modified by any party external to the protected processor. It cannot be examined externally while it is available for execution because of the logical and physical security of the processor, which inhibit all external access to the plaintext of the protected part. The encrypted form of the protected part cannot be modified directly because of the cryptographic techniques used to detect if it has been tampered with." ABYSS 1987 at 40.

- "A decoder for descrambling encoded satellite transmissions comprises an internal security module and a replaceable security module. The program signal is scrambled with a key and then the key itself is twice encrypted and multiplexed with the scrambled program signal. The key is first encrypted with a first secret serial number (SSN) which is assigned to a given replaceable security module. The key is then encrypted with a second secret serial number (SSN_2) which is assigned to a given decoder. The decoder performs a first key decryption using the second secret serial number (SSN_2) stored within the decoder. The partially decrypted key is then further decrypted by the replaceable security module using the first secret serial number (SSN_1) stored within the replaceable security module. The decoder then descrambles the program using the twice decrypted key." Gammie at Abstract.

- "At 16, the assembled teletext, video and audio signal is encrypted. The signal transmitted includes what are referred to as addressed packets, which among other functions alert an individual subscriber's decoder that a message has been sent to it, and teletext information." Smith at 19:60-64.

- "The present invention is a method and system for controlling and accounting for retrieval of data from a memory containing an encrypted data file from which retrieval must be authorized." Katznelson at 1:13-16.

Accordingly, the systems disclose content encrypted at least in part, and it would have been obvious to one skilled in the art at the time of the alleged invention of the '157 and '158 Patents to include such functionality in combinations for the reasons discussed above.

Claim [157.53p] – An Electronic Appliance

To the extent a reference does not expressly or inherently disclose claim an electronic appliance for the "controlling usage of pieces of electronic content … with electronic objects," this limitation is rendered obvious by the teaching of at least ABYSS 1987. '157 Patent at Claim 53. ABYSS 1987 teaches "ABYSS (A Basic Yorktown Security System) [which] is an architecture for the trusted execution of application software." ABYSS 1987 at Abstract. ABYSS 1987 produces the architecture in Figure 1 below.

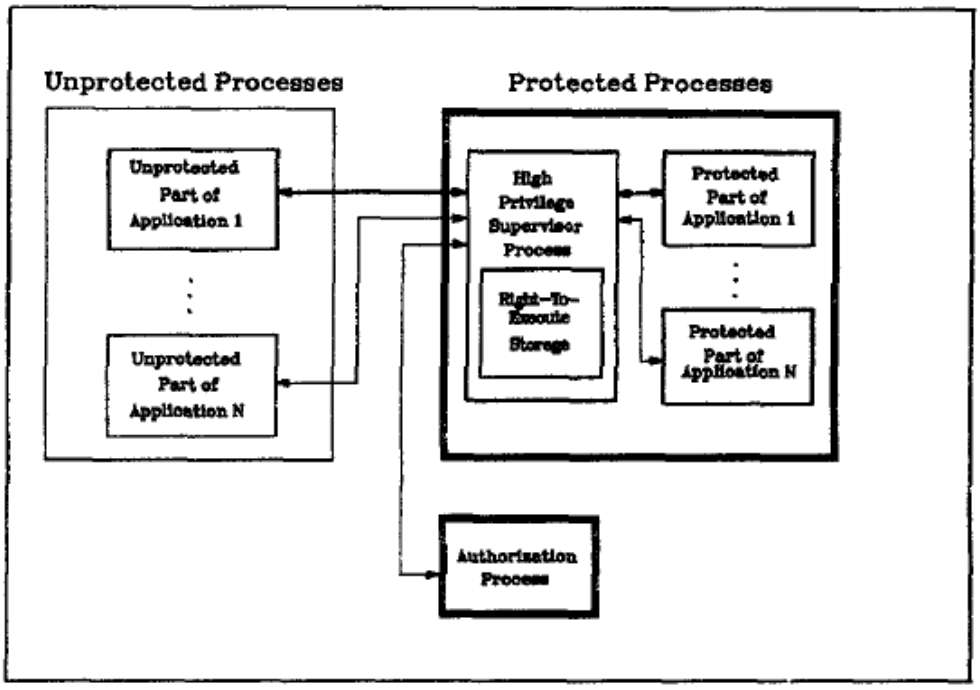


Figure 1. The Architecture of a Protected Processor System

The systems for the control of electronic objects to access electronic content are disclosed throughout the prior art. For example:

- "By means of the present invention, an authorized user at the target computer is able to "download" programs or data, via a telephone line and a programmable remote control module (RCM) connected at each end thereof from a central or host computer. Usage and other accounting data are monitored by the RCM and stored in memory resident therein. At predetermined times, the central or host computer accesses the RCM for the purpose of "uploading" the usage and other accounting data to the central or host computer." Hornbuckle at 3:27-36.

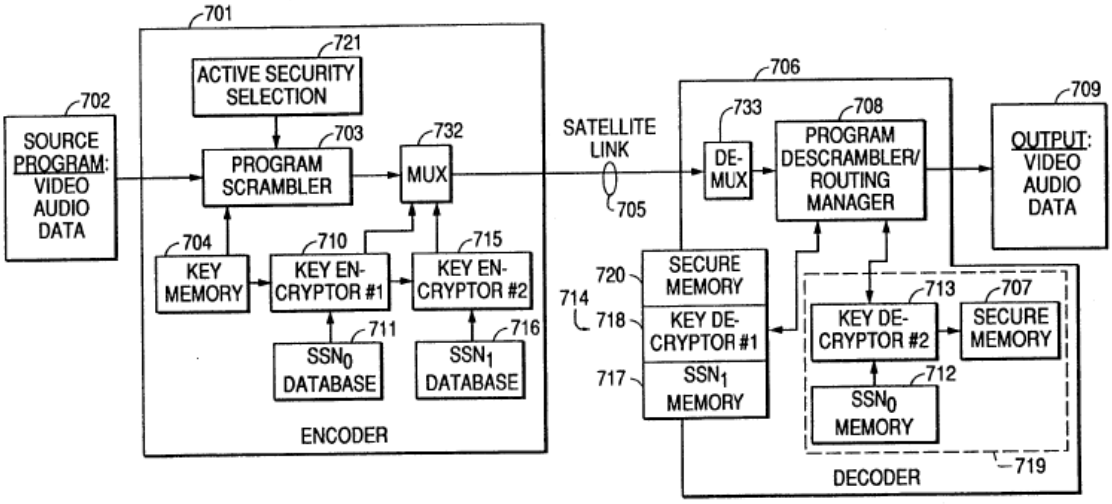
- "A process and system for activating various programs are provided in a personal computer (10), The personal computer (10) is initially provided with a registration shell program (11). A data link (30) is established between the personal computer (10) and a registration computer (12). By providing the registration computer (12) with various information, a potential licensee can register to utilize the main program (16). Once the registration process is complete, a tamperproof overlay program is constructed at the registration computer (12) and transferred to the personal computer (10). The tamperproof overlay includes critical portions of the main program (16), without which the main program (16) would not operate and also contains licensee identification and license control data." Waite at Abstract.

- "It is an object of the present invention to provide a system, by which it is possible to actualize the so-called pay-per program for viewing each program on a pay basis or the so-called pay-per-view for viewing a program on a pay basis without signing a contract, using a charging system. To attain the above system, it is disclosed in the present invention how the scrambled pattern can be protected, how the program to be viewed is identified, how a viewing request should be made, and how these means are applied on a pay broadcasting system." Saito at 5:1-10.

- "As described above, a primary aspect of the communications system described and claimed in the present application is the transmission of individually addressable, encrypted messages from a transmitter to an individual decoder for display to the subscriber." Smith at 19:60-64.

- "FIG. 7 shows the encryption system of the present invention comprising an encoder 701 for encoding a source program 702 for transmission over a satellite link 705 to at least one decoder 766." Gammie at 11:59-62.

FIG. 7



Accordingly, a system for the control of electronic objects to access electronic content was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged invention of the '157 Patent to include such functionality in combinations for the reasons discussed above.

Claims [157.73] and [157.88] – Electronic Content Item Being Non-Executable

The above-identified claims recite:

- "The method of claim 69, in which the first piece of electronic content consists of non-executable audio, video, and/or textual content." (157.73);
- "The method of claim 87, in which the first piece of electronic content comprises non-executable audio, video, and/or textual content." (157.88).

To the extent a reference does not expressly or inherently disclose non-executable electronic content, this limitation is rendered obvious by the teaching of, at least, Smith, which discloses "communication of video, audio, teletext, and data from a central transmitter to groups of decoders." Smith at 1:16-18. Smith expands:

> At 16, the assembled teletext, video and audio signal is encrypted. The signal transmitted includes what are referred to as addressed packets, which among other functions alert an individual subscriber's decoder that a message has been sent to it, and teletext information.

Smith at 19:60-64.

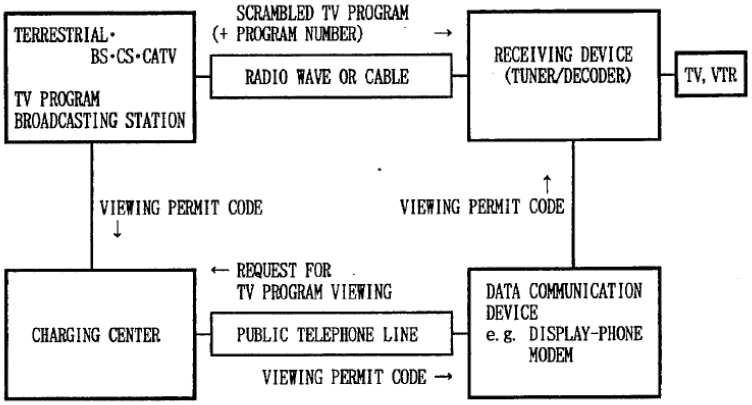
Electronic content that is non-executable is also disclosed in Saito. Saito teaches that a system that sends "a scrambled television program … so that only the subscribed viewers who signed the viewing contract can view the program, and the subscribed viewers receive the program on a pay basis using a tuner/decoder, which can descramble the program." Saito at 1:20-25. Saito further discloses:

> FIG. 2 shows a system for viewing a pay broadcasting program. The broadcasting station sends a viewing permit code for viewing a broadcasting program to a charging center before the program is broadcast, and also sends scrambled broadcasting program, which can be descrambled by the viewing permit code, to the receiving device. In this case, a program number for identifying the broadcasting program can be transmitted with the broadcasting program. When the viewer makes a request for viewing a television

program to the charging center via a public telephone line using the data communication device, the charging center sends the viewing permit code, which has been sent from the broadcasting station before the program is broadcast, to the data communication device.

Saito at 4:13-26.

Fig. 2



Saito at Figure 2.

The identified prior art references disclose that content may be non-executable audio, video, and/or textual content. For example:

- "A decoder for descrambling encoded satellite transmissions comprises an internal security module and a replaceable security module. The program signal is scrambled with a key and then the key itself is twice encrypted and multiplexed with the scrambled program signal. The key is first encrypted with a first secret serial number (SSN) which is assigned to a given replaceable security module. The key is then encrypted with a second secret serial number (SSN_2) which is assigned to a given decoder. The decoder performs a first key decryption using the second secret serial number (SSN_2) stored within the decoder. The partially decrypted key is then further decrypted by the replaceable security module using the first secret serial number (SSN_1) stored within the replaceable security module. The decoder then descrambles the program using the twice decrypted key." Gammie at Abstract.

Accordingly, the prior art discloses non-executable audio, video, and/or textual content, and it would have been obvious to one skilled in the art at the time of the alleged invention of the '157 Patent to include such functionality in combinations for the reasons discussed above.

Claims [157.54] and [157.87a] – First Cryptographic Key/First Key Being Encrypted

The above-identified claims recite:

- "The electronic appliance of claim 53, in which the information comprises a first cryptographic key." (157.54);
- "The method of claim 86, further comprising: receiving a first key, the first key being encrypted; and" (157.87a).

To the extent a reference does not expressly or inherently disclose a cryptographic key or encrypted key, this limitation is rendered obvious by the teaching of, at least, Hornbuckle, which discloses a "data encryption/decryption module 70 of RCM 16 [that] uses an encryption key unique to the individual target computer in which the rental software is to be used." Hornbuckle at 12:4-7. Hornbuckle expands:

> Method of encrypting and decrypting using a encryption key, such as described in U.S. Pat. No. 4,649,233, are well-known. However, since the encryption key is an important element which the software security scheme of the present invention depends, the encryption key itself is always transmitted in encrypted form to RCM 18 (utilizing an encryption key identical to the encryption key provided in RCM 18) to assure proper systems operation and integrity.

Hornbuckle at 12:7-15. Additionally, Hornbuckle states

> The encryption key used in the decryption process is inaccessible to the user. Thus, in accordance with the present invention, a downloaded rental software package will only run on the particular target computer 14 having an encryption key corresponding to the encryption key employed by the host computer 12 when the key module of the rental software package was encrypted. Since the rental software will operate only on a target computer 14 serviced by an RCM 18 utilizing an encryption key unique to the target computer 14 (to decrypt the key module), no other physical or licensing restrictions on the user's ability to make copies of the rental software package are required.

Hornbuckle at 12:36-48.

The identified prior art references disclose cryptographic or encrypted keys. For example:

- "The software vendor encrypts this data under a key *A*, called the *application key*, chosen by the software vendor for a particular application, for form $E_A(T_J)$. The plaintext token data is protected by making the token physically secure against tampering.
  The token can then act as a one-time-only authorization from the software vendor, to a protected processor which possesses the application key *A*. (The means by which the protected processor obtains the application key are discussed later.) To do this, the protected processor reads in and decrypts $E_A(T_J)$ to obtain the token data T_J." ABYSS 1987 at 41.

- "A unique set of encryption and decryption keys is generated and the entire contents of the tamperproof overlay file is encrypted using the encryption key. Based upon the encryption key, a decryption key is provided which is transferred along with the tamperproof overlay file. The encryption algorithm can be any technique which uses a different key for encryption and decryption similar to the public key encryption system. The registration system assembles the tamperproof overlay file and the decryption key into a single shipping file 38 for transmission to the registration shell of the personal computer." Waite at 8:13-23.

- "When installed in the coprocessor, the right-to-execute a particular protected application exists in the form of a software decryption key called an application key (AK). So long as the software decryption key AK is retained in the permanent memory of the coprocessor,, the corresponding protected software can be executed on the composite system including the host and coprocessor." Comerford at 1:29-37.

- "The scrambling process is accomplished via a key which may itself be encrypted. Each subscriber wishing to receive the signal is provided with a decoder having an identification number which is unique to the de coder. The decoder may be individually authorized with a key to descramble the scrambled signal, provided appropriate payments are made for service. Authorization is accomplished by distributing descrambling algorithms which work in combination with the key (and other information) to paying subscribers, and by denying that information to non-subscribers and to all would-be pirates." Gammie at 1:65-2:8.

Accordingly, the prior art discloses a cryptographic or encrypted key, and it would have been obvious to one skilled in the art at the time of the alleged invention of the '157 Patent to include such functionality in combinations for the reasons discussed above.

Claims [158.4f] and [157.57] – Decryption Key Being Stored in Secure Processing/First Cryptographic Key is Stored in the Internal Memory

The above-identified claims recite storing cryptographic keys, which is found throughout the prior art. Specifically, the claims recite:

- "using, at least in part, a decryption key to decrypt the electronic content item, the decryption key being stored in a secure processing unit contained in the electronic appliance." (158.4f);

- "The electronic appliance of claim 56, in which the first cryptographic key is stored in the internal memory of the second processing unit." (157.57).

To the extent a reference does not expressly or inherently disclose keys being stored, this limitation is rendered obvious by the teaching of, at least, Matyas. Matyas teaches that "[t]he cryptographic key storage unit 22 stores the cryptographic key in an encrypted form." Matyas at 6:15-16. Further, Matyas states:

> An example of recovering an encrypted key from the cryptographic key storage 22 occurs when the cryptographic instruction storage 10 receives over the input/output path 8 a cryptographic service request for recovering the cryptographic key from the cryptographic key storage units 22. The control vector checking unit 14 will then output in response thereto, an authorization signal on line 20 to the cryptographic processing unit 16 that the function of recovering the cryptographic key is authorized. The cryptographic processing unit 16 will then operate in response to the authorization signal on line 20, to receive the encrypted form of the cryptographic key from the cryptographic key storage 22 and to decrypt the encrypted form under the storage key which is a logical product of the associated control vector and the master key stored in the master key storage 18.
>
> The storage key is the exclusive-OR product of the associated control vector and the master key stored in the master key storage 18. Although the logical product is an exclusive OR operation in the preferred embodiment, it can also be other types of logical operations. The associated control vector, whose general format is shown in FIG. 5, is stored with the encrypted form of its associated cryptographic key in the cryptographic key storage 22. Since all keys stored on a cryptographic storage are encrypted under the master key, a uniform method for encryption and decryption of encrypted keys thereon can be performed.

Id. at 6:21-49.

Such storage of cryptographic keys is disclosed throughout the prior art. For example:

- "In order to save (for testing) the conditions which are tested against the programmed criteria, we use some storage space in the non volatile memory of the coprocessor; this storage space has already allocated to it the function of storing the decryption key necessary to decrypt the encrypted software." Comerford at 3:58-4:6.

- "The decrypted encryption key is then stored in the RCM memory 52 until decryption of a key module is required. Since the encryption key is retained in memory 52, the encryption key need only be transmitted to RCM 18 one time. If the RCM 18 is tampered with in any manner, the encryption key is destroyed." Hornbuckle at 12:19-25.

- "The supervisor process contains a cryptographic facility for managing encryption/decryption keys. This facility decrypts the protected parts of applications as they are loaded into the protected processor. We place the cryptographic transformation between primary memory (such as RAM) and secondary memory (such as a disk). Best [Best79]-[Best84b] places this transformation between primary memory and the instruction decoder of the processor. Placing it closer to the instruction decoder in the memory hierarchy forces a choice between significant performance degradation of the application, and the use of a cryptosystem with significantly less security than, say, DES.

  Placing the transformation between primary and secondary memory, on the other hand, matches the bandwidth of the cryptographic facility to the data transfer bandwidth, allows efficient pipelining of the data to be decrypted, and allows decrypted instructions to be used numerous times without being decrypted each time. It also allows the efficient use of message authentication or manipulation detection codes on parts of the application." ABYSS 1987 at 40.

Accordingly, a key for electronic content would be stored in secure processing or internal memory, and it would have been obvious to one skilled in the art at the time of the alleged invention of the '157 and '158 Patents to include such functionality in combinations for the reasons discussed above.

Claim [158.4d], [157.69f], [157.75], [157.86c], and [157.90] – Request to Use Content

The above-identified claims recite:

- "receiving, at the electronic appliance, a request to use the electronic content item;" (158.4d);

- "receiving, by the electronic appliance, a request to use the first piece of electronic content; and" (157.69f);

- "The method of claim 69, in which the request comprises a request to view the first piece of electronic content." (157.75);

- "receiving, by the electronic appliance a request from a user of the electronic appliance to use the first piece of electronic content; and" (157.86c);

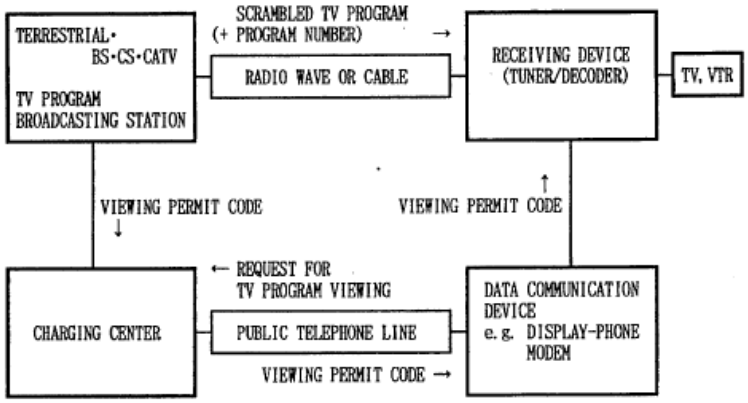
- "The method of claim 86, in which the request comprises a request to view the first piece of electronic content." (157.90).

To the extent a reference does not expressly or inherently disclose a request to use electronic content, this limitation is rendered obvious by the teaching of, at least, Saito. Saito teaches that a "method to request viewing, there are proposed a method to request according to the broadcasting time and a method to request by using an identifying information of the program itself." Saito at 5:34-37. Saito discloses in

> When the viewer makes a request for viewing a television program to the charging center via a public telephone line using the data communication device, the charging center sends the viewing permit code, which has been sent from the broadcasting station before the program is broadcast, to the data communication device. The viewing permit code sent to the data communication device is sent to the receiving device. The program is descrambled according to the viewing permit code by the receiving device when the desired broadcasting program is broadcast, and the desired program is displayed or recorded when the receiving device outputs the program to a television set (TV) or to a video tape recorder (VTR). (*see also* FIG.2)

Saito at 4:13-26.

Fig. 2



Saito at Figure 2.

Requests to use electronic content are disclosed throughout the prior art. For example:

- "A subscriber wishing to view the event must receive authorization in the form of a special descrambler mechanism, or in the form of a special code transmitted or input to the subscriber's decoder. Some pay-per-view television systems allow the subscriber to request a pay-per-view program (i.e.--movies) to watch. The pay television provider then transmits the requested program and authorizes that subscriber's decoder to receive the signal." Gammie at 19:10-18.

- "For purposes of the present invention, rental computer software refers to the service of providing computer software to customers (hereafter also users) on a pay-as-used basis, where the software is executed on the customer's own personal computer." Hornbuckle at 1:24-28.

- "In order to gain authorization to retrieve encrypted data from a given file stored in the memory loaded in the customer data retrieval terminal 11, the customer causes a file use request signal 12 to be communicated to the authorization and key distribution terminal 10. The file use request signal identifies the file for which retrieval authorization is requested and also contains an ID number identifying the customer terminal 11 from which the request signal 12 is sent." Katznelson at 2:7-15.

Accordingly, it would have been obvious to one skilled in the art at the time of the alleged invention of the '157 and '158 Patents to include such functionality in combinations for the reasons discussed above.

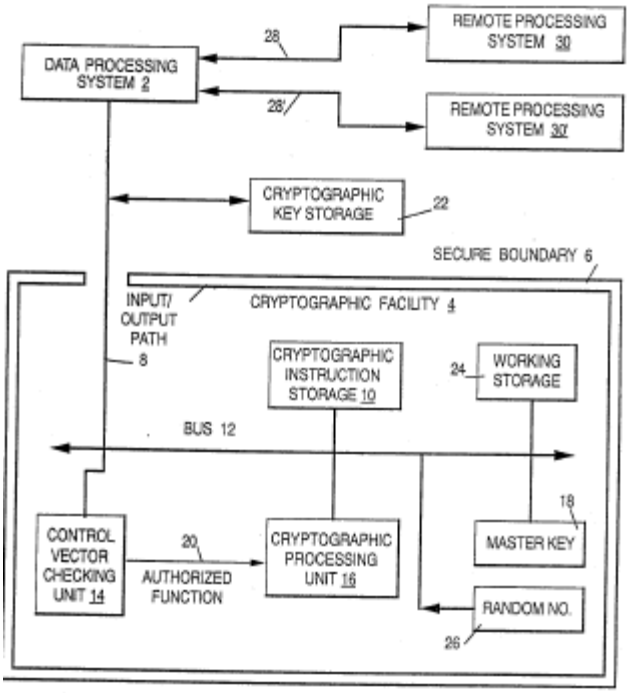
Claims [158.4p], [157.53a], [157.69p], [157.86p] – Processor and a Memory Encoded with Program Instructions

The above-identified claims recite:

- "a first processing unit;" (157.53a);
- "(c) software configured for execution by the first processing unit, the software comprising programming for controlling usage of pieces of electronic content such as the first piece of electronic content in accordance with electronic objects such as the one or more electronic objects, the software further comprising programming for causing the second processing unit to access information required for usage of pieces of electronic content. " (157.53f);
- "A method performed by an electronic appliance comprising a processor and a memory encoded with program instructions that, when executed by the processor, cause the electronic appliance to perform the method, the method comprising:" (157.69p);
- "A method for governing usage of electronic content performed by an electronic appliance, the electronic appliance comprising a processor and a memory encoded with program instructions that, when executed by the processor, cause the electronic appliance to perform the method, the method comprising:" (157.86p);
- "A method utilizing an electronic appliance comprising a processor and a memory encoded with program instructions that, when executed by the processor, cause the processor to perform the method, the method comprising:" (158.4p).

To the extent a reference does not expressly or inherently disclose a processor and a memory encoded with program instructions, this limitation is rendered obvious by the teaching of, at least, Matyas. Matyas teaches that "[t]he system can also employ a memory inside the CF to Store user's programs and a processing engine to execute the programs. An example of this is a program or macro for performing new algorithms for PIN verifications on new PIN formats." Matyas at 7:66-8:3. Matyas discloses in Figure 1

FIG. 1



> a block diagram representation of the data processing system with the cryptographic facility therein. In FIG. 1, the data processing system 2 executes a program such as the crypto facility access programs and the application programs illustrated in FIG. 2. These programs output cryptographic service requests for data cryptography operations using keys which are associated with control vectors. The general format for a control vector is shown in FIG. 5. Control vectors define the function which the associated key is allowed by its originator to perform. The invention herein is an apparatus and a method for validating that data cryptography functions requested for a data set by the program, have been authorized by the originator of the key.
>
> *Id.* at 5:28-42.

Such processing and coding functionalities are disclosed throughout the prior art. For example:

- "Referring again to FIG. 2, RCM 18 contains a program memory 52 and a read/write memory 54. The program memory 52 holds the program instructions

which microprocessor 50 implements in order to accomplish the functions of RCM 18." Hornbuckle at 10:51-55.

- "The encrypted program signal is input to decoder 806 through modem 875 into processor 870." Gammie at 19:63-64.

- "Two important features of 20 the coprocessor 20 are its permanent, non-volatile memory 25 and a temporary memory 26; the latter akin to the working memory (RAM) of a conventional computer. The coprocessor 20 is provided to the user in a form in which it has at least one decryption key CSK stored in the permanent memory 25; the decryption key CSK is provided and stored by the vendor of the coprocessor 20. In order for the user to execute a protected application, he must install a right to execute the application in the permanent memory 25; this right to execute is represented by a software decryption key AK. As described in the application [YO985- 091] the user, in order to install the right-to-execute, receives from the software vendor a distribution set which includes a hardware cartridge 30 and a distribution disk 16." Comerford at 22:19-36.

Accordingly, the systems have processors with executional code, and it would have been obvious to one skilled in the art at the time of the alleged invention of the '157 and '158 Patents to include such functionality in combinations for the reasons discussed above.

Claims [157.53b], [157.53c], and [157.59] – Second Processing Unit/Computer-Readable Medium External to Second Processing Unit

The above-identified claims recite:

- "a second processing unit, the second processing unit comprising a microprocessor, internal memory, and internal memory interface logic for impeding unauthorized access to the internal memory by the first processing unit; and" (157.53b);

- "computer-readable media external to the second processing unit, the computer-readable media storing at least" (157.53c);

- "The electronic appliance of claim 53, in which the second processing unit is operable to cryptographically seal information for storage on a computer-readable medium external to the second processing unit." (157.59).

To the extent a reference does not expressly or inherently disclose a second processing unit and computer readable media external thereto, this limitation is rendered obvious by the teaching of, at least, ABYSS 1987. ABYSS 1987 teaches that

> The supervisor process contains a cryptographic facility for managing encryption/decryption keys. This facility decrypts the protected parts of applications as they are loaded into the protected processor. We place the cryptographic transformation between primary memory (such as RAM) and secondary memory (such as a disk).

ABYSS 1987 at 40. ABYSS 1987 discloses in the system in Figure 1.

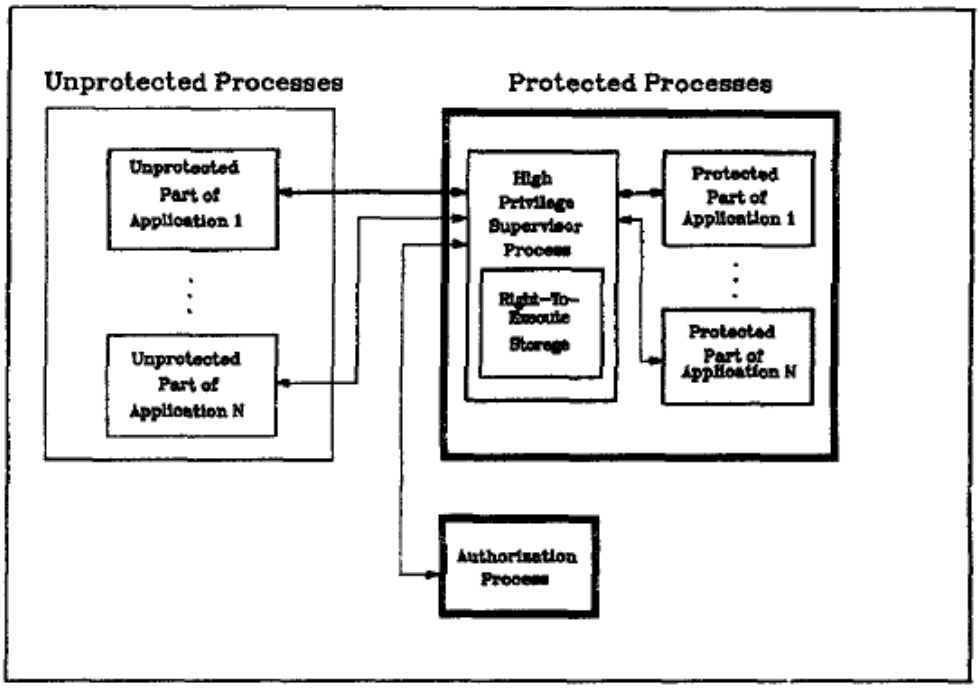


Figure 1. The Architecture of a Protected Processor System

Id. at 39.

Such second processors with external computer-readable medium are disclosed throughout the prior art. For example:

- "Program memory 52 is any conventional read-only memory (ROM) and is used to store the program executed by microprocessor 50 in performing the functions of RCM 18." Hornbuckle at 6:1-4.
- Hornbuckle at Figure 2.

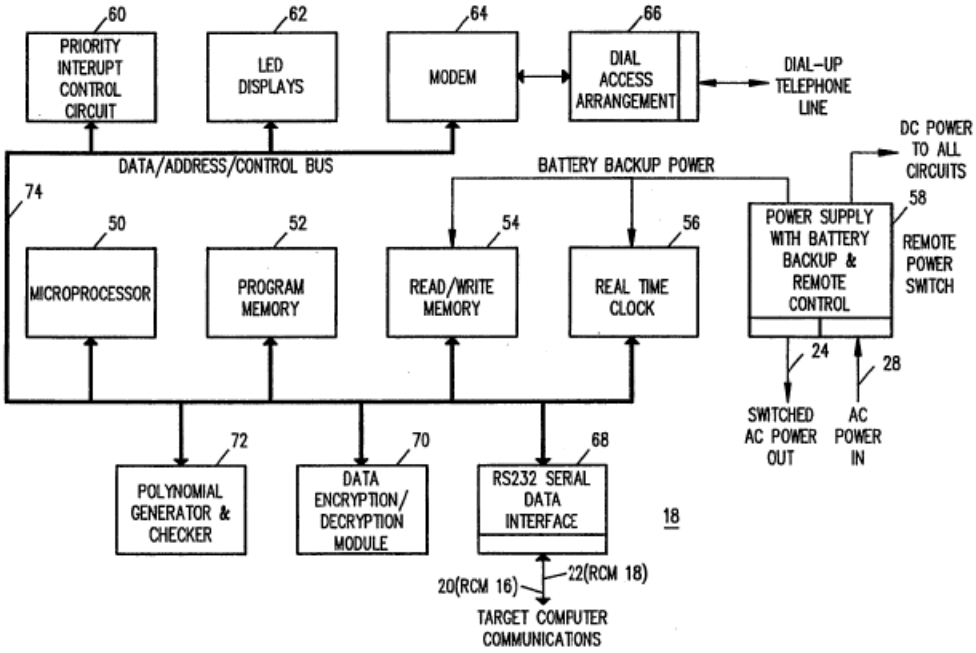


FIG. 2

- "Description will be given below on the information to be transmitted and received in this system, referring to FIG. 2 and FIG. 3. Shown in these figures is the information to be transmitted and received in this system, and each information is transmitted and received between broadcasting stations such as BS, CS, CATV, etc., receiving devices with tuner and decoder, charging centers, and data communication devices such as display phones, modem, etc. The broadcasting station and the receiving device are connected by radio wave or cable, and the charging center and the data communication device are connected by public telephone line. The broadcasting station and the charging center, and further, the receiving device and the data communication device are coupled directly, or by on-line communication means such as radio wave or cable, or by off-line means such as magnetic card, magnetic disk or memory card." Saito at 3:62-4:12.

Accordingly, the systems and methods can include a second processor with external computer-readable media, and it would have been obvious to one skilled in the art at the time of the alleged invention of the '157 Patent to include such functionality in combinations for the reasons discussed above.

Claims [157.56], [157.69c], and [157.87b] – One Key Used to Decrypt Another Key

The above-identified claims recite:

- "The electronic appliance of claim 54, in which the first cryptographic key is configured to decrypt a second cryptographic key, the second cryptographic key being configured to decrypt the piece of electronic content." (157.56);

- "decrypting, by the electronic appliance, the first key using (a) a second key and (b) a secure processing unit running on the electronic appliance, the second key being stored in memory of the secure processing unit;" (157.69c);

- "decrypting the first key using a second key stored in internal memory of a secure processing unit running on the electronic appliance;" (157.87b).

To the extent a reference does not expressly or inherently disclose using one key to decrypt another, this limitation is rendered obvious by the teaching of, at least, ABYSS 1987. ABYSS 1987 teach an "application key," and "unique supervisor keys," which can protect a another key. ABYSS 1987 at 40, 43. ABYSS 1987 discloses

> The fact that T, and the protected part of the application P are both encrypted under the application key A assures the protected processor that they were created by the same party.

Id. at 44.

> Targeted distribution can be achieved with unique supervisor keys. The software vendor uses the unique supervisor key of' the target system to encrypt the Right-To-Execute destined for that system. This ensures that no other system will be able to install' the Right-To-Execute. The software vendor can obtain the user's unique supervisor key, without it being revealed. This can be done by having the user's protected processor encrypt the unique key S. under a common supervisor key S_C to form $E_{SC}(S_U)$ is then sent to the software vendor's protected processor and decrypted.

Id. at 49.

Such second keys are disclosed throughout the prior art. For example:

- "However, since the encryption key is an important element which the software security scheme of the present invention depends, the encryption key itself is always transmitted in encrypted form to RCM 18 (utilizing an encryption key

> identical to the encryption key provided in RCM 18) to assure proper systems operation and integrity. When transmitted from RCM 16, the encryption key is then automatically decrypted as it is received by RCM 18 using a second, special key built into RCM 18 which is unique to each individual RCM 18. The decrypted encryption key is then stored in the RCM memory 52 until decryption of a key module is required. " Hornbuckle at 12:9-21.

Accordingly, using one key to decrypt another key would have been obvious to one skilled in the art at the time of the alleged invention of the '157 Patent to include such functionality in combinations for the reasons discussed above.

Claims [157.84a], [157.84b], [157.84c], [157.99a], [157.99b] and [157.99c] – Second Content

The above-identified claims recite:

- "The method of claim 69, further comprising: receiving, separately from the first piece of electronic content and the first electronic object, a second piece of electronic content;" (157.84a);
- "receiving a request to use the second piece of electronic content; and" (157.84b);
- "selectively granting the request [to use the second piece of electronic content] in accordance with the first electronic object." (157.84c);
- "The method of claim 86, further comprising: receiving, separately from the first piece of electronic content and the first electronic object, a second piece of electronic content;" (157.99a);
- "receiving a request to use the second piece of electronic content; and" (157.99b);
- "selectively granting the request [to use the second piece of electronic content] in accordance with the first electronic object." (157.99c).

To the extent a reference does not expressly or inherently disclose a second piece of content, this limitation is rendered obvious by the teaching of, at least, Waite. Waite teaches that sending a "shell which may contain a demonstration version of the software." Waite at 3:30-31. Waite discloses separately receiving a second piece of electronic content, to which access is selectively granted by the first electronic object:

> The shell may contain only sample displays and advertising descriptions or, alternatively, may contain an inactive version of the complete program. However, most embodiments are envisioned to include a registration program and a special program module called a loader segment.
>
> The marketing shell would be distributed freely by any appropriate method. If it contains a demonstration version of the program, the executive control loop will represent a limited version of the protected program. The marketing shell will prompt the prospective user to register. The registration program within the marketing shell relays registration data to a registration database computer. A unique encrypted package is assembled containing some data unique to the licensed user and an operational version of the program combined within an encrypted file. A unique decryption key is transmitted to the user's computer along with the encrypted file and any unprotected program files which may augment the marketing shell. Upon receiving the decrypt key, encrypted file, and unprotected files, the marketing shell will install each of these on the user's computer.
>
> Subsequently, each time the user executes the program, a loader segment will load and decrypt the encrypted file, as an overlay to the unprotected files, using the decrypt key provided.

Id. at 3:21-4:16.

Such second content are disclosed throughout the prior art. For example:

- "Moreover, it is not necessary to install a separate transmission system, such as a TV cable system, to access programs, since they are downloaded over conventional telephone lines. Finally, the software available for rent is not broadcast over the entire system, but rather individual programs are downloaded to the user's system from the host only after selection by the user." Hornbuckle at 2:65-3:5.

- "By means of the present invention, an authorized user at the target computer is able to "download" programs or data, via a telephone line and a programmable remote control module (RCM) connected at each end thereof from a central or host computer. Usage and other accounting data are monitored by the RCM and stored in memory resident therein. At predetermined times, the central or host computer accesses the RCM for the purpose of "uploading" the usage and other accounting data to the central or host computer." Hornbuckle at 3:27-36.

- "Accordingly, when downloading of software is desired, the host computer 12 calls the target computer 14, and once the call is acknowledged by RCM 18, the host computer 12 turns on the target computer 14 by actuating the AC power switch in

power supply 58 (FIG.2). When the target computer 14 is turned on by RCM 18 at the command of the host computer 12, the host computer 12 can download software to a storage device (not shown) associated with the target computer 14." Hornbuckle at 10:27-35.

- "As a method to request viewing, there are proposed a method to request according to the broadcasting time and a method to request by using an identifying information of the program itself. If the identifying information is not made public, the viewing request is made using a temporary identifying information. In case the broadcasting program is not identified according to the time, an identifying information is needed. In case the broadcasting program has an identifying information, which is open, the identifying information is used. If it is not open, a temporary identifying information is used for a viewing request." Saito at 5:34-45.

Accordingly, a second piece of electronic content may be received, and it would have been obvious to one skilled in the art at the time of the alleged invention of the '157 Patent to include such functionality in combinations for the reasons discussed above.

Claim 157.59 –Cryptographically Sealing Information

Claim 59 of the '157 Patent recites a "second processing unit [that] is operable to cryptographically seal information for storage on a computer-readable medium external to the second processing unit." Such cryptographic sealing of information was known in the art at the time of invention and, to the extent a reference does not expressly or inherently disclose "cryptographically seal[ing] information for storage on a computer-readable medium", this limitation is rendered obvious by the teaching of, at least, Hornbuckle. Hornbuckle teaches encryption and the application of encryption to keys and transmitted formats for protection of information. Hornbuckle at Abstract, 12:3-21. Hornbuckle discloses

> "Further referring to the encryption process of the present invention, data encryption/decryption module 70 of RCM 16 uses an encryption key unique to the individual target computer in which the rental software is to be used. Method of encrypting and decrypting using a encryption key, such as described in U.S. Pat. No. 4,649,233, are well-known. However, since the encryption key is an important element which the software security scheme of the present invention depends, the encryption key itself is always transmitted in encrypted

> form to RCM 18 (utilizing an encryption key identical to the encryption key provided in RCM 18) to assure proper systems operation and integrity. When transmitted from RCM 16, the encryption key is then automatically decrypted as it is received by RCM 18 using a second, special key built into RCM 18 which is unique to each individual RCM 18. The decrypted encryption key is then stored in the RCM memory 52 until decryption of a key module is required."

Id.

Such cryptographic sealing functionalities are disclosed throughout the prior art. For example:

- "The registration shell program 11 would provide a data entry form which would be displayed on the licensee PC, requesting the licensee to provide identification information, such as a billing address, an account number and the term of the license, etc. This information is entered into a registration request file 25 which is reviewed by the licensee. The registration shell program 11 would then wait for the licensee to initiate registration by pressing a designated key. When this key is pressed, the registration file is closed and a registration shell file transfer program 26 establishes a data link with the registration system file transfer program 32. The registration program 40 in the registration computer is protected by a validation means 42 to perform a security check ensuring that the data link has been established with a legitimate registration shell. The registration shell then transmits the registration request file 25 to the registration system which would receive the file, and perform the necessary error checking and hand-shaking operation between linked file transfer programs 26 and 32. When the complete registration request file is received at the central registration computer, the registration request is validated against a database of registered users 34." Waite at 7:13-33.

Accordingly, cryptographically sealing information was known in the art at the time of invention, and it would have been obvious to one skilled in the art at the time of the alleged invention of the '157 Patent to include such functionality in combinations of the prior art.

Claim [157.58] – Unique Identifier

Claim 58 of the '157 Patent recites "internal memory of the second processing unit [which] further comprises a unique identifier, the unique identifier being operable to distinguish the second processing unit from other processing units." Such a unique identifier was known in the art at the

time of invention and, to the extent an identified reference does not expressly or inherently disclose a unique identifier being operable to distinguish a processing unit, this limitation is rendered obvious by the teaching of, at least, ABYSS 1987. ABYSS 1987 teaches that "[u]nique supervisor keys allow unique identification of any protected processor." ABYSS 1987 at 49.

Such unique identifier functionalities are further disclosed throughout the prior art. For example:

- "The tamperproof overlay file contains both the executive control loop segment of the program instructions as well as unique user identification data which is appropriate to the method and control of the license. This data would include the time period of the license, the serial number of the computer, the telephone number of the computer's modem, as well as additional information." Waite at 11:22-28.

- "When transmitted from RCM 16, the encryption key is then automatically decrypted as it is received by RCM 18 using a second, special key built into RCM 18 which is unique to each individual RCM 18." Hornbuckle at 12:15-19.

- "In order to view the program on such pay satellite television broadcasting, it is necessary to use a special purpose tuner/decoder. The tuner/decoder is provided with an ID code, which is transmitted regularly (e.g. once monthly) from a satellite, and only the tuner/decoder receiving the transmitted ID code can descramble the program. The procedure to select and transmit ID for a viewer who signed a viewing contract is very troublesome, and an ID code is not transmitted unless the contract is signed in advance. Even when the viewer wants to view a pay-per-view program, there is no method of contracting for pay-per-program on occasion, and thus, the viewer cannot view the program upon request. Because the tuner/decoder is provided with ID which corresponds to each transmitting station, as many tuner/ decoders as the number of transmitting stations are needed to view programs of many pay satellite television stations." Saito at 1:26-31.

Accordingly, unique identifiers were known in the art, and it would have been obvious to one skilled in the art at the time of the alleged invention of the '157 Patent to include such functionality in combinations for the reasons discussed above.

Claims [157.60], [157.64], [157.65], [157.80], and [157.95] – Permitted or Prohibited Uses

Claims 60, 64, 65, 80, and 95 of the '157 Patent recite specified permitted or prohibited uses of content, or conditions thereof:

- "The electronic appliance of claim 53, in which the one or more permitted or prohibited uses of the piece of electronic content include viewing the piece of electronic content." (157.60);

- "The electronic appliance of claim 53, in which the one or more permitted or prohibited uses of the piece of electronic content include at least one of: editing the piece of electronic content, embedding additional content into the piece of electronic content, and/or extracting content from the piece of electronic content." (157.64);

- "The electronic appliance of claim 53, in which at least one of the one or more electronic objects specifies at least one condition associated with a permitted use of the piece of electronic content." (157.65);

- "The method of claim 69, in which the first electronic object specifies at least one condition associated with a permitted use of the first piece of electronic content." (157.80);

- "The method of claim 86, in which the first electronic object specifies at least one condition associated with a permitted use of the first piece of electronic content." (157.95).

To the extent a reference does not expressly or inherently disclose permitted or prohibited uses, this limitation is rendered obvious by the teaching of, at least, ABYSS 1987. ABYSS 1987 teaches that "[t]he software vendor can specify terms and conditions under which the application will execute, and allow the application itself to enforce them. In general, any terms and conditions that can be embodied in data in the protected processor, as a part of the Right-To-Execute, can be enforced." ABYSS 1987 at 49. ABYSS 1987 discloses:

> 4. At any time during execution, including at the very start, the protected part of the application may be allowed to access (and perhaps modify) selected parts of its own Right-To-Execute. It may use this in conjunction with the real-time clock in the protected processor, for instance, to verify that it is not being executed after its expiration date. Should the protected part of the application find that it is being executed contrary to the terms and conditions specified in its Right-To-Execute, it may effectively terminate its own execution..

Id. at 45.

Such content usage functionalities are disclosed throughout the prior art. For example:

- "The tamperproof overlay file contains both the executive control loop segment of the program instructions as well as unique user identification data which is appropriate to the method and control of the license. This data would include the time period of the license, the serial number of the computer, the telephone number of the computer's modem, as well as additional information." Waite at 3:11-28.

- "Remote control of the use of computer data is described in a system for renting computer software which derives use and billing information, prevents unauthorized use, maintains integrity of the software and controls related intercomputer communications." Hornbuckle at Abstract.

Accordingly, permitted or prohibited uses were known in the art at the time of invention, and it would have been obvious to one skilled in the art at the time of the alleged invention of the '157 and '158 Patents to include such functionality in combinations for the reasons discussed above.

Claims [157.66], [157.81], and [157.96] – Certain Time Period

Claims 66, 81, and 96 of the '157 Patent specify that a "permitted use may be made only for a certain time period." Specifically, the above-identified claims recite:

- "The electronic appliance of claim 65, in which the at least one condition comprises an indication that the permitted use may be made only for a certain time period." (157.66);

- "The method of claim 80, in which the at least one condition comprises an indication that the permitted use may be made only for a certain time period, and in which selectively granting the request comprises determining the at least one condition is satisfied." (157.81);

- "The method of claim 95, in which the at least one condition comprises an indication that the permitted use may be made only for a certain time period, and in which selectively granting the request comprises determining that the at least one condition is satisfied." (157.96).

To the extent a reference does not expressly or inherently disclose a certain time period for permitted use of electronic content, this limitation is rendered obvious by the teaching of, at least, ABYSS 1987. ABYSS 1987 teaches "an expiration date for its Right-To-Execute, and be assured that the application will not execute after that date." ABYSS 1987 at 40. ABYSS 1987 proceeds:

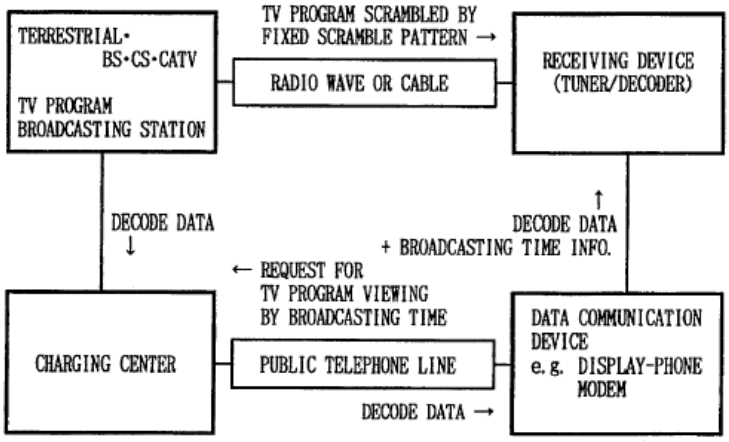
> The transferred Right-To-Execute may require renewal every minute or so to continue to be valid. The workstation can request renewal of the Right-To-Execute from the server at any time, and thus continue to possess a valid Right-To-Execute as long as is necessary. If the workstation does not check back with the server, the server knows that the workstation's Right-To-Execute has expired, so the server can increment its count of Rights-To-Execute for that application. The software lending library is much like a lending library for books, in which the books automatically reappear in the library when they are due.

Id. at 49.

Such permission functionalities are further disclosed throughout the prior art. For example:

- "A viewer, who wants to view a program, sends a viewing request to the charging center by specifying the broadcasting time via public telephone line using a data communication device. The charging center sends decode data of the program, to which the viewing request has been made, to the data communication device via public telephone line and collects a fee for the program. The data communication device sends the received decode data and broadcasting time information to a receiving device. Upon receipt of the decode data and the broadcasting time information, the receiving device descrambles the broadcasting program using the decode data." Saito at 7:5-19 (*see also* FIG.4, reproduced below).

Fig. 4



Accordingly, permitting use only during a certain time period was known in the art at the time of inventions, and it would have been obvious to one skilled in the art at the time of the alleged inventions of the '304, '157, and '158 Patents to include such functionality in combinations for the reasons discussed above.

c. Motivations to Combine Prior Art for the '815 Patent

Motivations to combine any of the prior art references identified herein for the '815 Patent with one another exists within the references themselves, as well as within the knowledge of those of ordinary skill in the art at the relevant time.

(1) Technical incentives and market forces drove similar solutions in the prior art.

Regarding the '815 Patent, many of the identified prior art references address the same technical issues and suggest similar solutions in the fields of digital rights management and cryptography. The '815 Patent's "invention relates generally to systems and methods for protecting data from unauthorized use or modification," and "[m]ore specifically . . . using digital signature and watermarking techniques to control access to, and use of, digital or electronic data."

’815 Patent at 1:23-28. The ’815 Patent recognized that the distribution and use of unauthenticated, unauthorized, corrupted, and/or modified files was a problem, especially in the Internet age. *See, e.g.*, ’815 Patent at 1:55-14. The ’815 Patent recognized that there was “a need for systems and methods for protecting electronic content and/or detecting unauthorized use or modification thereof.” ’815 Patent at 2:32-34. Indeed, this need was already recognized and addressed in the prior art and the field of the invention and would have provided a person of ordinary skill in the art motivation to combine the prior art references identified above.

For example, like the ’815 Patent, Renaud describes the need to control the use of files with the “increasing popularity of networked computing environments, such as the Internet.” Renaud at 1:21-22. For example, Renaud describes that there was “an increase in the demand to provide for the transferring of shared information among the networked computers in a secure manner” (Renaud at 1:24-26) and that it may be useful for a user to “verify that the data received was actually sent by the proper sending user rather than an imposter.” Renaud at 1:28-30. As noted by Renaud:

> For relatively open, unsecured networks such as the Internet, it may be useful for users to authenticate received data files prior to using them as intended. Such data files may include, but are not limited to, computer programs, graphics, text, photographs, audio, video, or other information that is suitable for use within a computer system. No matter the type of data file, authentication may be accomplished with a signature algorithm or similar type of encryption algorithm as described above. By way of example, if the data file is a software program the user may wish to authenticate that it was sent by a trustworthy authority prior to exposing his or her computer system to the software program, lest the program include a “Trojan Horse” that infects the user's computer with a virus. In such a case, the sending user may authenticate the data as described above.
>
> Another example is where the receiving user wishes to authenticate a text and/or image data file prior to displaying it on his or her computer screen. This may be useful to control the display of text and images having undesirable content. For example, parents may want to limit any access their children may have to pictures and text relating to adult subjects and materials. This can be accomplished by verifying that the data file (e.g., a text or image file), came from a trusted source. Similarly, providers of text and image files may want to provide a “stamp” of

approval or authenticity so as to control the use of tradenames and other intellectual property.

Renaud at 2:34-60. Accordingly, Renaud, like the '815 Patent, discloses systems and methods that addressed this need:

> The present invention provides more efficient methods, apparatuses and products for securing and verifying the authenticity of data files, such as data files intended to be transferred over computer networks. In accordance with one aspect of the present invention, a method for verifying the authenticity of data involves providing at least one data file which includes an identifier and a signature file which includes the identifier for the data file as well as a digital signature. The digital signature is then verified using a computer system, and the identifier in the data file is compared with the identifier in the signature file using the computer system.
>
> In one embodiment, the identifier for the data file includes at least one certificate authority, site certificate, software publisher identifier, or a site name, and verifying the authenticity of data involves setting a security level for at least one of the certificate authority, said site certificate, said software publisher identifier, and said site name. In such an embodiment, the data file is downloaded to the computer system, and if the data file is an applet and the digital signature is verified, then verifying the authenticity of data also involves branding and running the applet accordingly.

Renaud at 3:25-47.

As another example, Rohatgi also describes the need to ensure files are properly verified before enabling the use of a file in order to prevent damage to a user:

> Interactive television systems typically involve the transmission of programming and/or control data (hereafter PC-data), as well as audio and video information, to respective receiving apparatus. The receiving apparatus decodes the PC-data, and applies it to some type of control apparatus for automatic use by the receiver or selective use by the user of the receiver. The control apparatus may take the form of a computer, for example, and the use may include downloading selective e.g., financial data for subsequent user manipulation.
>
> As envisioned herein, information in the interactive television system (ITVS) is transmitted in compressed digital form. The receiving end of the system includes an integrated receiver decoder (IRD) for receiving and decompressing the transmitted information and providing decoded audio, video and PC-data to respective processors. The audio and video processors may be audio and video reproduction devices or a television receiver and the PC-data processor may be a computer. Ideally the system will only provide well tested PC-data provided by authorized service providers, and under such conditions there is little likelihood of

> transmitted information actually damaging respective receivers. However, if a large number of service providers are authorized to use the system, it becomes vulnerable to a) invasion by unauthorized users and intentional infliction of damage to system users, and b) careless preparation of PC-data and consequent unintentional damage to system users. The ability to broadcast PC-data to tens of thousands of IRD's simultaneously, multiplies the potential disruption that may be inflicted by ill behaved software many fold. Thus there is a need for measures to assure protection of respective ITVS receivers from both ill behaved and unauthorized PC-data.

Rohatgi at 1:11-44. Rohatgi also describes a solution similar to the '815 Patent: "A PC-data processor is configured to separate the certificate and to check it for authenticity. The processor hashes portions of the PC-data and compares the generated hash values with hash values transmitted with the PC-data and corresponding to the same portions of PC-data. If the hash values are identical and the certificate is authentic, the system is conditioned to execute the transmitted program." *Id*. at 1:52-59.

As another example, like the '815 Patent, Rabin describes the threat of piracy and the need to prevent the unauthorized use of files, and noted that "[p]rior art techniques for protecting the unauthorized use of software and information suffer from a variety of problems." Rabin at 2:10-11; *see also* Rabin at 1:6-2:44. Rabin, like the '815 Patent, proposes a solution that overcomes problems in the prior art:

> Specifically, the invention provides a system for supervising usage of software. The system includes a software vendor producing instances of software and a tag server accepting the instances of software. The tag server produces a plurality, of tags, one per instance of software, and each tag uniquely identifies an instance of software with which it is associated. A user device receives and installs an instance of software and securely receives a tag uniquely associated with that instance of software. The user device includes a supervising program which detects attempts to use the instance of software and which verifies the authenticity of the tag associated with the instance of software before allowing use of the instance of software. The supervising program on the user device verifies the authenticity of the tag and maintains or stores the tag in a tag table and maintains or stores the instance of software, preferably on a storage device, if the tag is authentic. The supervising program rejects the instance of software if the tag associated with the software is not authentic.

Rabin at 3:47-65.

Additional references address similar needs and provide solutions in the context of managing the use of, and authenticating files including:

- "The present invention relates generally to verifying the source of digital graphic information being transmitted. More particularly, the present invention relates to compressing data and attaching a digital signature to the compressed data. The invention is useful in authenticating compressed data when lossy compression techniques are used or when transmission is interrupted." Davis at 1:6-12.

- "This invention generally relates to data corruption detection and, more particularly, to a method and apparatus for efficient authentication and integrity checking in data processing using hierarchical hashing." Hanna at 1:6-8.

- "A method of signing digital streams so that a receiver of the stream can authenticate and consume the stream at the same rate which the stream is being sent to the receiver. More specifically, this invention involves computing and verifying a single digital signature on at least a portion of the stream. The properties of this single signature will propagate to the rest of the stream through ancillary information embedded in the rest of the stream." Gennaro at Abstract.

- "A system for controlling use and distribution of digital works is disclosed. A digital work is any written, aural, graphical or video based work including computer programs that has been translated to or created in a digital form, and which can be recreated using suitable rendering means such as software programs. The present invention allows the owner of a digital work to attach usage rights to the work. The usage rights for the work define how it may be used and distributed. Digital works and their usage rights are stored in a secure repository. Digital works may only be accessed by other secure repositories. Usage rights for a digital work are embodied in a flexible and extensible usage rights grammar. Conceptually, a right in the usage rights grammar is a label attached to a predetermined behavior and conditions to exercising the right. For example, a COPY right denotes that a copy of the digital work may be made. A condition to exercising the right is the requester must pass certain security criteria. Conditions may also be attached to limit the right itself. For example, a LOAN right may be defined so as to limit the duration of which a work may be LOANed. Conditions may also include requirements that fees be paid." Stefik '980 at 3:51-4:5.

- "The single most obvious use of the present invention in digital cameras would be in situations where proof of image authenticity is necessary; such as for legal evidence, insurance claims, or intelligence gathering. The inevitable transition to digital cameras and electronically-transmitted images will also make it more difficult for the photographer to protect his image copyright, since electronic images tend to proliferate faster and with less control from the author than the traditional distribution method which places image control in the hands of whoever holds the original negative or transparency. Just as it is common

practice today to obtain releases from photographed persons for any published picture containing a recognizable image of the person, it is reasonable that in the future no electronic image will be published without first having authenticated the image using the digital signature of the camera which is registered with the photographer in order to thwart claims that photographs published have been altered and to improve the trustworthiness of all publications and to uphold copyright claims." Friedman at 8:37-45.

- "In accordance with the present invention, a method is provided for generating a digital signature that authenticates information of a plurality of different information groups. Information from each of the groups is hashed to produce a separate hash key for each group. Each hash key authenticates the information in its respective group. Particular combinations of the hash keys are then hashed together to produce at least one combined hash key. The digital signature is derived from (e.g., equal to or produced from) at least one combined hash key. The digital signature can be used, for example, as a program key in a subscription television access control system. The signature can also be used for any other purpose in which authenticated information is required for data security purposes." Sprunk at 4:32-45.

- "The present invention provides systems and methods for electronic commerce including secure transaction management and electronic rights protection. Electronic appliances such as computers employed in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Secure subsystems used with such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions." Ginter '987 at Abstract.

- "The present invention relates to a platform and corresponding method to protect content from unauthorized observation and/or manipulation through hardware-based identification and a variety of content protection mechanisms. Selected combinations of content protection mechanisms combined with hardware-based identification can provide different levels of access control. Each level of access control is associated with a unique degree of protection against unauthorized observation and/or manipulation of content. Hence, each level of access control comprises: one or more authentication checks of a client identifier and/or auxiliary information associated with the content purchaser; content transformation and distortion; and possibly extraction of meta-data from delivered content." Yeung at 2:29-42.

- "A software use method control system including a storage device and an access controller. The storage device stores information for designating a right to access system resources of operating systems which are to be executed in the software use method control system. The access controller controls access to the system resources of the operating systems. The system also includes a privilege protecting section. The privilege protecting section includes an input receiver for receiving an execution request made by a software user, a

program-executing device for executing a program having a right to access all system resources of the operating systems, and a program-execution inhibiting device for determining whether the program-executing device is allowed to executed the program, from the execution request which the input receiver has received, and for inhibiting the program executing device from executing the programs when the programs are not allowed to be executed." Morishita at Abstract.

- "Accordingly, it is an object of this invention to provide a system and a method of low cost and secure data control using a electronic watermarking technique. It is another object of this invention to provide a system of safely controlling copying, play-back and receiving of data using a electronic watermarking technique. It is still another object of this invention to provide a method and a system which are resistive to an attack by a willful third party." Miwa at 3:19-28.

- "The bit string attached to the document when signed (in the previous example, the one-way hash of the document encrypted with the private key) will be called the digital signature, or just the signature. The entire protocol, by which the receiver of a message is convinced of the identity of the sender and the integrity of the message, is called authentication. Further details on these protocols are in Section 3.2." Schneier at 39 .

- "When a message is received, the recipient may desire to verify that the message has not been altered in transit. Furthermore, the recipient may wish to be certain of the originator's identity. Both of these services can be provided by the DSA. A digital signature is an electronic analogue of a written signature in that the digital signature can be used in proving to the recipient or a third party that the message was, in fact, signed by the originator. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time" FIPS PUB 186 at 5 .

- "The primary goal of information protection is to permit proprietors of digital information (i.e., the artists, writers, distributors, packagers, market researchers, etc.) to have the same type and degree of control present in the "paper world." Because digital information is intangible and easily duplicated, those rights are difficult to enforce with conventional information processing technology . . . . For example, the protections needed for content elements incorporate the licensing provisions for the intellectual property rights of the content rightsholders. In a broader sense, these rights include control over several activities: the right to be compensated for use of the property; the right to control how content is distributed; the right to prevent modification of content by a distributor; "fair use" rights; the rights to the usage data, privacy rights of individuals, and so on . . . . DigiBox is a foundation technology within InterTrust. It provides a secure container to package information so that the information cannot be used except as provided by the rules and controls associated with the content. InterTrust rules and controls specify what types of content usage are permitted, as well as the consequences of usage such as reporting and payment." DigiBox at 4-7.

- "The Packer Certificate is then authenticated. Then the authenticity of the entire package is validated. The Clearing Center then evaluates what rights to grant the consumer based on the consumer identity information, the environment, the RML, and the specific rights

> requested. Instructions which reflect these rights that can be implemented by the consumer workstation are then generated and placed in a file. An event record is also generated noting the rights granted the price, and so forth. This event record is forwarded, either immediately, or after aggregation, to the electronic commerce component responsible for tracking these events. While the generation of the event is the responsibility of the Cryptolope technology, the use made of the event is unique to the encompassing electronic commerce system. This typically includes at least financial accounting functions, but may include other forms of accounting as well." Cryptolope at 10-11.

Regarding the '815 Patent, market forces and design incentives demanded systems and methods that verified authenticity of files before granting a user's request to use the files to ensure content providers and users were protected against the proliferation of inauthentic files (e.g., unauthorized, pirated, corrupted, and/or incorrect copies, etc.). Thus one of skill in the art would have been motivated to combine or modify references using known methods that one of skill in the art would have recognized as offering improvements to solutions of that time. The references identified describe methods that were known to offer improvements, and, accordingly, one of skill in the art would have been motivated to combine or modify combined references to include such improvements.

(2) Combination of known elements yields predictable results.

Because the Asserted Claims of the '815 Patent simply arrange old elements known in digital rights management, cryptography, authentication of sent and received data, hash functions, integrity, and encryption, with each performing the same function it had been known to perform, and yields no more than what one would have expected from such an arrangement, combinations of the prior art concepts would have been obvious. At the time of the alleged invention of the '815 Patent, there were a finite number of predictable solutions for managing the use of files, e.g., the use of authenticating files with digital signatures and check values (e.g., hashes) and controlling

the use of a files in a predefined manner. Accordingly, a person of ordinary skill in the art had good reason to pursue and/or combine known options and related applications.

Moreover, the alleged invention of the '815 Patent is built upon technology that significantly pre-dates the alleged priority date. For example, hashes and signatures were well-known before the '815 Patent. *See, e.g.*, Schneier at 34 ("Handwritten signatures have long been used as proof of authorship of, or at least agreement with, the contents of a document."); *id*. at 30 ("One-way hash functions are another building block for many protocols. Hash functions have been used in computer science for a long time."); *id*. at 38 ("To save time, digital signature protocols are often implemented with one-way hash functions [432,433]. Instead of signing a document, Alice signs the hash of the document."). Indeed, the '815 Patent concedes hashing and digital signature techniques were well-known in the art. *See, e.g.*, '815 Patent at 23:54-57 ("The digital signature can be formed using any suitable one of the well-known digital signature techniques, and typically comprises a hash (1420) of a combination of the hashes 1402 . . . ."); *id*. at 10:35-37 ("[A]pplying a strong cryptographic hash algorithm 202 (e.g., SHA-1) to a block of data 200.") The prior art describes various authentication techniques involving digital signatures and hashes. *See, e.g.*, Renaud at 7:66-8:55, Davis at 5:43-57, Rabin at 8:13-34, Gennaro at 5:21-67, Rohatgi at 1:48-59, Hanna at 9:22-10:5, Friedman at 6:2-52. Further, the prior art describes various techniques to manage the use of files. *See, e.g.*, Renaud at 2:34-60, Rabin at 8:13-34, Gennaro at 5:54-63, Rohatgi at 5:6-15, Stefik '980 at 7:6-37, Ginter at Abstract, Yeung at 2:29-3:39, Morishita at Abstract, Miwa at 3:18-59. These techniques were available to a person of ordinary skill in the art at the time of the alleged invention, and a person of ordinary skill in the art could have easily drawn on and combined those concepts to implement a digital rights management system such as identified in the '815 Patent.

The art identified, including without limitation Rabin, Gennaro, Rohatgi, Renaud, and Stefik '980, all address systems and methods directed to digital rights management using authentication techniques. In particular, these references disclose systems and methods to manage the use of files which are implemented using digital signature and hashing techniques, like the Asserted Claims of the '815 Patent, and at the time of the alleged invention of the '815 Patent would have been well-known to a person of ordinary skill in the art.

A person of ordinary skill in the art having knowledge of these well-known concepts would have been motivated, taught, and suggested to combine the prior art as identified above. For example, it would have been obvious to a person of ordinary skill in the art to combine any one of the above references' authentication techniques with the knowledge of a person of ordinary skill in the art to implement the techniques in a digital rights management application and vice versa. At the time of the alleged invention of the '815 Patent, a person of ordinary skill in the art would know that authentication could be used to control the use of a file, and that it would be trivial and predictable to do so.

Further, motivation exists because the patents, publications, and systems all are from the same or similar field of art, and a person of ordinary skill in the art would have drawn equally from the field of art to solve the problem allegedly presented in the '815 Patent. The suggested combinations reflect at least combinations of prior art elements according to known methods to yield predictable results, simple substitutions of known elements to obtain predictable results, and combinations that are obvious to try. Further elaboration and information shall be provided with Defendants' expert reports.

(3) Exemplary prior art combinations

As discussed above, Appendix C sets out the references that disclose each element of the Asserted Claims of the '815 Patent and Defendants contend that it would have been obvious to modify such reference to include the allegedly missing element, in view of the knowledge of one of ordinary skill in the art, the admitted prior art of the '815 Patent, and/or in combination with any of the other prior art references identified in the '815 Patent. By way of example, and without limitation, Defendants provide the following exemplary combinations for particular claim limitations based on teachings of the cited prior art references. Defendants reserve the right to rely upon any combination of prior art references whether listed herein or otherwise.

Claim [815.42a] – Receiving a request to use the file in a predefined manner

To the extent a reference does not expressly or inherently disclose receiving a request to use the file in a predefined manner, this limitation is rendered obvious by the teachings of, at least, Renaud at 2:42-60:

> By way of example, if the data file is a software program the user may wish to authenticate that it was sent by a trustworthy authority prior to exposing his or her computer system to the software program, lest the program include a "Trojan Horse" that infects the user's computer with a virus. In such a case, the sending user may authenticate the data as described above.
>
> Another example is where the receiving user wishes to authenticate a text and/or image data file prior to displaying it on his or her computer screen. This may be useful to control the display of text and images having undesirable content. For example, parents may want to limit any access their children may have to pictures and text relating to adult subjects and materials. This can be accomplished by verifying that the data file (e.g., a text or image file), came from a trusted source. Similarly, providers of text and image files may want to provide a "stamp" of approval or authenticity so as to control the use of tradenames and other intellectual property.

Renaud at 2:42-60; *see also* 9:61-67.

This concept is also rendered obvious by the teachings of, at least, Rabin at 8:13-26:

> Another embodiment of the invention is a user device that includes an input port that receives an instance of software and receives a tag uniquely associated with that instance of software and also receives a request to use the instance of software. A processor included in the user device executes a supervising program. The supervising program detects the request to use the instance of software and verifies the authenticity of the tag associated with the instance of software before allowing use of the instance of software by the user device. The supervising program also verifies the authenticity of the tag and stores the tag in a tag table and maintains the instance of software if the tag is authentic and rejects the instance of software if the tag associated with the software is not authentic.

Rabin at 8:13-26; *see also* 3:29-44.

This concept is also rendered obvious by the teachings of, at least, Rohatgi at 5:6-15:

> The receiver functions related to execution of transmitted interactive applications will be described in the context of the IRD controller 89 operating with the transmitted application. (It should be noted, that interactivity does not necessarily mean that the user interacts with the provider, though this is one aspect of interactivity. Interactivity also includes the concept of a user being able to affect the signal/system at the user's end of the system in accordance with a transmitted application, particularly in the realm of educational programs.)

Rohatgi at 5:6-15; *see also* 1:11-22, 6:58-67.

This concept is also rendered obvious by the teachings of, at least, Stefik '980 at 7:19-33:

> Assuming that a session can be established, Repository 2 may then request access to the Digital Work for a stated purpose, step 104. The purpose may be, for example, to print the digital work or to obtain a copy of the digital work. The purpose will correspond to a specific usage right. In any event, Repository 1 checks the usage rights associated with the digital work to determine if the access to the digital work may be granted, step 105. The check of the usage rights essentially involves a determination of whether a right associated with the access request has been attached to the digital work and if all conditions associated with the right are satisfied. If the access is denied, repository 1 terminates the session with an error message, step 106. If access is granted, repository 1 transmits the digital work to repository 2, step 107.

Stefik '980 at 7:19-33; *see also* Fig. 1, 6:36-50, 5:56-6:14, 42:25-43:4.

Other example disclosures are included in the attached charts of Appendix C. Accordingly, receiving a request to use the file in a predefined manner was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged conception of the alleged

invention of the ’815 Patent to include such functionality in combinations for the reasons discussed above including, for example, that doing so would be applying a known technique to other digital rights management and cryptographic systems to achieve the same result.

Claims [815.42b] – Retrieving at least one digital signature and at least one check value associated with the file;

To the extent a reference does not expressly or inherently disclose retrieving at least one digital signature and at least one check value associated with the file, it would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the ’815 Patent to do so because digital signatures and check values (e.g., hashes) were well-known in the art. For example, the ’815 Patent itself acknowledges that “[t]he digital signature can be formed using any suitable one of the well-known digital signature techniques, and typically comprises a hash (1420) of a combination of the hashes 1402, hints 1404, and quality indicator(s) 1406, the hash being encrypted (1422) using the issuer's private key (or secret key as appropriate) 1410.” ’815 Patent at 23:54-60; *see also id*. at 10:31-56. The concept of retrieving digital signatures and hashes was well-known and extensively discussed in many different references. As Davis at 5:43-57 explains:

> During transmission, the SCSD 100 first sends a copy of the hash sequence table 137 accompanied by its digital signature 138. Thereafter, SCSD 100 transmits data forming the compressed image frame 130.
>
> FIG. 4 is an illustrative block diagram showing a receiving device which receives the data transmitted by the SCSD of FIG. 3. The receiving device 200 receives data over communication link 300. The receiving device 200 first authenticates the hash sequence table 137 transmitted over the link 300 by performing operations on digital signature 138. The received digital signature 138 is decrypted using the public key ("PUK1") 190 of the SCSD to recover a hash value 210 for the hash sequence table 137. If the hash value 210 matches the hash result 220 of the hash sequence table 137, the received hash sequence table 137 is authentic.

Davis at 5:43-57.

This concept is also rendered obvious by the teachings of, at least, Renaud at 7:55-60:

> The signed signature file from step 408 is then sent, provided or otherwise made available to the receiving user in step 410. Step 410 can, for example, include transmitting the signed Signature file over a data bus, data link, the Internet, or some other computer or data communication network or link.

Renaud at 7:55-60; *see also* 7:15-54, Figs. 4, 6.

This concept is also rendered obvious by the teachings of, at least, Rabin at 8:13-34:

> Another embodiment of the invention is a user device that includes an input port that receives an instance of software and receives a tag uniquely associated with that instance of software and also receives a request to use the instance of software. A processor included in the user device executes a supervising program. The supervising program detects the request to use the instance of software and verifies the authenticity of the tag associated with the instance of software before allowing use of the instance of software by the user device. The supervising program also verifies the authenticity of the tag and stores the tag in a tag table and maintains the instance of software if the tag is authentic and rejects the instance of software if the tag associated with the software is not authentic.
>
> According to one aspect of the user device, the supervising program computes a hash function value on the instance of software and compares the computed value with a hash function value in the tag to determine whether the tag is authentic and is properly associated with the instance of software. The tag is preferably digitally signed and the supervising program verifies the authenticity of the tag by verifying a digital signature of the tag.

Rabin at 8:13-26.

This concept is also rendered obvious by the teachings of, at least, Rohatgi at 8:61-9:7:

> The preferred method comprises performing hash functions over respective modules, inserting the respective hash values in the further security information fields of the directory module and subsequently performing a hash function over the Directory Module. The hash Value of the Directory Module is then encrypted with the providers private key.
>
> A trusted application provider will be assigned a signed certificate which includes items such as the providers public key, the providers ID, an expiration date of the certificate, possibly the amount of storage allocated the provider at the receiver etc. This certificate is signed with the system controller's private key. The encrypted hash value is appended to the signed certificate and the combination is appended to the Directory Module. The directory Module and all other modules are provided to the system controller in plaintext. Data Modules which are selected for protection and which are frequently changing, are protected by means of a signature of the provider on the hash value over the Data Module, which signature is made part of the respective module.

Rohatgi at 8:61-9:7; *see also* Abstract, Figs. 10, 11.

This concept is also rendered obvious by the teachings of, at least, Gennaro at 5:21-34:

> The following constitute the steps that the authentication software follows. Step 1) Before receiving the combined stream (1.100c) the receiver receives the initial authentication data (1.20) consisting of a digital signature on the hash of the first combined block (1.10c) and the size of first combined block, together with the purported values of the hash and size. The authentication software at this stage does the following (2.25a): It verifies the signature. If the provided signature verifies, then the purported hash and size values of the first combined block (1.10c) are authentic, and the hash and size values 1.25 are extracted out for use in authenticating the combined stream (1.100c).

Gennaro at 5:21-34.

This concept is also rendered obvious by the teachings of, at least, Hanna at 9:22-28:

> Fig. 3 is a flowchart of the steps used in the data receiving and verification procedure for systems consistent with the present invention. To verify data, the digital signature on the top level packet must be verified first (step 320). If the signature fails this verification step or it is determined that the packet was corrupted during transmission, the top level packet must be repaired or recovered before checking the other packets (steps 330, 335). If lower level hash blocks were signed for extraordinary redundancy, their signatures may be checked in this case to allow verification to proceed.

Hanna at 9:22-28; *see also* Fig. 3.

This concept is also rendered obvious by the teachings of, at least, Stefik '980 at 42:38-48:

> The requester extracts a copy of the digital certificate for the software. If the certificate cannot be found or the master repository for the certificate is not known to the requester, the transaction ends with an error.
>
> The requester decrypts the digital certificate using the public key of the master repository, recording the identity of the supplier and creator, a key for decrypting the software, the compatibility information, and a tamper-checking code. (This step certifies the software.)

Stefik '980 at 42:38-48.

Other example disclosures are included in the attached charts of Appendix C. Accordingly, retrieving a digital signature and check value associated with the file was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged conception of the

alleged invention of the '815 Patent to include such functionality in combinations for the reasons discussed above including, for example, that doing so would be applying a known technique to other digital rights management and cryptographic systems to achieve the same result.

Claim [815.42c] - Verifying the authenticity of the at least one check value using the digital signature

To the extent a reference does not expressly or inherently disclose verifying the authenticity of the at least one check value using the digital signature, this limitation is rendered obvious by the teachings of, at least, Davis at 5:50-57:

> The receiving device 200 first authenticates the hash sequence table 137 transmitted over the link 300 by performing operations on digital signature 138. The received digital signature 138 is decrypted using the public key ("PUK1") 190 of the SCSD to recover a hash value 210 for the hash sequence table 137. If the hash value 210 matches the hash result 220 of the hash sequence table 137, the received hash sequence table 137 is authentic.

Davis at 5:50-57.

This concept is also rendered obvious by the teachings of, at least, Renaud at 7:66-8:3:

> Upon receipt or access, the receiving user in step 412, verifies the authenticity of the signed signature file sent or made available in step 410. Step 412 can, for example, include verifying the digital signature on the signed signature file with a signature algorithm by way of a key.

Renaud at 7:66-8:3, *See also* Figs. 4, 6.

This concept is also rendered obvious by the teachings of, at least, Rabin at 8:13-34:

> Another embodiment of the invention is a user device that includes an input port that receives an instance of software and receives a tag uniquely associated with that instance of software and also receives a request to use the instance of software. A processor included in the user device executes a supervising program. The supervising program detects the request to use the instance of software and verifies the authenticity of the tag associated with the instance of software before allowing use of the instance of software by the user device. The supervising program also verifies the authenticity of the tag and stores the tag in a tag table and maintains the instance of software if the tag is authentic and rejects the instance of software if the tag associated with the software is not authentic.

> According to one aspect of the user device, the supervising program computes a hash function value on the instance of software and compares the computed value with a hash function value in the tag to determine whether the tag is authentic and is properly associated with the instance of software. The tag is preferably digitally signed and the supervising program verifies the authenticity of the tag by verifying a digital signature of the tag.

Rabin at 8:13-26.

This concept is also rendered obvious by the teachings of, at least, Rohatgi at 1:48-59:

> A receiver embodiment of the invention includes an IRD which is responsive to a transmitted program guide for selecting signal packets of PC-data. The IRD temporarily stores the selected PC-data. Authorized PC-data will include a certificate. A PC-data processor is configured to separate the certificate and to check it for authenticity. The processor hashes portions of the PC-data and compares the generated hash values with hash values transmitted with the PC-data and corresponding to the same portions of PC-data. If the hash values are identical and the certificate is authentic, the system is conditioned to execute the transmitted program.

Rohatgi at 1:48-59; *see also* Abstract, 16:4-29, Fig. 10, 11.

This concept is also rendered obvious by the teachings of, at least, Gennaro at 5:21-34:

> The following constitute the steps that the authentication software follows. Step 1) Before receiving the combined stream (1.100c) the receiver receives the initial authentication data (1.20) consisting of a digital signature on the hash of the first combined block (1.10c) and the size of first combined block, together with the purported values of the hash and size. The authentication software at this stage does the following (2.25a): It verifies the signature. If the provided signature verifies, then the purported hash and size values of the first combined block (1.10c) are authentic, and the hash and size values 1.25 are extracted out for use in authenticating the combined stream (1.100c).

Gennaro at 5:21-34.

This concept is also rendered obvious by the teachings of, at least, Hanna at 9:22-28:

> Fig. 3 is a flowchart of the steps used in the data receiving and verification procedure for systems consistent with the present invention. To verify data, the digital signature on the top level packet must be verified first (step 320). If the signature fails this verification step or it is determined that the packet was corrupted during transmission, the top level packet must be repaired or recovered before checking the other packets (steps 330, 335). If lower level hash blocks were signed for extraordinary redundancy, their signatures may be checked in this case to allow verification to proceed.

Hanna at 9:22-28; *see also* Fig. 3.

Other example disclosures are included in the attached charts of Appendix C. Accordingly, using a digital signature to verify the authenticity of a check value (e.g., hash) was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the '815 Patent to include such functionality in combinations for the reasons discussed above including, for example, that doing so would be applying a known technique to other digital rights management and cryptographic systems to achieve the same result.

Claims [815.42d] and [815.43] – verifying the authenticity of at least a portion of the file using the at least one check value

To the extent a reference does not expressly or inherently disclose verifying the authenticity of at least a portion of the file using the at least one check value (and claimed variant of claim 43: wherein the at least one check value comprises one or more hash and verifying the authenticity of at least a portion of the file using the at least one check value includes: hashing at least a portion of the file to obtain a first hash value; and comparing the first hash value to at least one of the one or more hash values), these limitations are rendered obvious by the teachings of, at least, Davis at 6:1-8:

> The receiving device 200 processes the coefficients that correspond to section A 230 by hashing these coefficients with the same hash function 231 originally used by SCSD to generate the digest A as shown in FIG. 3. Thus, if the data is authentic, digest A 232 will match the digest contained in the first portion 1361 of the authenticated hash sequence table 137. If the digests do not match, then the receiving device 200 may notify the user that the data is not authentic.

Davis at 6:1-8.

This concept is also rendered obvious by the teachings of, at least, Renaud at 8:43-55:

> Step 420 includes loading the ith data file. Step 420 can, for example, include any of the methods in step 410 to either download, upload, broadcast, or otherwise move the ith data file from one location to another location. Once the ith data file has been loaded, step 422 includes providing, computing or generating the identifier for the ith data file with the appropriate identifier algorithm (for that data file).

> Next, step 424 includes comparing the identifier provided in step 422 with the identifier listed, for the ith data file, in the signature file which was stored in step 416. If the identifiers match then the ith data file is verified as authentic. If the identifiers do not match then the ith data file is considered not to have been verified.

Renaud at 8:43-55; *see also* Figs. 4, 6.

This concept is also rendered obvious by the teachings of, at least, Rabin at 8:13-34:

> Another embodiment of the invention is a user device that includes an input port that receives an instance of software and receives a tag uniquely associated with that instance of software and also receives a request to use the instance of software. A processor included in the user device executes a supervising program. The supervising program detects the request to use the instance of software and verifies the authenticity of the tag associated with the instance of software before allowing use of the instance of software by the user device. The supervising program also verifies the authenticity of the tag and stores the tag in a tag table and maintains the instance of software if the tag is authentic and rejects the instance of software if the tag associated with the software is not authentic.
>
> According to one aspect of the user device, the supervising program computes a hash function value on the instance of software and compares the computed value with a hash function value in the tag to determine whether the tag is authentic and is properly associated with the instance of software. The tag is preferably digitally signed and the supervising program verifies the authenticity of the tag by verifying a digital signature of the tag.

Rabin at 8:13-34; *see also* 12:12-21.

This concept is also rendered obvious by the teachings of, at least, Rohatgi at 1:48-59:

> A receiver embodiment of the invention includes an IRD which is responsive to a transmitted program guide for selecting signal packets of PC-data. The IRD temporarily stores the selected PC-data. Authorized PC-data will include a certificate. A PC-data processor is configured to separate the certificate and to check it for authenticity. The processor hashes portions of the PC-data and compares the generated hash values with hash values transmitted with the PC-data and corresponding to the same portions of PC-data. If the hash values are identical and the certificate is authentic, the system is conditioned to execute the transmitted program.

Rohatgi at 1:48-59; *see also* Abstract, 16:30-40, Figs. 10, 11.

This concept is also rendered obvious by the teachings of, at least, Gennaro at 5:40-67:

> Step 3) The incoming combined stream is split into blocks by the authentication software shown in FIG. 2. This splitting is facilitated by the software always

> knowing in advance the authenticated size of the next incoming combined block long before the incoming block is fully received. The following algorithm or step (2.26a), which is repeated for all the blocks in the stream, is now applied:
>
> i) Compute the MD5 hash of the incoming bytes as they are transferred into the buffer of the receiver. As soon as a block comes in, its MD5 hash gets computed, and computation of the MD5 hash of the next incoming block is started (although its length is not immediately known).
>
> ii) The MD5 hash of the recently arrived block is compared against what it should be according to the authentication chain emanating from the Digital Signature from (1.20). If it is different, then tampering has been detected and processing halted. Otherwise, the MPEG software/hardware is informed that a block of bits of a certain size representing a frame has arrived and it can proceed to process the incoming original block that was authenticated.
>
> iii) Concurrently with the above, the now authenticated size and hash of the next block stored in the ancillary part of the processed block (1.50) is extracted for use to authenticate the next block.

Gennaro at 5:40-67.

This concept is also rendered obvious by the teachings of, at least, Hanna at 10:1-5:

> Once a hash block is received and verified, data packets that depend on it may be verified (step 340) by computing the hash of the packet and comparing it with the hash value stored in the hash block (step 350). If this check fails, the data packet is corrupt and should be repaired or recovered (step 350). Of course the verification process must use the same hash function used to sign the data.

Hanna at 10:1-5; *see also* Fig. 3.

This concept is also rendered obvious by the teachings of, at least, Stefik '980 at 42:49-55:

> The requester decrypts the software using the key from the certificate and computes a check code on it using a 1-way hash function. If the check-code does not match the tamper-checking code from the certificate, the installation transaction ends with an error. (This step assures that the contents of the software, including the various scripts, have not been tampered with.)

Stefik '980 at 42:49-55.

Other example disclosures are included in the attached charts of Appendix C. Accordingly, using the check value (e.g., hash) to verify the authenticity of the file was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged conception of the

alleged invention of the '815 Patent to include such functionality in combinations for the reasons discussed above including, for example, that doing so would be applying a known technique to other digital rights management and cryptographic systems to achieve the same result.

Claim [815.42e] – Granting the request to use the file in the predefined manner

To the extent a reference does not expressly or inherently disclose granting the request to use the file in the predefined manner this limitation is rendered obvious by the teachings of, at least, Renaud at 13:36-14:4:

> If security is satisfied, either by virtue of the fact that the brand placed on the applet compares favorably with the Security Settings, or by Virtue of the fact that the user has authorized the applet action, then the applet action is allowed in step 620. Process control then returns to step 610, and the continued execution of the applet. On the other hand, if Security is not satisfied in Step 618, then the applet action is disallowed in Step 622.
>
> . . .
>
> Returning to the check for signature validity in step 606, if a determination is made that the signature is not valid, then the archive is considered to be unsigned, and process flow proceeds to step 624 which is the determination of whether the unsigned stream should be accepted. In the described embodiment, the determination of whether the unsigned stream should be accepted is made by a user through the use of a user interface. By way of example, the user can be prompted with a warning dialog which indicates that while the signature was not valid, he can make the decision to run the applet. If the determination is made that the unsigned stream is to be accepted, process flow moves to step 608 in which the applet is branded as appropriate, e.g., branded to indicate that the stream associated with the applet is unsigned. If the determination in step 624 is that the unsigned stream is not to be accepted, then the applet is stopped, or prohibited, from running in step 626, and the process of executing an applet ends.

Renaud at 13:36-14:4; *see also* 8:66-9:7, 9:22-29, 10:38-43, Fig. 4, 6.

This concept is also rendered obvious by the teachings of, at least, Rabin at 8:13-26:

> Another embodiment of the invention is a user device that includes an input port that receives an instance of software and receives a tag uniquely associated with that instance of software and also receives a request to use the instance of software. A processor included in the user device executes a supervising program. The supervising program detects the request to use the instance of software and verifies the authenticity of the tag associated with the instance of software before allowing

use of the instance of software by the user device. The supervising program also verifies the authenticity of the tag and stores the tag in a tag table and maintains the instance of software if the tag is authentic and rejects the instance of software if the tag associated with the software is not authentic.

Rabin at 8:13-26.

This concept is also rendered obvious by the teachings of, at least, Rohatgi at 1:48-59:

A receiver embodiment of the invention includes an IRD which is responsive to a transmitted program guide for selecting signal packets of PC-data. The IRD temporarily stores the selected PC-data. Authorized PC-data will include a certificate. A PC-data processor is configured to separate the certificate and to check it for authenticity. The processor hashes portions of the PC-data and compares the generated hash values with hash values transmitted with the PC-data and corresponding to the same portions of PC-data. If the hash values are identical and the certificate is authentic, the system is conditioned to execute the transmitted program.

Rohatgi at 1:48-59; *see also* Abstract, 17:3-7, Figs. 10, 11.

This concept is also rendered obvious by the teachings of, at least, Gennaro at 5:54-63:

The MD5 hash of the recently arrived block is compared against what it should be according to the authentication chain emanating from the Digital Signature from (1.20). If it is different, then tampering has been detected and processing halted. Otherwise, the MPEG software/hardware is informed that a block of bits of a certain size representing a frame has arrived and it can proceed to process the incoming original block that was authenticated.

Gennaro at 5:54-63.

This concept is also rendered obvious by the teachings of, at least, Stefik '980 at 7:19-33:

Assuming that a session can be established, Repository 2 may then request access to the Digital Work for a stated purpose, step 104. The purpose may be, for example, to print the digital work or to obtain a copy of the digital work. The purpose will correspond to a specific usage right. In any event, Repository 1 checks the usage rights associated with the digital work to determine if the access to the digital work may be granted, step 105. The check of the usage rights essentially involves a determination of whether a right associated with the access request has been attached to the digital work and if all conditions associated with the right are satisfied. If the access is denied, repository 1 terminates the session with an error message, step 106. If access is granted, repository 1 transmits the digital work to repository 2, step 107.

Stefik '980 at 7:19-33; *see also* Fig. 1, 6:37-50, 42:25-43:5.

Other example disclosures are included in the attached charts of Appendix C. Accordingly, granting the request to use the file in the predefined manner was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the '815 Patent to include such functionality in combinations for the reasons discussed above including, for example, that doing so would be applying a known technique to other digital rights management and cryptographic systems to achieve the same result.

d. Motivations to Combine Prior Art for the '602 Patent

Motivations to combine any of the prior art references identified herein for the '602 Patent with one another exists within the references themselves, as well as within the knowledge of those of ordinary skill in the art at the relevant time.

(1) Technical incentives and market forces drove similar solutions in the prior art.

Regarding the '602 Patent, many of the identified prior art references address the same technical issues and suggest similar solutions in the field of data authentication. Indeed, the need for an effective method to authenticate data is a problem already recognized in the prior art and the field of the invention and would provide a person of ordinary skill in the art motivation to combine the prior art references identified above. The '602 Patent "relates to systems and methods for authenticating and protecting the integrity of electronic information using cryptographic techniques." '602 Patent at 1:39-42. Like the '602 Patent, Preneel notes at 1:21-33 that "Hash functions play a fundamental role in modern cryptography" and "[o]ne main application is their use in conjunction with digital signature schemes; another is in message authentication." Barton notes at 4:5-15 in 1994 that "[i]t would be a significant advance in the art of electronic distribution if digital information could be secured against unauthorized use or copying, for example by providing a tamper proof authentication scheme." Barton notes in 1:53-64 regarding the

authentication problem that "'Authentication' refers to techniques that are used to avoid the problem of electronic tampering and similar problems" including "know[ing] with assurance that the object originated with the proper source," such as "that a movie came directly from the studio," and that having "assurance that the object has not been modified in some way," such that "the movie is the same one paid for, with all portions intact." As a further example, Ehrsam describes as early as 1975 that "[v]arious cryptographic arrangements have been developed in the prior art for maintaining the security and privacy of data transmissions between a sending station and a receiving station."

Here, regarding the '602 Patent, market forces demanded that authentication capability be improved to allow distribution of data in a manner that allows authentication of the distributed data. Thus one of skill in the art would have been motivated to combine or modify references using known methods that one of skill in the art would have recognized as offering improvements to solutions of that time. The references identified describe methods that were known to offer improvements, and, accordingly, one of skill in the art would have been motivated to combine or modify combined references to include such improvements.

(2) Combination of known elements yields predictable results.

Because the Asserted Claims of the '602 Patent simply arrange old elements known in the field of message communications, with each performing the same function it had been known to perform, and yields no more than what one would expect from such an arrangement, combinations of the prior art are obvious. At the time of the alleged invention of the '602 Patent, there were a finite number of predictable solutions for authenticating data, including the use of check values and framing of data with corresponding check values, a person of ordinary skill in the art had good reason to pursue and/or combine known options and related applications.

Moreover, the alleged invention of the ’602 Patent is built upon technology that significantly pre-dates the alleged conception date. In-band embedding of information, such as a check value, for authentication was well-known as described, for example, in Barton at 2:9. Computation of hash values for use as check values was well-known as described, for example, in Schneier.

A person of ordinary skill in the art having knowledge of the data authentication techniques described in the references listed above, among other things, would be motivated, taught, and suggested to combine the prior art as identified above. Further, motivation exists because the patents and articles all are commonly related and are from the same field of art, and a person of ordinary skill in the art would draw equally from the field of art to solve the problem allegedly presented in the ’602 Patent. The suggested combinations reflect at least combinations of prior art elements according to known methods to yield predictable results, simple substitutions of known elements to obtain predictable results, and combinations that are obvious to try. Further elaboration and information shall be provided with Defendants’ expert reports.

(3) Exemplary prior art combinations

As discussed above, Appendix D sets out the references that disclose each element of the Asserted Claims of the ’602 Patent and Defendants contend that it would have been obvious to modify such references to include any allegedly missing element, in view of the knowledge of one of ordinary skill in the art, the admitted prior art of the ’602 Patent, and/or in combination with any of the other prior art references identified in the ’602 Patent. By way of example, and without limitation, Defendants provide the following exemplary combinations for particular claim limitations based on teachings of the cited prior art references. Defendants reserve the right to rely upon any combination of prior art references whether listed herein or otherwise.

Claims [602.25a] – Progression of Check Values

To the extent a reference does not expressly or inherently disclose a "progression of check values, each check value in the progression being derived from a portion of the block of data and from at least one other check value in the progression," it would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the '602 Patent to do so because doing so was one of a finite number of known ways to compute hash values. For example, Preneel teaches at 2:54-64 that "an iterated hash function operation" is useful for "data encryption and authentication." Figure 2 and 4:15-26 of Preneel describe the generation of a progression of check values, and in particular hash values as check values, according to the function: "H_0 =IV (initialization value); $H_i = f(H_{i-1}, X_i), 1 \leqq i \leqq t$; $h(X)=H_t$." In fact, Preneel states at 4:8-14 that "[m]ost hash functions, including MACs, are designed as iterative processes." As another example, Erickson describes the use of "nested error checking methods." As a further example, Ehrsam at 2:33-35 discloses a progression of check values used such that "each succeeding ciphered data block [is] chained to all preceding cycles of operation." Other example disclosures are included in the attached charts of Appendix D. The use of iterative check values or a progression of check values improves the ability to authenticate the data by reducing the likelihood of the check values being replicated by a third party.

Accordingly, the use of a progression of check values for authenticating data was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the '602 Patent to include such functionality in combinations for the reasons discussed above including, for example, that doing so would be applying a known technique to other authentication techniques.

Claim [602.25b] – Check Values Inserted in Proximity to Corresponding Blocks of Data

To the extent a reference does not expressly or inherently disclose "error-check value being inserted in proximity to a portion of the block of data to which it corresponds," this limitation is rendered obvious by the teachings of, at least, Tanenbaum at P. 184-85 describing that a "parity bit is appended to the data" as an example of "include[ing] enough redundant information along with each block of data." Tanenbaum provides one example that "when 10110101 is sent in even parity by adding a bit at the end, it becomes 101101011." As another example, Erickson describes at 3:30-60 that "a subset of the error checkword is appended to the end of each frame to form a transmission block." Erickson illustrates an example in figure 4 and describes at 4:31-30 that "FIG. 4 shows a data stream which has been broken into data frames and error detection bits inserted. The data stream has been divided into N frames, with a checkword subset CW1 through CWn inserted after every frame." As a further example, Gennaro describes "a software component for adding ancillary information to each of the original blocks to form a combined block for each original block, where said ancillary information is used to authenticate at least one of said original blocks of said original stream." Other example disclosures are included in the attached charts of Appendix D. The placement of check values in proximity to the data from which the check values were derived was well known and would improve communications by allowing portions of the data, e.g., individual packets or frames, to be processed prior to receipt of the entire data set.

The use of check values inserted in proximity to corresponding blocks of data was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the '602 Patent to include such functionality in combinations

for the reasons discussed above including, for example, that doing so would be applying a known technique to other data authentication techniques to achieve the same result.

Claims [602.25d] – Receiving and authenticating portions of the encoded block of data before the entire encoded block of data is received

To the extent a reference does not expressly or inherently disclose authenticating portions of data before receiving the entire block of data, this recitation is rendered obvious by the teachings of, at least, Gennaro. Gennaro teaches that a "receiver [of a stream] must consume the data it receives at more or less the input rate, ie., it can't buffer large amounts of unconsumed data" and that "in many applications the receiver stores relatively very small amounts of the stream." Gennaro provides example applications including "digitized video and audio" and notes that "the receiver cannot be expected to receive the entire stream before verifying" the data. Gennaro describes a solution as "split[ing] the stream in[to] blocks" in which "[t]he sender signs each individual block and the receiver loads an entire block and verifies its signature before consuming it" such that "the sender [is forced] to generate a signature for each block of the stream and the receiver to verify a signature for each block." Other example disclosures are included in the attached charts of Appendix D.

Accordingly, the authentication of data before receiving the entire stream of data was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the '602 Patent to include such functionality in combinations for the reasons discussed above including, for example, that doing so would be applying a known technique to other authentication techniques to achieve the same result.

Claims [602.25e] – Hash Values

To the extent a reference does not expressly or inherently disclose using a hash value for authenticating data as required by the recitation that "each error-check value comprises a hash of the portion of the block of data to which it corresponds," this recitation is rendered obvious by the teachings of, at least, Preneel. Preneel teaches at 1:21-33 that "[h]ash functions play a fundamental role in modern cryptography" and at 1:60-65 that "[s]uch hash functions … have received widespread use in practice for data integrity and data origin authentication." Additionally, Schneier (Applied Cryptography, 2d ed) teaches that a hash value is one example of a check value that can be used for authentication at P. 30 (§ 2.4) that "[a] one-way hash function has many names: compression function, contraction function, message digest, fingerprint, cryptographic checksum, message integrity check (MIC), and manipulation detection code (MDC)." The '602 Patent itself acknowledges at 2:2-5 that in prior art [m]any cryptographic signature schemes are based on public key cryptography" in which "a party creates a signature by applying a strong cryptographic hash algorithm (e.g., SHA-1)." The use of hash functions was well known in cryptography and message authentication for verifying data. Common hash functions that predated the '602 Patent include the MD4 (disclosed in RFC1320) and the MD5 (disclosed in RFC1321). Other example disclosures are included in the attached charts of Appendix D. Hash values are well-known in the art for being difficult to replicate and thus the use of such hash values improves the likelihood of the authenticity of the content.

Accordingly, the use of a hash function for authenticating data was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the '602 Patent to include such functionality in combinations for the reasons

discussed above including, for example, that doing so would be applying a known technique to other authentication techniques to achieve the same result.

Claims [602.26a] – Check Value Comprises a Hash of a Combination of Data Elements

To the extent a reference does not expressly or inherently disclose "each check value in the progression compris[ing] the hash of a combination of at least (i) a hash of the portion of the block of data to which it corresponds, and (ii) another check value in the progression," this limitation is rendered obvious by the teachings of, at least, Kaufman and other example disclosures included in the attached charts of Appendix D.

The computation of a hash value of user data was well known, as were the benefits. For example, U.S. Pat. Publ. No. 2002/0164026 describes at [0012] that "[t]he use of a double hash function is particularly advantageous in providing a secure method of communication" and WO97/24675 at 8:9-13 discloses "[t]he hashed value generated at the output of function 306 is fed to a second MD2 hash function 308 which implements a second MD2 hash function and provides a second hashed value at an output port thereof." In addition, Kaufman shows that it was also known to compute a hash of the combination of 1) a previously computed hash and 2) additional data. As Kaufman explains, this provides increased security because it can help address two potential vulnerabilities. First, the server's database could be compromised (7:11). Additionally, an eavesdropper could intercept communications between a user and the server (7:23-24). Kaufman describes a solution, based on computing a hash of a combination of a hash and other information, that "provides protection against a compromise of the server database coupled with an eavesdropping on an authentication exchange" (9:9-11). Thus, a person of ordinary skill understood that, relative to only performing a single hash, there were additional advantages

obtainable by using a previously computed hash as the input to a process that performs a hash of a combination of a previous hash and other information.

Kingdon provides further evidence regarding knowledge among persons of skill in the art regarding performing a hash of an input that includes the output of a previous hash. For example, Claim 26 of Kingdon recites:

> A method of generating a session key, in a computer system comprising the steps of:
> providing a random number sequence;
> requesting a password from a user;
> creating a first hash from said password;
> combining said first hash and said sequence;
> creating a second hash of said combined first hash and sequence; and
> defining a session key as a portion of said second hash.

Thus, Kingdon discloses performing a hash (in this instance, of a password), combining that hash with a sequence, and then performing a hash of the combination of the first hash and the sequence.

Thus, the hash of a hash value, such as recited in claim 26, results in a higher degree of certainty of authenticity of the message attached to the check values. The choice of the check value to combine with the hash of the data and hashing of the result would be an obvious selection of available values to improve likelihood of authenticity of the message. When seeking to improve authenticity of a message by decreasing an ability to attack the check values, a person of ordinary skill in the art would seek to combine a value with a hash of the data block. Because the check value is already available, the use of the check value to combine with the hash of the data is an obvious choice that results in little increase in processing time. The use of a hash value in a checksum as recited in claim 26 is thus well-known, and it would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the ’602 Patent to include such functionality in combinations for the reasons discussed above including, for example, that

doing so would be applying a known technique to other authentication techniques to achieve the same result.

e. Motivations to Combine Prior Art for the '603 Patent

Motivations to combine any of the prior art references identified herein for the '603 Patent with one another exists within the references themselves, as well as within the knowledge of those of ordinary skill in the art at the relevant time.

(1) Technical incentives and market forces drove similar solutions in the prior art.

Regarding the '603 Patent, many of the identified prior art references address the same technical issues and suggest similar solutions in the field of securing electronic media content from unauthorized use. Indeed, the need for an effective digital rights management is a problem already recognized in the prior art and the field of the invention and would provide a person of ordinary skill in the art motivation to combine the prior art references identified above. Although copying of analog content was a problem, the problem was restrained by the inability to create a high-quality duplicate. In contrast, Imai describes at 1:15-39 that "a copying of the writing data offered electronically is neither costly nor time consuming, and a quality of the data is hardly deteriorated" such that "an unauthorized duplication can be just as good as the original in a case of the electronically offered writing data." Imai recognized at 4:23-29 a need for "a sophisticated input/output management to permit only a reading or a displaying on a display device and prohibit a copying for the specified data such as electronic writing data, while enabling normal data output for data other than the specified data." Schneck echoes a similar problem and need at 1:14-3:30 that the "inevitable gradual degradation of quality [of analog copies] has proven to be a practical disincentive to large scale copying of analog information" but that "[a] digital file can be copied with no loss of fidelity." Schneck concludes that "[t]he uncertainty of legal protection over time

and from country to country only serves to emphasize the importance of and need for technical protection of intellectual property rights in information and data." Other examples are provided in the charts attached as Appendix E.

Here, regarding the '603 Patent, market forces demanded that protection of electronic media content be improved to meet the increasing threat presented by developments of computer networks and digitization of information that threatened digital content owner's intellectual property rights. Thus one of skill in the art would have been motivated to combine or modify references using known methods that one of skill in the art would have recognized as offering improvements to solutions of that time. The references identified describe methods that were known to offer improvements, and, accordingly, one of skill in the art would have been motivated to combine or modify combined references to include such improvements.

(2) Combination of known elements yields predictable results.

Because the Asserted Claims of the '603 Patent simply arrange old elements known in the field of digital rights management, with each performing the same function it had been known to perform, and yields no more than what one would expect from such an arrangement, combinations of the prior art are obvious. At the time of the alleged invention of the '603 Patent, there were a finite number of predictable solutions for protecting electronic media content, including protection by evaluating a software module that processes the electronic media content such as described in Grecsek identified by the Examiner during prosecution of the patent application leading to the '603 Patent cited in the Non-Final Rejection of November 28, 2005, a person of ordinary skill in the art had good reason to pursue and/or combine known options and related applications.

Moreover, the alleged invention of the '603 Patent is built upon technology that significantly pre-dates the alleged conception date. The processing of electronic media content

and denying access when the processing device is not secure was well known, such as described in the Imai at 12:60-13:13 and in other charts in the attached Appendix E. Likewise, evaluation of whether electronic media content is only output to certain secure channels is well known, such as described in Imai at 23:43-53 and in other charts in the attached Appendix E.

A person of ordinary skill in the art having knowledge of the electronic media content protection described in the references listed above, among other things, would be motivated, taught, and suggested to combine the prior art as identified above. Further, motivation exists because the patents and articles all are commonly related and are from the same field of art, and a person of ordinary skill in the art would draw equally from the field of art to solve the problem allegedly presented in the '603 Patent. The suggested combinations reflect at least combinations of prior art elements according to known methods to yield predictable results, simple substitutions of known elements to obtain predictable results, and combinations that are obvious to try. Further elaboration and information shall be provided with Defendants' expert reports.

(3) Exemplary prior art combinations

As discussed above, Appendix E sets out the references that disclose each element of the Asserted Claims of the '603 Patent and Defendants contend that it would have been obvious to modify such references to include any allegedly missing element, in view of the knowledge of one of ordinary skill in the art, the admitted prior art of the '603 Patent, and/or in combination with any of the other prior art references identified in the '603 Patent. By way of example, and without limitation, Defendants provide the following exemplary combinations for particular claim limitations based on teachings of the cited prior art references. Defendants reserve the right to rely upon any combination of prior art references whether listed herein or otherwise.

Claims [603.01b] – Identifying Software Modules for Processing Content

To the extent a reference does not expressly or inherently disclose a "identifying one or more software modules responsible for processing the piece of electronic media content," it would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the '603 Patent to do so because doing so was one of a finite number of known ways to process electronic media content. For example, Griswold describes at 5:19-32 the use of different functional portions for processing respective associated data portions. As another example, file associations between file types and particular applications (e.g., software modules) for processing the files of a file type were well known and incorporated into operating systems such as Windows 3.1 and Windows 95. In a further example, WO1997/025798 describes at 28:21-24 that "[t]he display or output devices used will depend on the application and the type of data, and include, but are not limited to, printers, video display monitors, audio output devices, and the like." As another example, U.S. Pat. No. 5,731,813 at 3:24-25 describes "creat[ing] associations between application programs and files." Other example disclosures are included in the attached charts of Appendix E. When a request for content was received, a person of ordinary skill in the art would understand that the operating system or device would identify a software module for processing the content based on, e.g., the file association or meta-data stored with the content. The identification of a software module for processing the content as described in these references improves the user's experience by allowing playback of the content.

Accordingly, the identification of software modules for processing content was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the '603 Patent to include such functionality in combinations

for the reasons discussed above including, for example, that doing so would be applying a known technique to other authentication techniques.

Claim [603.01c] – Processing Electronic Media Content

To the extent a reference does not expressly or inherently disclose "processing at least a portion of said piece of electronic media content using at least one of the one or more software modules" and "evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner," this limitation is rendered obvious by the teachings of, at least, Griswold. For example, Griswold describes at 4:23-29 that "[a]fter a request datagram has been sent out, a user may be permitted to use the licensed product for a limited duration" and at 11:55-62 that "[t]he presently described embodiment allows the licensee to access the licensed product concurrent with the sending and receiving of datagram 3." Other example disclosures are included in the attached charts of Appendix E. A person of ordinary skill in the art would understand that the processing of content by a software module and the evaluation of that software module would improve the rights management by, e.g., preventing changes in system configurations from allowing the content to be redirected to an unauthorized data channel.

The processing of electronic media content using a software module prior to evaluating the software module was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the '603 Patent to include such functionality in combinations for the reasons discussed above including, for example, that doing so would be applying a known technique to other electronic media content systems.

Claims [603.01d] – Evaluation of a Software Module

To the extent a reference does not expressly or inherently disclose the particular manners of evaluation of software modules as required by the recitation of "evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner, the evaluating including at least one action selected from the group consisting of: evaluating whether the at least one of the one or more software modules make calls to certain system interfaces; evaluating whether the at least one of the one or more software modules direct data to certain channels; analyzing dynamic timing characteristics of the at least one of the one or more software modules for anomalous timing characteristics indicative of invalid or malicious activity," these limitations are rendered obvious by the teachings of, at least, Imai. Imai teaches at 23:43-53 that output of files should only be permitted to certain data channels (e.g., permitted output targets). Other example disclosures are included in the attached charts of Appendix E.

Accordingly, the evaluation of software modules according to the claimed techniques was well-known in the art, and it would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the '603 Patent to include such functionality in combinations for the reasons discussed above including, for example, that doing so would be applying a known technique to other electronic media content protection systems to achieve the same result.

f. Motivations to Combine Prior Art for the '342 and '106 Patents

Motivations to combine any of the prior art references identified herein for the '342 and the '106 Patents with one another exists within the references themselves, as well as within the knowledge of those of ordinary skill in the art at the relevant time.

(1) Technical incentives and market forces drove similar solutions in the prior art.

Regarding the '342 and the '106 Patents, many of the identified prior art references address the same technical issues and suggest similar solutions in the field of content protection. The need for protecting the interests of content owners and ensuring the integrity of electronic transactions through improved security and authentication when distributing electronic content, is a problem already recognized in the prior art and the field of the invention and would provide a person of ordinary skill in the art motivation to combine the prior art references identified above. More specifically, problems that existed in the context of receiving and rendering electronic content, including receiving, using, and verifying digital certificates, rules, conditions, and other authorizing documents, and associated solutions were well known in the prior art.

For example, like the '342 and the '106 Patents, Downs describes the limitations of existing systems due to the increased use of the Internet for distribution of "digital assets such as music, film, computer programs, pictures, games and other content" and that content owners and publishers are "are afraid of unauthorized copying or pirating of digital content." *See* Downs at 1:59-66. As noted by Downs:

> Providers of digital content desire to establish a secure, global distribution system for digital content that protects the rights of content owners. The problems with establishing a digital content distribution system includes developing systems for digital content electronic distribution, rights management, and asset protection.
>
> . . .
>
> Therefore a need exists for a secure digital content electronic distribution system that provides protection of digital assets and ensures that the Content Provider (s) rights are protected even after the digital content is delivered to consumers and businesses. A need thus exists for rights management to allow for secure delivery, licensing authorization, and control of the usage of digital assets.

Downs at 2:26-3:6.

As another example. Stefik '340 describes the desire for content owners to restrict what a user can do with distributed digital content, but is faced with the dilemma that the "content owner

has very little if any control over the digital content." *See* Stefik '340 at 1:57-2:11. Stefik '340 proposes a solution that mirrors the '342 and the '106 Patents that includes "providing an enforcement architecture and method that allows the controlled rendering or playing of arbitrary forms of digital content, where such control is flexible and definable by the content owner of such digital content," and "a trusted component running on the computing device, where the trusted component enforces the rights of the content owner on Such computing device in connection with a piece of digital content,." Stefik '340 at 3:30-53.

Additional references provide similar solutions in the context of controlling electronic content in networked distribution systems:

- A "VDE [virtual distribution environment] is the first general purpose, configurable, transaction control/rights protection solution . . . [addressing] [a] fundamental problem for electronic content providers [ ] extending their ability to control the use of proprietary information. Content providers often need to limit use to authorized activities and amounts. Participants in a business model involving, for example, provision of movies and advertising on optical discs may include actors, directors, script and other writers, musicians, studios, publishers, distributors, retailers, advertisers, credit card services, and content end-users. These participants need the ability to embody their range of agreements and requirements, . . . This extended agreement is represented by electronic content control information that can automatically enforce agreed upon rights and obligations." Ginter at 2:26-47.

- "A need exists, then, for providing an enforcement architecture and method that allows the controlled rendering or playing of arbitrary forms of digital content, where such control is flexible and definable by the content owner of such digital content. A need also exists for providing a controlled rendering environment on a computing device Such as a personal computer, where the rendering environment includes at least a portion of such enforcement architecture. Such controlled rendering environment allows that the digital content will only be rendered as specified by the content owner, even though the digital content is to be rendered on a computing device which is not under the control of the Content Owner." England 432 at [0008]; *see also* Peinado at 2:30-43.

- "What is needed is a mechanism by which copyrightable content of digital Storage media is protected against unauthorized copying while affording the owner of such digital storage reasonable unimpeded convenience of use and enjoyment of the content." Ansell at 2:21-25.

- "Therefore, there is a need in the art for a digital rights management operating System that enforces digital rights on content downloaded from a provider while operating on a general purpose personal computer without the need of specialized or additional hardware." England 063 at 3:57-61.

- "The present invention is directed to a digital content file including a license control mechanism and a system and method for distributing licensable digital content files, pro viding licenses for digital content files, and controlling the licensed use of digital content." Doherty at 3:58-61.

- "With the growing number of data rights management architectures, content types, consumers and the amount of content available, granting access to protected content has become a very difficult task. Incompatible data rights management architectures make commercial distribution of rights to protected content difficult. In particular, management of transactions, tracking and auditing of rights to content becomes very difficult. . . . Accordingly, what is needed is a system and method to integrate multiple, incompatible data rights management architectures that allow access rules to content to be defined outside the container." Lockhart at 3:16-33

- "[T]here is a need for an improved digital rights management System that allows of delivery of electronic works to purchasers in a manner that protects ownership rights, while also being flexible and easy to use. There is also a need for the system that provides flexible levels of security protection and is operable on several client platforms Such that electronic content may be viewed/ rendered by its purchaser on each platform. The digital rights management system of the present invention advantageously provides solutions to the above problems which protect the intellectual property rights of content owners and allow for authors or other content owners to be compensated for their creative efforts, while ensuring that purchasers are not over-burdened by the protection mechanism." DeMello at 1:56-2:2.

Here, regarding the '342 and the '106 Patents, market forces demanded that electronic content distribution systems included mechanisms to control distribution and use of the electronic content, such as digital certificates, rules, conditions, and other authorizing documents. Thus one of skill in the art would have been motivated to combine or modify references using known methods that one of skill in the art would have recognized as offering improvements to solutions of that time. The references identified describe methods that were known to offer improvements, and, accordingly, one of skill in the art would have been motivated to combine or modify combined references to include such improvements.

(2) Combination of known elements yields predictable results.

Because the Asserted Claims of the '342 and '106 Patents simply arrange old elements known in the field of electronic content distribution systems, with each performing the same function it had been known to perform, and yields no more than what one would expect from such an arrangement, combinations of the prior art are obvious. At the time of the alleged invention of the '342 and the '106 Patents, there were a finite number of predictable solutions for electronic content distribution systems, including the use of digital certificates, rules, conditions, and other authorizing documents, a person of ordinary skill in the art had good reason to pursue and/or combine known options and related applications.

Moreover, the alleged invention of the '342 and the '106 Patents Patent is built upon technology that significantly pre-dates the alleged conception date, namely digital certificates. ITU-T X.509 digital certificate standards were first published in 1988. *See* RFC 2459 at 9. The prior art describes the functionality of X.509 digital certificates, as well as numerous systems and methods that build upon or use the X.509 digital certificate protocol. *See, e.g.*, Ginter at 226:21-25; Elgamal 390 at 30:16-21; Elgamal 279 at 16:18-19, 20:36-43; Weinstein at 17:1-7; Ansell at 5:31-39, 8:38-41; England 063 at 18:34-38. The X.509 digital certificate protocol was one protocol available to a person of ordinary skill in the art at the time of the alleged invention, and a person of ordinary skill in the art may draw on this protocol to implement an electronic content distribution system such as that described in the alleged invention of the '342 and '106 Patents.

In addition to the X.509 digital certificates, and associated rules, conditions, encryption, and signatures, being well established in the art, the concept and implementation of rendering digital content on a user's computing device, was well known. *See* SDMI at 11, 13, 19; England

432 at Abstract; Stefik ’684 at Abstract; Peinado at Abstract; England ’063 at claim 9; Lockhart at 15:23-31.

A person of ordinary skill in the art having knowledge of the prior art, electronic content distribution systems including digital certificates, rules, conditions, and authorizing documents, among other things, would be motivated, taught, and suggested to combine the prior art as identified above. Further, motivation exists because the patents and articles all are commonly related and are from the same field of art, and a person of ordinary skill in the art would draw equally from the field of art to solve the problem allegedly presented in the ’342 and ’106 Patents. The suggested combinations reflect at least combinations of prior art elements according to known methods to yield predictable results, simple substitutions of known elements to obtain predictable results, and combinations that are obvious to try. Further elaboration and information shall be provided with Defendants’ expert reports.

(3) Exemplary prior art combinations

As discussed above, Appendices F-Combination and I-Combination set out the references that disclose each element of the Asserted Claims of the ’ ’342 and ’106 Patents, respectively, and Defendants contend that it would have been obvious to modify such reference to include the allegedly missing element, in view of the knowledge of one of ordinary skill in the art, the admitted prior art of the ’342 and ’106 Patents, and/or in combination with any of the other prior art references identified in the ’342 and ’106 Patents. By way of example, and without limitation, Defendants provide the following exemplary combinations for particular claim limitations based on teachings of the cited prior art references. Defendants reserve the right to rely upon any combination of prior art references whether listed herein or otherwise.

Claim [342.1a] “the first digital certificate being generated by or on behalf of a first entity comprising an association of one or more content providers, the first digital certificate being associated with the application program if the application program

meets certain predefined criteria set by the association, the predetermined criteria including that the application program will handle the electronic content with at least a predefined level of security"

To the extent a reference does not expressly or inherently disclose that the first entity comprises an association of one or more content providers and the first digital certificate is associated with the application program if it meets certain predefined criteria set by the association these limitations are rendered obvious by the teachings of, at least, SDMI. The Secure Digital Music Initiative is an association known at the time of the '342 and '106 Patents. The members of the association consist of over 120 companies and organizations including members of the recording industry. SDMI discloses that an application is SDMl-Compliant if it conforms to the requirements set forth in the specification published by the members of the Secure Digital Music Initiative and content can only be rendered by an application meeting these requirements. SDMI at 6-8.

Likewise, Doherty teaches "a license control mechanism for controlling the licensed use of digital content of the digital content file to user systems." Doherty at 8:7-36. An eLicense is generated by a publisher and includes a unique system ID ("SID") 66 and an associated Security Code 74 defined by the publisher (association of one or more content owners):

> In further detail, therefore, the remote eLicense acquisition method is comprised of the steps:
>
> (a) The LMCM 18 calls the AFSM 72, which generates a SID 66 fingerprint that the LMCM 18 encrypts and combines into a Request Identifier (ReqID) 88 with date and instance information.
>
> (b) A LicReq 86 is constructed that includes a RequestID 88, the ProdID 80, read from embedded code or the wrapper of the FACM 12, and an OrderID 58, which may be pre-configured by the publisher or generated automatically as part of an e-commerce transaction.
>
> (c) The LicReq 86 is sent via the DeLMM 40 to the LicGen 76, for example, through an Intranet or Internet communication and a standard, secured HTTP protocol.
>
> (d) The OrderID 58 and ProdID 80 are used by the LicGen 76 to identify the ParTemp 78 assigned by the publisher for the requested license and conditions of acquisition.

(e) An eLicense is created by passing to the LicGen 76 the inputs
ProdID 80;
License type;
Security Code 74;
Adapt 84;
Expiration data;
Execution count limit;
Hours of use limit;
Custom control codes; and
SID 66, as extracted from the ReqID 88.

(f) The LicGen 76 returns an encrypted ACSII string which contains the requisite license data, that is, an ELDP 82, and a message containing the ELDP 82 is constructed and returned to the requesting system.

(g) Upon receiving the ELDP 82, the LMCM 18 and eLCU 20 call the AFSM 72, and the current SID 66 and the SID 66 contained in the eLicense data are compared. If they are the same, then the process will proceed. If they differ, then the Adapt 84 setting in the eLicense data is checked to see if the difference is within allowable limits. If it is, then the process will proceed.

(h) The Security Code 74 in the eLicense data is validated against the Security Code 74 in the DCF 10 on the host system, which may be embedded in the DCF 10 code or embedded within the FACM 12 wrapper.

(i) The ELDP 82 data is written to the Dldb 14, and the DCF 10 is fully licensed on the user system according to the limits and behavior set by the publisher.

Doherty at 30:47-31:27.

Downs teaches a digital content distribution system that includes "End-User Device(s) 109 [that] can be any player device that contains an End-User Player Application 195 (described later) compliant with the Secure Digital Content Electronic Distribution System 100 specifications." Downs further describes:

> [T]he Electronic Digital Content Store(s) 103 has downloaded the End-User Player Application 195 to an End-User Device(s) 109 based on standard Web protocols. The architecture requires that the Electronic Digital Content Store(s) 103 assigns a unique application ID to the downloaded Player Application 195 and that the End-User Device(s) 109 stores it for later application license verification (see below).

Downs at 23:21-28. The Electronic Digital Content Store(s) 103 market the Content 113 from Content Provider(s) 101, and are entities such as "[w]eb sites that provide electronic downloads of software." Downs at 9:61-10:35.

England 063 teaches a rights manager certificate 210 that is provided by "an operating system vendor, content provider, or third party, certifying the properties of the application" and also provides a rational for ensuring an application program meets security requirements:

> Most operating systems do not directly process media content, such as video or audio. That function is usually available through special application programs. Therefore, a content provider must not only trust the operating system but must also trust the application that will process the content. Content also can be accompanied by a predicate stating which applications are to be trusted to access that content, and this statement can include a list of generic properties that implicitly define a set of applications. Further associating a rights manager certificate with the application provides identification of the application and certification of its properties. This allows the content provider to determine if the application fulfills the requirements of the content provider before downloading content, and also allows the operating system to restrict future access to only the appropriate applications.
>
> One exemplary embodiment of rights manager certification is shown in FIG. 9. A list of application properties 903 is appended to the digital certificate fields 901 standard in some digital certificate format such as X.509. The certificate names the application. Each entry 905 in the list 903 defines a property 906 of the application, along with optional arguments 907. For example, one property might be that the application cannot be used to copy content. Another example of a property is one that specifies that the application can be used to copy content, but only in analog form at 480P resolution. Yet another example of a property is one that specifies that the application can be used to copy content, but only if explicitly allowed by an accompanying license. Additional examples include the right to store an encrypted copy of the content and to restrict such storage to only certain, acceptable peripheral devices. The property 906 can also be used to specify acceptable helper applications, such as third-party multimedia processing stacks or other libraries, to be used in conjunction with the application named in the certificate. The certificate is signed by an operating system vendor, content provider, or third party, certifying the properties of the application.

England 063 at 18:18-55.

Thus, at least these prior art references, show that content providers are interested in security control of their content to the extent of even specifying what set of criteria an application must meet before being allowed to render the content. They also show that it was possible at the time the applicant's invention was made to do provide such control. In light of the above, it would have been obvious for one of ordinary skill in the art at the time of the '342 and '106 Patents to

further modify a digital content distribution system. One of ordinary skill would have been motivated to do so at least because it would allow content providers to have better security and control over their contents.

Claim [342.1f] – "the piece of electronic content comprises an authorizing document, and the second entity associates the second digital certificate with the authorizing document if the authorizing document originated from a certified entity"

To the extent a reference does not expressly or inherently disclose that the electronic content comprises an authorizing document and the second entity associates the second digital certificate with the authorizing document if the authorizing document originated from a certified entity, this limitation is rendered obvious by the teachings of, at least, England 063. England 063 teaches an application 209 requesting access to content 221. Content 221 is associated with access predicate 222 and license 223 generated by or on behalf of content provider 220. *See* England 063 at 9:26-10:36, 20:17-21. England 063 teaches that the access predicate 222 is an access control list (ACL) 1000:

> The required properties ACL 1000 contains a basic trust level field 1001, which specifies the minimum rights management functions that must be provided by any application wishing to process the content. These minimum functions can be established by a trade association, such as the MPAA (Motion Picture Association of America), or by the DRMOS vendor. A unique identifier is used to reference a list of the minimum functions. The minimum functions list can include CPU, DRMOS, and application specific requirements.

England 063 at 18:56-19:5.

DeMello teaches a digital content distribution system that provides eBooks and describes an order process that employs an encrypted blob generated by the retailer and a license provided by a fulfillment site:

> The receipt page may contain information "confirming" the order or thanking the user for his/her order, and also contains links (HTTP POST requests) for downloading each title purchased. For fully individualized titles (level 5), a client-side script populates the body of the POST with the activation certificate, via web commerce object 86. (E.g., web commerce object 86 is used to retrieve the

> activation certificate for provision to the retailer's site.) In one example, the activation certificate may be provided to the retailer web site, which then creates an HTTP request (i.e., a POST request) which includes an encrypted blob (i.e., in the body of the POST). The HTTP request (including the encrypted blob) is then rendered as a link at the client site, where the client clicks the link to download the purchased title (as described below). In this example scenario, the HTTP request and encrypted blob (which are generated by the retailer, who, preferably, is in privy with the fulfillment site) contains information that identifies the particular eBook to be provided to the purchaser, as well as information that demonstrates to the fulfillment site that the encrypted blob was generated by a retailer for whom the fulfillment site has agreed to fulfill eBook orders. Additionally, in the case of the purchase of level 5 titles, client side software adds the activation certificate to the body of the POST to allow the symmetric key of the eBook to be encrypted for use with readers activated to the user's persona.

DeMello at 13:42-67.

> Upon clicking on any of the links at step 206, the browser initiates a download from a download or "fulfillment" server specified in the receipt page. For individually sealed ("inscribed") copies, the download server adds the consumer's name (or other identifying information as determined by the retail site, such as the user's credit card number, a transaction ID, etc.) to the title meta-data and re-seals the symmetric key using the new cryptographic hash resulting from the new meta-data, which now includes such identifying information. (The particular information to be included is determined by the retailer and provided as part of the encrypted blob in the body of the POST.) For fully individualized copies (level 5) a license is generated and embedded in the LIT file, in addition to the bookplate being created. This license contains the symmetric key that encrypted the LIT file "sealed" with the public key in the activation certificate. When the download is complete (step 208), the download server logs the transaction and, on the client, the reader 92 may be launched automatically (step 210). The title may, at this time, be moved into local store/LIT store 98, or another folder or directory designated for the storage of eBook titles. Upon launch of the reader 92, the eBook may be opened to its cover page 100.

DeMello at 14:1-23

As such, he electronic content comprises an authorizing document and the second entity associates the second digital certificate with the authorizing document if the authorizing document originated from a certified entity, was well known and common practice in the art. Because of this, it would have been obvious to modify any electronic content distribution system so that the he electronic content comprises an authorizing document and the second entity associates the

second digital certificate with the authorizing document if the authorizing document originated from a certified entity. It would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the '342 and '106 Patents to include such functionality in combinations for the reasons discussed above including, for example, that doing so would be applying a known technique to other digital content distribution systems to achieve the same result.

Claim [342.12] – "verifying the association of the second digital certificate with the piece of electronic content is performed during or after the step of verifying the association of the first digital certificate with the application program"

To the extent a reference does not expressly or inherently disclose that verifying the association of the second digital certificate with the piece of electronic content is performed during or after the step of verifying the association of the first digital certificate with the application program, this limitation is rendered obvious by the teachings of, at least, England 063, Ansell, and Peinado. England 063 teaches an application 209 requesting access to content 221. The DRMOS 205 verifies the association of the rights manager certificate 210 for the application 209, and after trust is established, verifies the association of the access predicate 222 and license 223 with content 221. *See* England 063 at 9:26-10:36.

Similarly, Ansell teaches a method of processing passports during access and playback of that includes verifying the association of the first digital certificate with the application program before verifying the association of the second digital certificate with the piece of electronic content:

> In test step 1008, content player 142 determines whether a machine-bound passport is present. . . . On the other hand, if a machine-bound passport is present, processing transfers to step 1010 in which content player 142 verifies that hardware identifier 140 corresponds to the machine-bound passport in the manner described above with respect to steps 712 (FIG. 7) and 714. . . . Conversely, if verification is successful, processing transfers to step 1006.
>
> In step 1006, content player 142 attempts to playback the selected content. In test step 1012, content player 142 determines whether attempted playback is successful, i.e., whether the passport key successfully decodes the selected content. . . .

> If the selected passport key successfully decrypts the selected content, processing transfers to step 1014 in which content player 142 continues with playback of the selected content. At step 1014, the user and/or client computer system 104 have been authenticated as entitled to access the selected content.

Ansell at 18:9-50, Fig. 10.

Peinado teaches that verification of the first digital certificate with the application program can happen at any time, such as during verification of the association of the second digital certificate with the electronic content:

> The aforementioned process for approving a rendering application 34 or module 62 as is shown in FIG. 17 may be performed at any appropriate time without departing from the spirit and scope of the present invention. For example, the approval process may be performed during license evaluation as discussed above and shown in FIG. 6, or may be performed as part of path authentication as discussed above and shown in FIG. 15. Moreover, the approval process for the rendering application 34 may for example take place at a time different than for a module 62, if in fact any module is in fact to be approved in the manner shown in FIG. 17.

Peinado at 40:66-41:9, Figs. 6, 17.

As such, verification that an application is authorized to use content before allowing the application to use the content for any purpose, i.e., such as rendering content, was well known and common practice in the art. Because of this, it would have been obvious to modify any electronic content distribution system so that the verification of the association of the second digital certificate with the piece of electronic content must be performed after the step of verifying the association of the first digital certificate with the applications program. It would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the ’342 and ’106 Patents to include such functionality in combinations for the reasons discussed above including, for example, that doing so would be applying a known technique to other digital content distribution systems to achieve the same result.

Claim [106.17b] – "receiving, separately from the piece of electronic content, data specifying one or more conditions associated with rendering the piece of electronic content"

To the extent a reference does not expressly or inherently disclose receiving, separately from the piece of electronic content, data specifying one or more conditions associated with rendering the piece of electronic content, this limitation is rendered obvious by the teachings of, at least, Peinado, Downs, Doherty, and Ginter. Peinado teaches transmitting encrypted digital content 12 to a user's computing device (step 1809) (Peinado at 41:49-63) and separately "digital license 16 with such key (KD) may thereafter be so sent out to the requester's computing device 14 (step 1825)" (Peinado at 42:60-64, Fig. 18). Downs also teaches steps including "145 The License SC is then transmitted to the End-User(s)" and separately "148 Content 113 is sent to the end-User Device(s) 109. Upon the receipt the Content 113 is de-encrypted by the End-User Device(s) 109 using the Symmetric Key." Downs at 19:3-35, Figs 1A-1D, 6. Doherty teaches a trial period where a digital content file ("DCF") 10 is received and accessed and then a valid eLicense for the DCF 10 is requested and received separately. Doherty at 13:32-14:30.

Similarly, Ginter teaches "systems and methods for electronic commerce including secure transaction management and electronic rights protection" that includes a virtual distribution environment ("VDE"). Ginter at Abstract. Ginter teaches that "Content control information may be partially or fully delivered separately from its associated content to a user VDE installation" (Ginter at 17:48-51) and:

> VDE control information (e.g., methods) that collectively control use of VDE managed properties (database, document, individual commercial product), are either shipped with the content itself (for example, in a content container) and/or one or more portions of such control information is shipped to distributors and/or other users in separably deliverable "administrative objects."

Ginter at 43:21-28. Ginter further indicates that "VDE may be combined with, or integrated into, many separate computers and/or other electronic appliances. These appliances typically include a

secure subsystem that can enable control of content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc." Ginter at 9:13-22.

Accordingly, receiving, separately from the piece of electronic content, data specifying one or more conditions associated with rendering the piece of electronic content, was well known and common practice in the art. One of skill in the art would recognize that there were multiple reasons for separate delivery of data specifying one or more conditions associated with rendering the piece of electronic content including (1) the use of trial versions of content that are later fully licensed (Doherty at 13:32-14:30); (2) the need to provide licensing authorization to unlock content only after successful completion of a licensing transaction; and (3) allowing the electronic digital content infrastructure to not have to be secure or trusted in itself—"This is due to the fact that the Content is encrypted within Secure Containers and its Storage and distribution are separate from the control of its unlocking and use" (Downs at 7:11-31). It would have been obvious to one skilled in the art at the time of the alleged conception of the alleged invention of the '342 and '106 Patents to include such functionality in combinations for the reasons discussed above including, for example, that doing so would be applying a known technique to other digital content distribution systems to achieve the same result.

g. Motivations to Combine Prior Art for the '627 Patent

Motivations to combine any of the prior art references identified herein for the '627 Patent with one another exists within the references themselves, as well as within the knowledge of those of ordinary skill in the art at the relevant time.

(1) Technical incentives and market forces drove similar solutions in the prior art.

Regarding the '627 Patent, many of the identified prior art references address the same technical issues and suggest similar solutions in the field of digital rights management using decryption to access protected content. Indeed, the need for a content management system that safeguards digital works through the use of cryptographic techniques, and more generally, a need to employ a system that thwarts the pirating of such works, are problems already recognized in the prior art and the field of the invention and would provide a person of ordinary skill in the art motivation to combine the prior art references identified above.

For example, like the '627 Patent, Tripathy, at 1:56-58, recognizes that "for receivers which are connected to a network, the stored A/V content of a receiver may be vulnerable to surreptitious behavior, such as piracy." Tripathy elaborates on this vulnerability as follows:

> The media storing the A/V content may be connected to other circuitry by a bus. If the bus is open, e.g., accessible to other software or hardware, the A/V content may be copied.
>
> For example, some receivers may include a peripheral component interconnect, or PCI, bus. The PCI bus is compliant with the PCI Local Bus Specification, Revision 2.2 (Jun. 8, 1998, available from the PCI Special Interest Group, Portland, Oreg. 97214). The PCI bus is an open bus with well-known, publicly available specifications.
>
> Alternatively, the media of the receiver may be removable, such as those including a removable hard disk drive. With removable media, the stored A/V content may be sent to another receiver. Thus, for some receivers, the stored A/V content may be stolen.
>
> Further, for receivers which are connected to other receivers, the stored A/V content may be downloaded to another site without leaving evidence of having been downloaded. An entire network of receivers, for example, may potentially retrieve the stored content from a single paying site.

Tripathy at 1:58-2:10.

As another example, Morley '589 echoes Tripathy in its concern over the pirating of valuable digital properties likes movies, songs, and other copyrightable works. Morley '589 explains as follows:

> Because of the large number of duplicates made, it becomes increasingly difficult to prevent illegal duplication and theft of the material. It is estimated that revenues lost due to piracy and theft account for billions of dollars lost each year by the motion picture industry. Further, duplicated film material tends to degrade over time due to dust collection, wear-and-tear, thermal variances, and other known factors. Finally, management cost and other expenses are involved in the eventual destruction of the film material, which may contain regulated hazardous material….
>
> New digital cinema systems require improved forms of protection to prevent theft from theaters.

Morley '589 at 2:12-20 and 3:65-67.

Both Tripathy and Morley '589 describe solutions that mirror that of the '627 Patent: the use of decryption to safeguard valuable content against theft. Tripathy describes "A system for protecting audio/video content during storage and playback on systems with open buses receives a multiplexed signal, including a plurality of A/V signals and decryption keys." *Id*. at Abstract. According to Tripathy at 8:59-9:5:

> The descrambler 122 receives the single channel A/V signal 45 and the decryption keys signal 40 (block 320), from the transport demultiplexer memory regions 140 a and 140 b, respectively. The descrambler 122 uses the decryption keys 40 to descramble the channel signal 45, producing the descrambled signal 35. The descrambler 122 sends the descrambled signal 35 to the A/V decoder 112 (block 322). The A/V decoder 112 decompresses the signal 35, then separates out the video signal 30 and the audio signal 32 (block 324). The digital video signal 30 (or the analog video signal 34, depending on the display type) is sent to the video display 142 a while the audio signal 32 is sent to the speakers 142 b (block 326). The requested A/V channel is thus experienced (block 328).

Morley '589 describes its use of decryption for the protection of content at least at 20:49-21:9:

> The image decryptor/decompressor 320 takes the image data stream from depacketizer 316, performs decryption, and reassembles the original image for

> presentation on the screen. The output of this operation generally provides standard analog RGB signals to digital cinema projector 148. Typically, decryption and decompression are performed in real-time, allowing for real-time playback of the programming material. The image decryptor/decompressor 320 decrypts and decompresses the image data stream to reverse the operation performed by the image compressor 184 and the image encryptor 188 of the hub 102. Each auditorium module 132 may process and display a different program from other auditorium modules 132 in the same theater subsystem 104 or one or more auditorium modules 132 may process and display the same program simultaneously. Optionally, the same program may be displayed on multiple projectors, the multiple projectors being delayed in time relative to each other. The decryption process uses previously provided unit-specific and program-specific electronic cryptographic key information in conjunction with the electronic keys embedded in the data stream to decrypt the image information. (The decryption process has previously been described with reference to FIG. 4.) Each theater subsystem 104 is provided with the necessary cryptographic key information for all programs authorized to be shown on each auditorium module 132.

Thus, like the '721 Patent, both Tripathy and Morley '589 recognize that digital media content is vulnerable to theft via unauthorized duplication or other forms of piracy. Also like the '721 Patent, Tripathy and Morley '589 offer solutions in the form of respective content management systems that rely on cryptography to ensure that only authorized access to such content is executed.

Additional references provide similar solutions in the context of systems that protect content through the use of cryptography:

- When the program is to be played back, the theater or location specific and program specific keying information is used, preferably with a symmetric algorithm, that was used in encryption system 110 in preparing the encrypted signal to now descramble/ decrypt program information in real-time. Morley '335 at 7.

- In the illustrative embodiment, the exchange controller comprises an application program interface (API) that is distributed among user workstations (i.e., workstation APIs) and the authentication database (i.e., the database API) ; preferably, both the database API and authentication database reside in a network directory services (NDS) system. When the authentication inquiry is received from the program at the controller, the workstation API verifies that the user is a valid network client (i.e., has successfully logged-on and has been authenticated to the NDS) by requesting the proper application secret for that particular program. In

response to this request, the database API accesses the authentication database and provides the workstation with an encrypted application secret along with the private key for decrypting that secret. The workstation API then decrypts and forwards the proper secret (and user identity) to the particular application program. Mashayekhi at 3:54-4:3.

- Disk 100 may also store an encrypted key block 208. In this example, disk 100 may further store one or more hidden keys 210. In this example, encrypted key block 208 provides one or more cryptographic keys for use in decrypting one or more properties 200 and/or one or more metadata blocks 202. Key block 208 may provide different cryptographic keys for decrypting different properties 200 and/or metadata blocks 202, or different portions of the same property and/or metadata block. Thus, key block 208 may comprise a large number of cryptographic keys, all of which are or may be required if all of the content stored by disk 100 is to be used. Although key block 208 is shown in FIG. 3 as being separate from container 206, it may be included within or as part of the container if desired. Cryptographic key block 208 is itself encrypted using one or more additional cryptographic keys. In order for player 52 to use any of the protected information stored on disk 100, it must first decrypt corresponding keys within the encrypted key block 208—and then use the decrypted keys from the key block to decrypt the corresponding content. Shear at [0225]-[0226].

- The system further comprises a routing manager/decoder coupled to the transmitter for receiving and descrambling the scrambled signal. The decoder comprises first and second key decryptors and a descrambler. In the twice encrypted mode, the first key decryptor is coupled to the transmitter and performs a first key decryption on the twice-encrypted key using the second secret serial number and outputs a partially decrypted key. The second key decryptor is coupled to the first key decryptor and perform a second key decryption on the partially decrypted key using the first secret signal number and outputs the decrypted key. The descrambler is coupled to the second key decryptor and the transmitter and descrambles the scrambled signal using the decrypted key and outputs the descrambled signal. The decoder may function without the use of a replaceable security module. In the event of a system breach or a service level change, a replaceable security module may then be inserted into the decoder to "upgrade" the decoder. Gammie at 10:36-55.

- The client then uses the key to decrypt the personal security device and gain access to its contents (Step 530). In this embodiment, the key and the decrypted contents are stored in the client's volatile storage medium. In one embodiment, the key is a symmetric key and decryption is performed using a symmetric cipher. In an alternate embodiment, the key is a first asymmetric key of a key pair, the personal security device was encrypted with a second key of a key pair, and the decryption is performed using a public-key cryptographic cipher. FIG. 6 illustrates the hardware of an embodiment used to store and access a personal security device and its contents. The hardware includes a central processing unit ("CPU") 600 in operative association with volatile storage 610 and non-volatile storage 620. In this

embodiment, an encrypted personal security device 630 is stored in the non-volatile storage 610. When a user wishes to access the contents of the personal security device 630, a key 640 is stored in the volatile storage 610. The CPU 600 then uses the key 640 to decrypt the contents of the personal security device and store the decrypted contents 650 in the volatile storage 610. Duane at 11:4-25.

- For example, one or more VDE electronic appliances 600 can be used as input/output device(s) of a computer system. This may eliminate the need to decrypt information in one device and then move it in unencrypted form across some bus or other unsecured channel to another device such as a peripheral. If the peripheral device itself is a VDE electronic appliance 600 having a SPU 500, VDE-protected information may be securely sent to the peripheral across the insecure channel for processing (e.g., decryption) at the peripheral device. Giving the peripheral device the capability of handling VDE-protected information directly also increases flexibility. For example, the VDE electronic appliance 600 peripheral device may control VDE object 300 usage. It may, for example, meter the usage or other parameters associated with the information it processes, and it may gather audit trials and other information specific to the processing it performs in order to provide greater information gathering about VDE object usage. Providing multiple cooperating VDE electronic appliances 600 may also increase performance by eliminating the need to move encrypted information to a VDE electronic appliance 600 and then move it again in unencrypted form to a non-VDE device. The VDE-protected information can be moved directly to its destination device which, if VDE-capable, may directly process it without requiring involvement by some other VDE electronic appliance 600. Ginter ’987 at 224:1– 24.
- DigiBox 1204 consists of DigiBox Header 1205, Rules 1206 and Data 1207. Rules 1206 may include one or more rules. Data - 18 -1207 may include various types of data, including ES_ID 1208, Cryptographic Key 1209, and Validation Data 1210… System 1 may be designed so that a DigiBox may only be decrypted (opened) in a protected environment such as IRP 22. In an alternate embodiment, Control Block 13 may directly incorporate the functionality of IRP 22, so that the DigiBox may be opened in Control Block 13 without the necessity of routing the DigiBox to ERP 22 for processing. In one embodiment, the cryptographic key used to decrypt DigiBox 1204 may be stored in IRP 22 (or Control Block 13), so that the DigiBox can only be opened in that protected environment….. IRP 1708 may process DigiBox 1404 and extract a cryptographic key…. Shamoon ‘296 at 17:34-18:2; 18:21-27; 32:13.

Here, regarding the ’627 Patent, market forces demanded the protection of valuable digital media content from theft and other forms of unauthorized access or copying. The above references serve as examples of systems that implement such protection through cryptographic techniques. Thus, one of skill in the art would have been motivated to combine or modify references using known methods that one of skill in the art would have recognized as offering improvements to

solutions of that time. The references identified describe methods that were known to offer improvements, and, accordingly, one of skill in the art would have been motivated to combine or modify combined references to include such improvements.

(2) Combination of known elements yields predictable results.

Because the Asserted Claims of the ’627 Patent simply arrange old elements known in the field of electronic content distribution systems, with each performing the same function it had been known to perform, and yields no more than what one would expect from such an arrangement, combinations of the prior art are obvious. At the time of the alleged invention of the ’627 Patent, since there were a finite number of predictable solutions for content management systems that safeguard digital works through the use of cryptographic techniques, a person of ordinary skill in the art had good reason to pursue and/or combine known options and related applications.

Moreover, the alleged invention of the ’627 Patent is built upon technology that significantly pre-dates the alleged priority date, namely the use of cryptography to protect content. For instance, at least as early as 1990, approximately 10 years before the alleged priority date of the ’627 patent, the use of decryption to protect content was already well-known, as exemplified by General Instrument's Video Cypher II™ system. Gammie at 8:64-9:4. The recognition that cryptography can protect digital media content is ubiquitous throughout the prior art. As one example of this recognition, Morley ’589, at 12:28-36, describes the operation of image encryptor 192 and audio encryptor 196 as encrypting content “using any number of known encryption techniques.” Still another example may be found in Tripathy, which at 5:1-16, describes an encryption unit 150a that may operate according to the Digital Encryption Standard (DES) or the Rivest-Shamir-Adelman (RSA) standard, both of which were devised in the 1970s. The use of cryptography in the context of a content protection system had a long pedigree by the alleged

priority date of '627 patent. *See, e.g.*, Gammie at 7:59-66; Duane at 7:22-27; Ginter at 66:34-45; Mashayekhi at 1:29-39 and 3:14-22; Shear at [0092]. Such cryptographic techniques were available to a person of ordinary skill in the art at the time of the alleged invention, and a person of ordinary skill in the art may draw on such techniques to implement an content protection system such as that described in the alleged invention of the '627 Patent.

A person of ordinary skill in the art having knowledge of the prior art, digital encryption/decryption standards, and their use in the area of content protection, would be motivated to combine the prior art as identified above. Further, motivation exists because the references all are commonly related and are from the same field of art, and a person of ordinary skill in the art would draw equally from the field of art to solve the problem allegedly presented in the '627 Patent. The suggested combinations reflect at least combinations of prior art elements according to known methods to yield predictable results, simple substitutions of known elements to obtain predictable results, and combinations that are obvious to try. Further elaboration and information shall be provided with Defendants' expert reports.

(3) Exemplary prior art combinations

As discussed above, Appendix J-Combination sets out the references that disclose each element of the Asserted Claims of the '627 Patent, and Defendants contend that it would have been obvious to modify such references to include the allegedly missing element, in view of the knowledge of one of ordinary skill in the art, the admitted prior art of the '627 Patent, and/or in combination with any of the other prior art references identified in the '627 Patent. By way of example, and without limitation, Defendants provide the following exemplary combinations for particular claim limitations based on teachings of the cited prior art references. Defendants reserve the right to rely upon any combination of prior art references whether listed herein or otherwise.

Claim [627.1a] "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;"

To the extent a reference does not expressly or inherently disclose 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, these limitations are rendered obvious by the teachings of, at least, Tripathy. *See, e.g.,* Tripathy, at 4:1-12. Figure 2 of Tripathy illustrates receiver 100 as including a transport demultiplexer 140, a bus interface unit 160, and random access storage 154. Figure 2 illustrates as well a multi-function chip 196, also disposed within receiver 100, that in turn includes a descrambler 122. Figure 11 shows transport demultiplexer 140, bus interface unit 160, and random access storage 154 collectively outside of, and therefore in an environment separate from, multi-function chip 196. Because "memory regions 140a and 140b [of transport demultiplexer 140] are not addressable and may thus be impervious to attack," the processing environment composed at least in part by demultiplexer 140 is protected. *Id.* at 44-51. Further, at 6:44-64 and 7:59-67, Tripathy describes that within the separate processing environment of chip 196 descrambler 122 is governed by decryption keys 40 received from control word area 140b of transport demultiplxer 140.

Likewise, Morley '589 describes a digital cinema system in which a decoder 144 processes program information for visual projection onto a screen in an auditorium. Decoder 144 includes a pair of image and audio decryptors 320, 324 governed by CPU 312 but operating in a processing environment separate from that of CPU 312. Figure 11 of Morley '589 shows that decoder 144 is controlled by CPU 312, and includes image and audio decryptors 320, 324 for delivering decrypted

and uncompressed video and audio content to projector 148 and sound system 152, respectively. Morley '359 explains at 19: 63 – 20: 12:

> A block diagram of the decoder 144 is also illustrated in FIG. 11. The decoder 144 processes a compressed/encrypted program to be visually projected onto a screen or surface and audibly presented using the sound system 152. The decoder 144 is controlled by its controller 312 or via the theater manager 128, and comprises at least one depacketizer 316, the controller, or CPU 312, a buffer 314, an image decryptor/decompressor 320, and an audio decryptor/decompressor 324. The buffer may temporarily store information for the depacketizer 316. All of the may be implemented on one or more circuit card assemblies. The circuit card assemblies may be installed in a self-contained enclosure that mounts on or adjacent to the projector 148. Additionally, a cryptographic smart card 328 may be used which interfaces with controller 312 and/or image decryptor/decompressor 320 for transfer and storage of unit-specific cryptographic keying information.

Mashayekhi teaches a system for protecting an application program 240 by automating an authenticating exchange between an API 214 at a user workstation 210 and a governed application in the form of an application program 240 that is disposed in a processing environment separate from that of API 214. Specifically, Mashayekhi at 7: 10–38 describes::

> FIGS. 4A and 4B are a flow chart of the function performed by workstation API 214 in response to the authentication request generated by a particular program. As noted, when a user 201 attempts to access a particular application program, such as a local application 240 or network-based application program 236, the particular application program requires that the user be authenticated prior to accessing its processes or data. The function begins at block 400 and proceeds to block 402 where workstation API 214 receives this authentication inquiry from the application program. Upon receipt, the workstation API 214 determines whether the user is a valid network client at block 404. If the user is not a valid network client, workstation API 214 denies the user access to the distributed authentication service at block 406. However, if the user is a valid network client, then the workstation API 214 requests the proper application secret for the particular application program at block 410. For example, the workstation API 214 calls a "Retrieve Application Secret" API for retrieving the user's identity and proper application secrets. Workstation API 214 provides the application identifier of the particular application as part of the API call. The request to the database API 206 is preferably encoded in a network protocol element in a matter that is well-known in the art. The database API 206, in a matter described below with reference to FIG. 5, returns encrypted data and a keychain private key to the workstation API 214. At block 414, the workstation API 214 receives the encrypted data and keychain private key.

Thus, at least these prior art references show that as of the alleged priority date of the '627 Patent it was known for a content management system to include a secure controller for processing a request to access protected content by a governed application like, for example, decryptors or other applications. These prior art references also show that the secure controllers and the governed applications may be disposed in separate processing environments. In light of the above, it would have been obvious for one of ordinary skill in the art at the time of the '627 Patent to further modify a digital content management system to include such features. One of ordinary skill would have been motivated to do so at least because it would allow content providers to preserve their content from unauthorized access, and also because doing so would involve applying a known technique to other digital content management systems to achieve the same result.

> **Claim [627.1b] – "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"**

To the extent a reference does not expressly or inherently disclose 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, these limitations are rendered obvious by the teachings of, at least, Tripathy. In receiver 100 of Tripathy, encrypted decryption keys 146 are decrypted into unencrypted decryption keys 40, which are passed along to descrambler 122, which in turn uses keys 40 to descramble an A/V signal and thereby put it into a form suitable for display. Tripathy describes this decryption process at 6:28-38 and 6:59-7:4 as follows:

> The encrypted decryption keys 146 may be decrypted inside the PCI bus interface unit 160. In one embodiment of the invention, the decryption unit 150 b performs PCX decryption. In another embodiment of the invention, the decryption unit 150 b performs an operation to reverse the encryption performed by the encryption unit 150 a. Using the decryption key 108 from the decryption unit 150 b, one or more decryption keys 40 may be produced. The decryption keys signal 40 produced in the PCI bus interface unit 160 may be identical to that supplied by the service provider 62 (FIG. 1)….
>
> For example, the descrambler 122 expects two inputs: a signal to be descrambled and a keys signal for descrambling the first signal. The staging areas enable the two signals to independently reach the transport demultiplexer 140, such that the two signals 40 and 45 may be presented simultaneously to the descrambler 122. Accordingly, in FIG. 2, from the buffer area 140 a and the control word area 140 b, the single channel A/V signal 45 and the decryption keys 40 enter the descrambler 122, in one embodiment of the invention. The descrambler 122, the A/V decoder 112, and the video encoder 114, operate just as for the real-time transmission of the channel signal, described above.

Similarly, Morley ‘589 describes a digital cinema system that delivers to a theater an encrypted program key that, once converted to unencrypted form, is capable of decrypting visual content that is to be projected onto an auditorium screen. At 12: 56 – 13: 9 and 13: 10 – 18, Morley ‘589 states:

> Each image or audio program may use specific electronic keying information which is provided, encrypted by presentation-location or theater-specific electronic keying information, to theaters or presentation locations authorized to show that specific program. The conditional access manager 124, or CAM, handles this function. The encrypted program key needed by the auditorium to decrypt the stored information is transmitted, or otherwise delivered, to the authorized theaters prior to playback of the program. Note that the stored program information may potentially be transmitted days or weeks before the authorized showing period begins, and that the encrypted image or audio program key may be transmitted or delivered just before the authorized playback period begins. The encrypted program key may also be transferred using a low data rate link, or a transportable storage element such as a magnetic or optical media disk, a smart card, or other devices having erasable memory elements. The encrypted program key may also be provided in such a way as to control the period of time for which a specific theater complex or auditorium is authorized to show the program….

> Each theater subsystem 104 that receives an encrypted program key decrypts this value using its auditorium specific key, and stores this decrypted program key in a memory device or other secured memory. When the program is to be played back, the theater or location specific and program specific keying information is used, preferably with a symmetric algorithm, that was used in the encryptor 112 in preparing the encrypted signal to now descramble/decrypt program information in real-time.

Likewise, Gammie describes a content security system in which a twice-encrypted decryption key, after being decrypted into unencrypted form, is passed along to a descrambler that uses the unencrypted decryption key to decrypt scrambled content into a form suitable for presentation. Gammie details this process at 10: 36 – 62:

> The system further comprises a routing manager/decoder coupled to the transmitter for receiving and descrambling the scrambled signal. The decoder comprises first and second key decryptors and a descrambler. In the twice encrypted mode, the first key decryptor is coupled to the transmitter and performs a first key decryption on the twice-encrypted key using the second secret serial number and outputs a partially decrypted key. The second key decryptor is coupled to the first key decryptor and perform a second key decryption on the partially decrypted key using the first secret signal number and outputs the decrypted key. The descrambler is coupled to the second key decryptor and the transmitter and descrambles the scrambled signal using the decrypted key and outputs the descrambled signal. The decoder may function without the use of a replaceable security module. In the event of a system breach or a service level change, a replaceable security module may then be inserted into the decoder to "upgrade" the decoder. In another embodiment of the present invention, authorization signals are transmitted from a master uplink through satellite transponder into a loop-back uplink. At the loop-back uplink, program audio and video signals are combined with the authorization signals and sent back to the satellite transponder then to an individual subscription television signal receiver.

Thus, at least these prior art references show that as of the alleged priority date of the ‘627 Patent it was known for a content management system to extract, by a secure control application, secret information from a secure electronic container, in which secret information is configured to be used, at least in part, to decrypt protected content, and in which extracting the secret information comprises decrypting at least a portion of a secure electronic container to generate unencrypted

secret information. In light of the above, it would have been obvious for one of ordinary skill in the art at the time of the '627 Patent to further modify a digital content management system to include such limitations. One of ordinary skill would have been motivated to do so at least because it would allow content providers to preserve their content from unauthorized access, and also because doing so would involve applying a known technique to other digital content management systems to achieve the same result.

> **Claim [627.1c] – "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"**

To the extent a reference does not expressly or inherently disclose 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, these limitations are rendered obvious by the teachings of, at least, Tripathy. In receiver 100 of Tripathy, a PCI bus interface unit 160 decrypts encrypted decryption keys 146 into unencrypted decryption keys 40. Control word area 140b of transport demultiplexer 140 in receiver 100 sends the unencrypted decryption keys 40 to descrambler 122 in the separate processing environment of multi-function chip 196. Tripathy describes this decryption process at 6:28-38 and 6:59-7:4 as follows:

> The encrypted decryption keys 146 may be decrypted inside the PCI bus interface unit 160. In one embodiment of the invention, the decryption unit 150 b performs PCX decryption. In another embodiment of the invention, the decryption unit 150 b performs an operation to reverse the encryption performed by the encryption unit 150 a. Using the decryption key 108 from the decryption unit 150 b, one or more decryption keys 40 may be produced. The decryption keys signal 40 produced in the PCI bus interface unit 160 may be identical to that supplied by the service provider 62 (FIG. 1)….
>
> For example, the descrambler 122 expects two inputs: a signal to be descrambled and a keys signal for descrambling the first signal. The staging areas enable the two signals to independently reach the transport demultiplexer 140, such

> that the two signals 40 and 45 may be presented simultaneously to the descrambler 122. Accordingly, in FIG. 2, from the buffer area 140 a and the control word area 140 b, the single channel A/V signal 45 and the decryption keys 40 enter the descrambler 122, in one embodiment of the invention. The descrambler 122, the A/V decoder 112, and the video encoder 114, operate just as for the real-time transmission of the channel signal, described above.

Similarly, Morley '589 describes a digital cinema system that delivers to a theater subsystem 104 an encrypted program key that is decrypted and then sent in unencrypted form to image and audio decryptors 320, 340 for decrypting visual and audio content that is to be exhibited in an auditorium. Morley describes this process at least at 13: 10 – 18 and 19: 63 – 20: 12::

> Each theater subsystem 104 that receives an encrypted program key decrypts this value using its auditorium specific key, and stores this decrypted program key in a memory device or other secured memory. When the program is to be played back, the theater or location specific and program specific keying information is used, preferably with a symmetric algorithm, that was used in the encryptor 112 in preparing the encrypted signal to now descramble/decrypt program information in real-time….
>
> A block diagram of the decoder 144 is also illustrated in FIG. 11. The decoder 144 processes a compressed/encrypted program to be visually projected onto a screen or surface and audibly presented using the sound system 152. The decoder 144 is controlled by its controller 312 or via the theater manager 128, and comprises at least one depacketizer 316, the controller, or CPU 312, a buffer 314, an image decryptor/decompressor 320, and an audio decryptor/decompressor 324. The buffer may temporarily store information for the depacketizer 316. All of the may be implemented on one or more circuit card assemblies. The circuit card assemblies may be installed in a self-contained enclosure that mounts on or adjacent to the projector 148. Additionally, a cryptographic smart card 328 may be used which interfaces with controller 312 and/or image decryptor/decompressor 320 for transfer and storage of unit-specific cryptographic keying information.

In Mashayekhi, a workstation API 214 of an exchange controller 207 decrypts encrypted secret information and sends it in unencrypted form to an application program that may reside at a separate processing environment embodied as a separate network node:

> As noted, in the illustrative embodiment, the exchange controller 207 comprises an API that is distributed among user workstations (i.e., workstation APIs 214) and the

> authentication database (i.e., the database API 206). A particular program, e.g., program 236, issues an authentication inquiry to user 112 in response to an attempt by that user to access the program's processes or data. When the authentication inquiry is received at the controller, the workstation API 214 verifies that the user is a valid network client (i.e., has successively logged-on and has been authenticated to the NDS) by requesting the proper application secret for program 236. In response to this latter request, the database API 206 accesses the authentication database 204 and provides an encrypted application secret along with the private key for decrypting the secret. The workstation API then decrypts and forwards the proper application secret (and user identity) to the particular application program.

Mashayekhi at 6: 60–7: 9; Fig. 2.

In Morley '335 an encrypted program key received at an auditorium system 128A is decrypted and then sent in unencrypted form to image and audio decompression systems 296, 298:

> Each image and audio program uses specific electronic keying information which is provided, encrypted by presentation-location or theater- specific electronic keying information, only to theaters or presentation locations authorized to show that specific program. The encrypted program key is needed by the auditorium to decrypt the program data stream. The encrypted program key is transmitted, or otherwise delivered, to the authorized theaters prior to playback of the program. Note that the program data stream may be transmitted days or weeks before the authorized showing period begins and that the encrypted program key may be transmitted just before the authorized playback period begins. The encrypted program key can also be transferred using a low data rate link, or a transportable storage element such as a magnetic or optical media disk, a Smart card, or other devices having erasable memory elements. The encrypted program key may be provided in such a way as to control the period of time for which a specific theater complex or auditorium is authorized to show the program. Each auditorium that receives an encrypted program key decrypts this value using its auditorium specific key, and stores this decrypted program key in a memory device or other secured memory. When the program is to be played back, the theater or location specific and program specific keying information is used, preferably with a symmetric algorithm, that was used in encryption system 110 in preparing the encrypted signal to now descramble/ decrypt program information in real-time.

Morley '335 at 22; Fig. 11. *See also, e.g.*, Morley '335 at 40-41:

> Auditorium controller 294 configures, manages the security of, operates, and monitors auditorium system 128A. This includes the external interfaces, image and audio decryption /decompression systems 296 and 298, along with projector 132A and sound system 134A. Control information comes from theater management system 122, a remote control port, or a local control input, such as a control panel on the outside of the auditorium

> system 128A housing or chassis. Auditorium controller 294 manages the electronic keys assigned to auditorium system 128A. Preselected electronic cryptographic keys assigned to auditorium system 128 are used in conjunction with the electronic cryptographic key information that is embedded in the image and audio data to decrypt the image and audio information before the decompression process. In a preferred embodiment, auditorium controller 294 uses a standard micro-processor running embedded auditorium system 128A software, as a basic functional or control element.

Thus, at least these prior art references show that as of the alleged priority date of the '627 Patent it was known for a content management system to send, by a secure control application, unencrypted secret information from a protected processing environment to a governed application executing in the processing environment separate from the protected processing environment. In light of the above, it would have been obvious for one of ordinary skill in the art at the time of the '627 Patent to further modify any digital content management system to include these limitations. One of ordinary skill would have been motivated to do so at least because it would allow digital content management systems to preserve content from unauthorized access, and also because doing so would involve applying a known technique to other digital content management systems to achieve the same result.

> **<u>Claim [627.4]</u> – "The method of claim 1 further comprising:**
> **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."**

To the extent a reference does not expressly or inherently disclose 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, these limitations are rendered obvious by the teachings of, at least, Shear. In Shear, playback equipment 60 is permitted to copy content only if meets certain conditions such as the ability to enforce securely rights management rules:

> Secure node 72 provides a secure rights management facility that may, for example, permit more invasive or extensive use of the content stored on disk. For example, dedicated player 52 may prevent any copying of content stored by disk 100, or it may allow the content to be copied only once and never again. Platform 60 including secure node 72, on the other hand, may allow multiple copies of some or all of the same content—but only if certain conditions are met (e.g., the user of equipment 60 falls within a certain class of people, compensation at an agreed on rate is securely provided for each copy made, only certain excerpts of the content are copied, a secure audit trail is maintained and reported for each copy so made, etc.). (In some embodiments, dedicated player 52 may send protected content only to devices authenticated as able to enforce securely rights management rules and usage consequences. In some embodiments, devices may authenticate using digital certificates, one non-limiting example being certificates conforming to the X.509 standard.) Hence, platform 60 including secure node 72 can, in this example, use the content provided by disk 100 in a variety of flexible, secure ways that are not possible using dedicated player 52—or any other appliance that does not include a secure node.

Shear at [0177]; Fig. 1B.

Similarly, Gammie at 4: 1 – 7 describes the deauthorization of a content decoder 206:

> After receiving the addressed data packet, key decryptor 213 then decrypts the key using the secret serial number stored in SSN memory 212. If service to any decoder 206 in the network is to be terminated, the secret serial number for that decoder is simply deleted from SSN database 211, and decoder 206 is deauthorized at the beginning of the next key period.

Smith describes a network that, prior to transferring a service to a terminal, determines whether the requirements of a user profile 10 and an application profile 12 are met by the terminal profile 12 of an intended terminal:

> Thus the service 14 can only be provided when the requirements of the user's profile 10 and the application profile 11 are met by the terminal profile 12 and the network profile 13. The level of the service provided at the terminal can be varied dependent upon the level at which the resources meet with the requirements . Terminals throughout the network can thus have different levels of service dependent upon how the specific terminal resources and the specific network resources match the specific user's profile and the application requirements.
> Smith at 15.

Thus, at least these prior art references show as of the alleged priority date of the '627 Patent that determining that a governed application meets one or more requirements may be performed prior to sending secret information to the application. Accordingly, it would have been obvious to modify any content management system to determine by the secure control application, prior to sending the secret information to the governed application, that the governed application satisfies one or more requirements. One of ordinary skill would have been motivated to do so at least because it would allow digital content management systems to preserve content from unauthorized access by governed application that no longer satisfy required conditions, and because doing so would involve applying a known technique to other digital content management systems to achieve the same result.

2. Additional References

In addition to the prior art listed herein, additional prior art references may be referenced to show the state and evolution of technology at the time of the alleged invention and may be relevant to the validity of the Asserted Claims depending on the claim construction, infringement, and other positions taken by Intertrust.

C. P.R. 3-3(c) Disclosures: Charts Identifying Where in Each Item of Prior Art Each Element of the Asserted Claim Is Found

Appendices A-J of these Contentions include charts that specifically identify where each element of each Asserted Claim is found in the prior art.

To the extent limitations of any of the Asserted Claims are construed to have a similar meaning, or to encompass similar feature(s) and function(s), as apparently contended by Intertrust in its Infringement Contentions, or later determined by the Court, Defendants' incorporate by reference their contentions with respect to one such limitation into all other similarly construed claim limitations.

D. P.R. 3-3(d) Disclosures: Invalidity Under 35 U.S.C. § 112

Pursuant to Local Rule 3-3(d), Defendants contend that certain claims of the Asserted Patents are invalid under 35 U.S.C. § 112 because: (1) the claims are indefinite; (2) the claims are not enabled; and/or (3) the claims lack adequate written description. Defendants' contentions that certain of the Asserted Claims are invalid under 35 U.S.C. § 112 are made in the alternative, and do not constitute, and should not be interpreted as, admissions regarding the construction or scope of the Asserted Claims, or an admission that any of the Asserted Claims are not anticipated or rendered obvious by any prior art.

These contentions are based on Defendants' current understanding of Intertrust's Infringement Contentions. To the extent Intertrust contends that the prior art references identified above would not enable a person of ordinary skill to make or use the elements of the Asserted Claims against which they are cited, and to the extent Intertrust contends that the Asserted Claims cover something different from what Defendants understand them to cover, the Asserted Claims may not comply with the enablement, written description, and/or definiteness requirements of 35 U.S.C. § 112 ¶¶ 1 and 2. Because compliance with the requirements of 35 U.S.C. § 112 ¶¶ 1 and 2 depends on the construction of those phrases—and no claim construction positions have been exchanged, no claim construction order issued, and no expert discovery undertaken—Defendants' positions on written description, enablement, and/or indefiniteness are necessarily preliminary at this early stage of the case. Defendants reserve all rights to amend or further revise these contentions based on further developments in the case in accordance with the Court's Rules or as otherwise authorized by the Court.

The written description and enablement requirements are analyzed by comparing the claims with the disclosure in the specification. If the claimed invention does not appear in the

specification, the claim fails regardless of whether one of skill in the art could make or use the claimed invention. *Ariad Pharms., Inc. v. Eli Lilly & Co*., 598 F.3d 1336, 1348 (Fed. Cir. 2010). To satisfy the written description requirement, the patentee must convey to those skilled in the art that, as of the filing date, the applicant was in possession of the invention, and demonstrate that possession by disclosing the invention in the specification. *Id.* at 1352. To satisfy the enablement requirement, a patentee must "describe the manner and process of making and using the invention so as to enable a person of skill in the art to make and use the full scope of the invention without undue experimentation." *LizardTech, Inc. v. Earth Res. Mapping, Inc.*, 424 F.3d 1336, 1344-45 (Fed. Cir. 2005). A patent must also be precise enough to afford clear notice to what is claimed. *Nautilus, Inc. v. Biosig Instruments, Inc*., 572 U.S. 898, 899 (2014). A patent is invalid for indefiniteness if its claims, read in light of the specification delineating the patent, and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention. *Id*. at 898-99. The standard for assessing if a patent claim is sufficiently definite to satisfy the statutory requirement is whether "one skilled in the art would understand the bounds of the claim when read in light of the specification." *Novo Indus., L.P. v. Micro Molds Corp*., 350 F.3d 1348, 1358 (Fed. Cir. 2003).

A claim term can be indefinite based on multiple grounds ranging from the substantive concerns to unresolvable drafting errors, each of which can be fatal to the validity of the claims as a matter of law. For example, the Federal Circuit has repeatedly held that apparatus claims that contain method claim limitations are indefinite because it is impossible to determine when direct infringement occurs. *See, e.g., Rembrandt Data Techs., LP v. AOL, LLC*, 641 F.3d 1331, 1339-40 (Fed. Cir. 2011) (an independent claim that recited both an apparatus and a method of using that apparatus was indefinite, as was its dependent claims); *IPXL Holdings v. Amazon.com*,

430 F.3d 1377, 1384 (Fed. Cir. 2005); *In re Katz Interactive Call Processing Patent Litigation*, 639 F.3d 1303, 1318 (Fed. Cir. 2011) (mixed claims "create confusion as to when direct infringement occurs because they are directed both to systems and to actions performed by" users).

Claim terms that lack antecedent basis are indefinite. *See, e.g., Allen Eng'g Corp. v. Bartell Indus., Inc*., 299 F.3d 1336, 1348-49 (Fed. Cir. 2002) (claim ending in the middle of a claim limitation was indefinite because it was "impossible to discern the scope of such a truncated limitation"). Furthermore, means plus function claims, which invoke 35 U.S.C. § 112 ¶ 6, may be invalid as indefinite where a patent owner has failed to disclose adequate corresponding structure linked to the recited claim functionality. *Noah Sys., Inc. v. Intuit Inc*., 675 F.3d 1302, 1311-12 (Fed. Cir. 2012).

In *Nautilus, Inc. v. Biosig Instruments, Inc*., the Supreme Court clarified that a patent is invalid "for indefiniteness if its claims read in light of the specification delineating the patent, and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." 572 U.S. at 898-99. "It cannot be sufficient that a court can ascribe *some* meaning to a patent's claim; the definiteness inquiry trains on the understanding of a skilled artisan at the time of the patent application, not that of a court viewing matters *post hoc*." *Id*. at 911 (emphasis in original).

The Asserted Claims fail to satisfy the enablement, written description, and/or definiteness requirements as set forth by 35 U.S.C. § 112. For example, the Asserted Claims fail to satisfy the definiteness requirements set forth by 35 U.S.C. § 112. ¶ 2 for at least the following reasons:

- use of terms that lack an ordinary meaning in the art and are undefined in the specification;
- use of terms that are used in the specification in a manner which is internally inconsistent, as well as inconsistent with their ordinary meaning, but are not specifically defined in the specification;
- use of such excessive disclaimers of specificity of a term that the term becomes meaningless;
- inconsistent uses of a term within a single specification and/or within the specifications of related patents;
- inconsistent uses of a term between a specification and something allegedly incorporated into that specification;
- inconsistencies within the language of a given claim;
- inconsistent use of terms that may be synonyms for one another.

The indefiniteness of the asserted claims is exacerbated by Intertrust' s attempt to apply the Asserted Claims to very different structures and techniques than those described in the Asserted Patents.

The Asserted Patents also fail to provide an adequate written description as required under 35 U.S.C. § 112, ¶ 1. For example, the Asserted Claims are invalid under 35 U.S.C. § 112, ¶ 1 to the extent they are construed to contradict and/or fail to require the essential, non-optional attributes of the alleged "inventions" identified in the specifications of the Asserted Patents (and any specification allegedly incorporated by reference) and the applications from which the Asserted Patents issued. The Asserted Claims also fail to comply with the written description requirement to the extent the scope of any Asserted Claim exceeds the scope of the alleged

"invention" as set forth in the specifications of the Asserted Patents (and any specification allegedly incorporated by reference).

Additionally, the Asserted Claims fail the enablement, written description, and/or definiteness requirements in view of at least the following claim terms and phrases:

Asserted Claim(s)	Claim Term/Phrase	Invalidity Under 35 U.S.C. § 112
[721.9], [721.29]	"at least one public key secured behind a tamper resistant barrier and therefore hidden from the user"	The claims are invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention. The claims are invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims.
[721.9], [721.29]	"the user"	The claims are invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[304.24b], [304.24c]	"first entity's control information"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[304.24b]	"separately"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention. The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the

Asserted Claim(s)	Claim Term/Phrase	Invalidity Under 35 U.S.C. § 112
		claims.
[304.24c]	"using the first entity's control information to govern"	The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims. The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[304.24d]	"reporting information"	The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims. The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[304.24e]	"designed to impede the ability of a user of the computing system to tamper"	The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims.
[815.42c]	"the authenticity"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention. "The authenticity" has no antecedent basis.
[602.25b]	"each error-check value being inserted in proximity to a portion of the block of data to which it corresponds"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.

Asserted Claim(s)	Claim Term/Phrase	Invalidity Under 35 U.S.C. § 112
[602.25a]	"generating a progression of check values, each check value in the progression being derived from a portion of the block of data and from at least one other check value in the progression"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[602.25b]	"inserting error-check values into the block of data, … and each error-check value being operable to facilitate authentication of a portion of the block of data and of a check value in the progression of check values"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[602.25c]	"transmitting the encoded block of data and the check values to a user's system, whereby the user's system is able to receive and authenticate portions of the encoded block of data before the entire encoded block of data is received"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[603.1b]	"identifying one or more software modules responsible for processing the piece of electronic media content and enabling use of the piece of electronic media content by the user"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[603.1d]	"evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[603.1d]	"evaluating whether the at least one of the one or more software modules make calls to certain system interfaces"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[603.1d]	"evaluating whether the at least one of the one or more software modules direct data to certain channels"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[603.1d]	"analyzing dynamic timing	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim

Asserted Claim(s)	Claim Term/Phrase	Invalidity Under 35 U.S.C. § 112
	characteristics of the at least one of the one or more software modules for anomalous timing characteristics indicative of invalid or malicious activity"	limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[342.1a]	"the predetermined criteria"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention. The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims.
[342.1f]	"authorizing document"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention. The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims.
[342.1f]	"wherein the piece of electronic content comprises an authorizing document, and the second entity associates the second digital certificate with the authorizing document if the authorizing document originated from a certified entity"	The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims.
[342.7]	"wherein the certified entity is identified by a third digital certificate issued by a third entity different from the first and second entities"	The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims.
[342.8]	"wherein the second entity	The claim is invalid under pre-AIA

Asserted Claim(s)	Claim Term/Phrase	Invalidity Under 35 U.S.C. § 112
	determines that an authorizing document originated from the certified entity by checking for the presence of the third digital certificate issued by the third entity"	35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims.
[157.53e]	"(b) one or more electronic objects received by the electronic appliance separately from the piece of electronic content and via separate delivery, the one or more electronic objects specifying one or more permitted or prohibited uses of the piece of electronic content; and"	The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims. The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[157.53b]	"impeding unauthorized access"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention. The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims.
[157.59]	"cryptographically seal"	The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims. The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[157.69e], [157.86b]	"via separate delivery"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the

Asserted Claim(s)	Claim Term/Phrase	Invalidity Under 35 U.S.C. § 112
		invention.
[157.53e], [157.69b], [157.69e], [157.84a], [157.86b], [157.99a]	"separately"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention. The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims.
[157.69e], [157.69g], [157.74], [157.80], [157.84a], [157.84c], [157.86b], [157.86d], [157.99a], [157.99c]	"a first electronic object"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[157.69c], [157.87b], [157.89]	"secure processing unit"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention. The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims.
[157.86e]	"wherein the electronic appliance comprises hardware and/or software operable to impede the user from tampering with performance of said selectively granting step"	The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims.
[157,73], [157.88]	"non-executable audio, video, and/or textual content"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[158.4c]	"receiving, at the electronic	The claim is invalid under pre-AIA

Asserted Claim(s)	Claim Term/Phrase	Invalidity Under 35 U.S.C. § 112
	appliance, independently from the electronic content item via separate delivery and protected separately from the electronic content item, a rule specifying one or more permitted uses of the electronic content item"	35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims. The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention.
[158.4f]	"secure processing unit"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention. The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims.
[158.4e]	"determining that the requested use of the electronic content item corresponds to a permitted use of the electronic content item specified in the rule"	The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims.
[627.1]	"a secure control application executing on the system in a protected processing environment"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention. The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims.
[627.1]	"a governed application executing on the system in a processing environment separate from the protected processing environment"	The claim is invalid under 35 U.S.C. § 112, ¶ 2 because the claim limitation fails to inform, with reasonable certainty, those skilled

Asserted Claim(s)	Claim Term/Phrase	Invalidity Under 35 U.S.C. § 112
		in the art about the scope of the invention. The claim is invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 because the specification fails to describe or enable the full breadth of the claims.

These examples are merely exemplary and are not intended to be limiting. Defendants reserve all rights to amend their Contentions under 35 U.S.C. § 112, including after the Asserted Claims are ultimately construed by the Court, in response to any interpretation of the Asserted Claims embodied in Intertrust's infringement positions, and/or to account for any changes in the law concerning invalidity under 35 U.S.C. § 112. Defendants additionally reserve the right to provide additional explanation and/or argument for their Contentions under § 112, including, for example, based on expert testimony.

III. P.R. 3-4 DISCLOSURES AND CONTENTIONS

A. P.R. 3-4(a) Disclosures

Pursuant to P.R. 3-4(a), Defendants are separately producing representative technical documentation that shows the operation of aspects or elements of any Accused Instrumentality identified by Intertrust in its Infringement Contentions. Such documents can be found at the following Bates ranges: INT-AMC00000001 to INT-AMC00011622, INT-CMK00000001 to INT-CMK00010463, and INT-REG00000001 to INT-REGC00012997. Defendants reserve the right to supplement these disclosures with additional documentation.

B. P.R. 3-4(b) Disclosures

In accordance with P.R. 3-4(b), Defendants are producing a single set of all prior art references identified in these Contentions. Such documents can be found at the following Bates range: INTER-DEF-PA-00000001 - INTER-DEF-PA-00041500. Defendants are also producing prior art references concerning prior art systems and methods. Any prior art references not in English are produced with an English translation of the portion(s) relied upon. These prior art references are cited herein and support the contentions presented. Defendants' search for prior art references, additional documentation, and/or corroborating evidence concerning prior art apparatuses and methods is ongoing. Accordingly, Defendants reserve the right to supplement its production, as provided by the local rules, as additional prior art references, additional documentation, and/or corroborating evidence concerning prior art documents/apparatuses, and methods are obtained during the course of discovery.

IV. SUBJECT MATTER ELIGIBILITY CONTENTIONS

Defendants contend the Asserted Claims are directed to patent ineligible subject matter. Specifically, the Asserted Claims are directed to abstract ideas relating to methods of controlling access to content. Methods of controlling access to content were well-known long before the time of the Asserted Patents, and indeed long before the rise of modern computing and the Internet. The Asserted Claims add nothing to these well-known methods beyond requiring that they be performed using generic computer systems in conventional and generic arrangements. As a result, the Asserted Claims fail to add anything to the underlying abstract ideas sufficient to transform them into patent-eligible subject matter.

Pursuant to the Court's Standing Order Regarding Subject Matter Eligibility Contentions, the following appendices include charts that: (1) identify each exception to eligibility (*e.g.*, abstract idea, law of nature, and natural phenomenon) to which Defendants contend the Asserted Claims

are directed; (2) describe how each element of the Asserted Claims, both individually and in combination with the other elements of that claim, was well understood, routine, and conventional in the relevant industry at the relevant time; (3) describe the industry, at the relevant time, in which the Asserted Claims are alleged to be well understood, routine, and conventional; and(4) state the factual and legal bases for each of the foregoing contentions.

Appendix K	U.S. Patent No. 6,157,721 ("the '721 Patent")
Appendix L	U.S. Patent No. 6,640,304 ("the '304 Patent")
Appendix M	U.S. Patent No. 6,785,815 ("the '815 Patent")
Appendix N	U.S. Patent No. 7,340,602 ("the '602 Patent")
Appendix O	U.S. Patent No. 7,406,603 ("the '603 Patent")
Appendix P	U.S. Patent No. 7,694,342 ("the '342 Patent")
Appendix Q	U.S. Patent No. 8,191,157 ("the '157 Patent")
Appendix R	U.S. Patent No. 8,191,158 ("the '158 Patent")
Appendix S	U.S. Patent No. 8,931,106 ("the '106 Patent")
Appendix T	U.S. Patent No. 9,569,627 ("the '627 Patent")

The Court has not yet construed any terms of the Asserted Claims. Although Defendants' position is that the Asserted Claims do not require construction to determine their eligibility, Defendants reserve the right to supplement their Contentions based upon the Court's construction of the Asserted Claims. In addition, Defendants' investigation, including their investigation of the Asserted Patents and industry at the time of the alleged inventions, is ongoing. Defendants base these Contentions on their current knowledge and understanding of the Asserted Claims, and reserve the right to supplement these Contentions in accordance with the Federal Rules of Civil Procedure, the Local Rules, the Local Patent Rules, the Docket Control Order, the Court's Standing Order, any Order issued by this Court, or otherwise.

A. Exceptions to Eligibility

As noted above, the Asserted Claims are directed to patent-ineligible abstract relating to methods of controlling access to content. Appendices K-T identify, on a patent-by-patent basis, the abstract idea to which each Asserted Claim is directed.

B. Representative Claims

The following claims are representative of the Asserted Claims for purposes of the subject-matter eligibility analysis:

Asserted Patents	Asserted Claims	Representative Claims
'721 Patent	Claims 9 and 29	Claim 9
'304 Patent	Claim 24	Claim 24
'815 Patent	Claims 42 and 43	Claim 42
'602 Patent	Claims 25 and 26	Claim 25
'603 Patent	Claims 1 and 2	Claim 1
'342 Patent	Claims 1, 7, 8, and 12	Claim 1
'157 Patent	Claims 53, 54, 56-60, 64-66, 69-75, 80, 81, 84, 86-90, 95, 96, and 99	Claims 53 and 69
'158 Patent	Claim 4	Claim 4
'106 Patent	Claim 17	Claim 17
'627 Patent	Claims 1, 4, 5, 6, 7, and 8	Claim 1

C. Description of the Industry

Defendants contend that the industry, at the relevant time, in which the Asserted Claims are alleged to be well understood, routine and conventional is, broadly speaking, rights management (*i.e.*, methods of controlling access to content). A more specific identification of the industry relevant to each Asserted Patent is included in Appendices K-T.

Defendants reserve the right to rely on percipient and/or expert testimony to supplement, summarize, and/or explain the state of the industry at the time the Asserted Patents were filed. Any such witnesses will be disclosed pursuant to the Federal Rules of Civil Procedure and the Court's Docket Control Order in this case for initial, additional, and expert disclosures.

D. Well Understood, Routine, and Conventional Nature of the Asserted Claims

Appendices K-T to these Contentions describe how each element of the Asserted Claims, both individually and in combination with other elements of the claim, was well understood, routine, and conventional. Defendants incorporate by reference the P.R. 3-3 Disclosures set forth above, as well as Appendices A-J to these Contentions as further evidence of how each element of the Asserted Claims, both individually and in combination with other elements of the claim, was well understood, routine, and conventional.

E. Accompanying Document Production

Defendants P.R. 3-4(b) productions, served concurrently with these Contentions, include the evidence currently known or available to Defendants that evidences the patent ineligibility of the Asserted Claims, including substantial evidence that the Asserted Claims merely recite well-known, routine, and conventional elements that amount to nothing more than underlying abstract ideas to which they are directed. To the extent any such prior art reference is not in English, Defendants have produced to or will produce an English translation of the portion(s) of the non-English prior art reference(s) relied upon by Defendants.

January 30, 2020

Respectfully submitted,

By: */s/ Richard S. Zembek*

Richard S. Zembek
Texas State Bar No. 00797726
richard.zembek@nortonrosefulbright.com
Eric B. Hall
Texas State Bar No. 24012767
eric.hall@nortonrosefulbright.com
1301 McKinney, Suite 5100
Houston, Texas 77010-3095
Tel: (713) 651-5151
Fax: (713) 651-5246

James S. Renard
Texas State Bar No. 16768500
james.renard@nortonrosefulbright.com
Michael A. Swartzendruber
Texas State Bar No. 19557702
michael.swartzendruber@nortonrosefulbright.com
2200 Ross Avenue, Suite 3600
Dallas, Texas 75201-7932
Tel: (214) 855-8000
Fax: (214) 855-8200

Stephanie N. DeBrow
Texas State Bar No. 24074119
stephanie.debrow@nortonrosefulbright.com
Eric C. Green
Texas State Bar No. 24069824
eric.green@nortonrosefulbright.com
Catherine J. Garza
Texas State Bar No. 24073318
cat.garza@nortonrosefulbright.com
98 San Jacinto Boulevard, Suite 1100
Austin, Texas 78701-4255
Tel: (512) 536-3094
Fax: (512) 536-4598
ATTORNEYS FOR DEFENDANT

COUNSEL FOR AMC ENTERTAINMENT HOLDINGS, INC., CINEMARK HOLDINGS, INC., AND REGAL ENTERTAINMENT GROUP

CERTIFICATE OF SERVICE

I hereby certify that on January 30, 2020 the foregoing document, as well as all associated Appendices, were served via e-mail upon all counsel of record in this case.

/s/ Richard S. Zembek