EXHIBIT 1

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

CERTICOM CORP. and CERTICOM PATENT HOLDING CORP., Plaintiffs,	
v.	Civil Action No. 2-07CV-216-TJW
SONY CORPORATION, SONY CORPORATION OF AMERICA, SONY COMPUTER ENTERTAINMENT INC., SONY COMPUTER ENTERTAINMENT AMERICA INC., SONY PICTURES ENTERTAINMENT INC., SONY ELECTRONICS INC. and SONY DADC US INC. Defendants.	JURY

AMENDED DISCLOSURE OF ASSERTED CLAIMS AND PRELIMINARY INFRINGEMENT CONTENTIONS

Pursuant to local Patent Rule 3-1, Plaintiffs Certicom Corp. and Certicom Patent Holding Corp. (collectively "Certicom") provide the following Disclosure Of Asserted Claims And Preliminary Infringement Contentions to Defendants Sony Corporation ("Sony Japan"), Sony Corporation of America ("Sony America"), Sony Computer Entertainment Inc. ("SCE Japan"), Sony Computer Entertainment America Inc. ("SCE America"), Sony Pictures Entertainment Inc. ("Sony Pictures"), Sony Electronics Inc. ("Sony Electronics"), and Sony DADC US Inc. ("Sony DADC") (collectively "Sony").

Certicom's investigation of the matters disclosed is ongoing and the following disclosures are based solely upon information and belief and information that is publicly available to Certicom at this time. Sony has not produced any specifications, flow charts, source code or documents relating to the accused instrumentalities. Certicom reserves the right to supplement or modify these disclosures as new information, through discovery or otherwise, becomes available.

I. PATENT RULE 3-1(a) DISCLOSURE

Certicom alleges that Sony Japan infringes, either directly under 35 U.S.C. §§ 271(a) or indirectly by inducing and/or contributing to the infringement of its customers, suppliers and/or licensees under 35 U.S.C. §§ 271 (b), (c), (f) and/or (g), claim 61 of U.S. Patent No. 6,563,928 ("the '928 patent") and claims 3, 18 and 22 of U.S. Patent No. 6,704,870 ("the '870 patent").

Certicom alleges that Sony America infringes, either directly under 35 U.S.C. §§ 271(a) or indirectly by inducing and/or contributing to the infringement of its customers, suppliers and/or licensees under 35 U.S.C. §§ 271 (b), (c), (f) and/or (g), claim 61 of the '928 patent and claims 3, 18 and 22 of the '870 patent.

Certicom alleges that SCE Japan infringes, either directly under 35 U.S.C. §§ 271(a) or indirectly by inducing and/or contributing to the infringement of its customers, suppliers and/or licensees under 35 U.S.C. §§ 271 (b), (c), (f) and/or (g), claims 3, 18 and 22 of the '870 patent.

Certicom alleges that SCE America infringes, either directly under 35 U.S.C. §§ 271(a) or indirectly by inducing and/or contributing to the infringement of its customers, suppliers and/or licensees under 35 U.S.C. §§ 271 (b), (c), (f) and/or (g), claims 3, 18 and 22 of the '870 patent.

Certicom alleges that Sony Pictures infringes, either directly under 35 U.S.C. §§ 271(a) or indirectly by inducing and/or contributing to the infringement of its customers, suppliers and/or licensees under 35 U.S.C. §§ 271 (b), (c), (f) and/or (g), claims 3, 18 and 22 of the '870 patent.

Certicom alleges that Sony Electronics infringes, either directly under 35 U.S.C. §§ 271(a) or indirectly by inducing and/or contributing to the infringement of its customers, suppliers and/or licensees under 35 U.S.C. §§ 271 (b), (c), (f) and/or (g), claim 61 of the ‘928 patent and claims 3, 18 and 22 of the ‘870 patent.

Certicom alleges that Sony DADC infringes, either directly under 35 U.S.C. §§ 271(a) or indirectly by inducing and/or contributing to the infringement of its customers, suppliers and/or licensees under 35 U.S.C. §§ 271 (b), (c), (f) and/or (g), claims 3, 18 and 22 of the ‘870 patent.

II. PATENT RULE 3-1(b) DISCLOSURE

A. The ‘928 Patent

The Sony Japan accused instrumentalities for the ‘928 patent, claim 61 are each and every product that utilizes Sony’s DTCP-enabled i.LINK™ or DTCP-IP technology. These products include but are not limited to Sony VAIO computers with i.LINK™ ports or DTCP-IP, Sony KDL-32XBR950 television, Sony KDL-42XBR950 television, Sony KDF-60XBR950 television, Sony KDF-70XBR950 television, Sony KDP-51WS550 television, Sony KDP-57WS550 television, Sony KDP-65WS550 television, Sony KDE-42BR950 television, Sony KDE-50BR950 television, Sony KDE-61BR950 television, Sony KDS-R50XBR1 television, Sony KDS-60XBR1 television, Sony VAIO i.LINK DVD+/-R DL/DVD+/-RW Drive External, Sony RDR-GX330 DVD player, Sony DRD-VX555 DVD player, Sony DVP-NS9100ES/B DVD player, Sony HDW-D1800 (with HKDW-105 board) VTR, Sony STR-DA9000ES home theater receiver, Sony SCD-XA9000ES super audio CD player, Sony CXD 3204 chip, Sony CXD 3205 chip, Sony VGX-XL3 VAIO digital living system, and Sony VGX-TP1 VAIO living room PC.

The Sony America accused instrumentalities for the ‘928 patent, claim 61 are each and every product that utilizes Sony’s DTCP-enabled i.LINK™ or DTCP-IP technology. These products include but are not limited to Sony VAIO computers with i.LINK™ ports or DTCP-IP, Sony KDL-32XBR950 television, Sony KDL-42XBR950 television, Sony KDF-60XBR950 television, Sony KDF-70XBR950 television, Sony KDP-51WS550 television, Sony KDP-57WS550 television, Sony KDP-65WS550 television, Sony KDE-42BR950 television, Sony KDE-50BR950 television, Sony KDE-61BR950 television, Sony KDS-R50XBR1 television, Sony KDS-60XBR1 television, Sony VAIO i.LINK DVD+/-R DL/DVD+/-RW Drive External, Sony RDR-GX330 DVD player, Sony DRD-VX555 DVD player, Sony DVP-NS9100ES/B DVD player, Sony HDW-D1800 (with HKDW-105 board) VTR, Sony STR-DA9000ES home theater receiver, Sony SCD-XA9000ES super audio CD player, Sony CXD 3204 chip, Sony CXD 3205 chip, Sony VGX-XL3 VAIO digital living system, and Sony VGX-TP1 VAIO living room PC.

The Sony Electronics accused instrumentalities for the '928 patent, claim 61 are each and every product that utilizes Sony's DTCP-enabled i.LINK™ or DTCP-IP technology. These products include but are not limited to Sony VAIO computers with i.LINK™ ports or DTCP-IP, Sony KDL-32XBR950 television, Sony KDL-42XBR950 television, Sony KDF-60XBR950 television, Sony KDF-70XBR950 television, Sony KDP-51WS550 television, Sony KDP-57WS550 television, Sony KDP-65WS550 television, Sony KDE-42BR950 television, Sony KDE-50BR950 television, Sony KDE-61BR950 television, Sony KDS-R50XBR1 television, Sony KDS-60XBR1 television, Sony VAIO i.LINK DVD+/-R DL/DVD+/-RW Drive External, Sony RDR-GX330 DVD player, Sony DRD-VX555 DVD player, Sony DVP-NS9100ES/B DVD player, Sony HDW-D1800 (with HKDW-105 board) VTR, Sony STR-DA9000ES home theater receiver, Sony SCD-XA9000ES super audio CD player, Sony CXD 3204 chip, Sony

CXD 3205 chip, Sony VGX-XL3 VAIO digital living system, and Sony VGX-TP1 VAIO living room PC.

B. The ‘870 Patent

The Sony Japan accused instrumentalities for the ‘870 patent, claims 3, 18 and 22 are each and every product that utilizes Sony’s DTCP-enabled i.LINK™, DTCP-IP or Blu-ray technology. These products include but are not limited to Sony HES-V1000 Home Entertainment Server, Sony BDP-S1 Blu-ray disc player, Sony BDP-S2000ES Blu-ray disc player, Sony BDP-S500 Blu-ray disc player, Sony BDP-S300 Blu-ray disc player, Sony BWU-100A Blu-ray disc rewritable drive, Sony HT-SF2000 Blu-ray Disc Matching Component Home Theater, Sony HT-SS2000 Blu-ray Disc Matching Component Home Theater, Sony PlayStation 3 console, Sony PlayStation 3 software distributed on Blu-ray discs, motion pictures and television shows distributed on Blu-ray discs, Blu-ray discs, including but not limited to VGhN-FZ180U/B 50GB BD-R Dual Layer Recordable discs, BNE-25AHF Rewritable discs and BNR-50AHE, BNR-25AHE Recordable discs, Sony VAIO computers with i.LINK™ ports, DTCP-IP and/or Blu-ray drives, including but not limited to model numbers VGN-AR690U, VGN-AR630E, VGN-AR390E, VGN-AR370, VGN-AR570, VGN-FZ190, VGN-FZ90, VGN-FZ190E/1, VGN-FZ190E/2, VGN-FZ180U/B, VGN-FZ285U/B, VGN-FZ280E/B, VGN-FZ290 and VGC-L19U, Sony KDL-32XBR950 television, Sony KDL-42XBR950 television, Sony KDF-60XBR950 television, Sony KDF-70XBR950 television, Sony KDP-51WS550 television, Sony KDP-57WS550 television, Sony KDP-65WS550 television, Sony KDE-42BR950 television, Sony KDE-50BR950 television, Sony KDE-61BR950 television, Sony KDS-R50XBR1 television, Sony KDS-60XBR1 television, Sony VAIO i.LINK DVD+/-R DL/DVD+/-RW Drive External, Sony RDR-GX330 DVD player, Sony DRD-VX555 DVD player, Sony DVP-NS9100ES/B DVD player, Sony HDW-D1800 (with HKDW-105 board)

VTR, Sony STR-DA9000ES home theater receiver, Sony SCD-XA9000ES super audio CD player, Sony CXD 3204 chip, Sony CXD 3205 chip, Sony VGX-XL3 VAIO digital living system, and Sony VGX-TP1 VAIO living room PC.

The Sony America accused instrumentalities for the '870 patent, claims 3, 18 and 22 are each and every product that utilizes Sony's DTCP-enabled i.LINK™, DTCP-IP or Blu-ray technology. These products include but are not limited to Sony HES-V1000 Home Entertainment Server, Sony BDP-S1 Blu-ray disc player, Sony BDP-S2000ES Blu-ray disc player, Sony BDP-S500 Blu-ray disc player, Sony BDP-S300 Blu-ray disc player, Sony BWU-100A Blu-ray disc rewritable drive, Sony HT-SF2000 Blu-ray Disc Matching Component Home Theater, Sony HT-SS2000 Blu-ray Disc Matching Component Home Theater, Sony PlayStation 3 console, Sony PlayStation 3 software distributed on Blu-ray discs, motion pictures and television shows distributed on Blu-ray discs, Blu-ray discs, including but not limited to VGhN-FZ180U/B 50GB BD-R Dual Layer Recordable discs, BNE-25AHF Rewritable discs and BNR-50AHE, BNR-25AHE Recordable discs, Sony VAIO computers with i.LINK™ ports, DTCP-IP and/or Blu-ray drives, including but not limited to model numbers VGN-AR690U, VGN-AR630E, VGN-AR390E, VGN-AR370, VGN-AR570, VGN-FZ190, VGN-FZ90, VGN-FZ190E/1, VGN-FZ190E/2, VGN-FZ180U/B, VGN-FZ285U/B, VGN-FZ280E/B, VGN-FZ290 and VGC-L19U, Sony KDL-32XBR950 television, Sony KDL-42XBR950 television, Sony KDF-60XBR950 television, Sony KDF-70XBR950 television, Sony KDP-51WS550 television, Sony KDP-57WS550 television, Sony KDP-65WS550 television, Sony KDE-42BR950 television, Sony KDE-50BR950 television, Sony KDE-61BR950 television, Sony KDS-R50XBR1 television, Sony KDS-60XBR1 television, Sony VAIO i.LINK DVD+/-R DL/DVD+/-RW Drive External, Sony RDR-GX330 DVD player, Sony DRD-VX555 DVD player, Sony DVP-NS9100ES/B DVD player, Sony HDW-D1800 (with HKDW-105 board) VTR, Sony STR-DA9000ES home theater receiver, Sony SCD-XA9000ES super audio CD player, Sony CXD 3204 chip, Sony CXD 3205 chip, Sony VGX-XL3 VAIO digital living system, and Sony VGX-TP1 VAIO living room PC.

The SCE Japan accused instrumentalities for the '870 patent, claims 3, 18 and 22 are each and every product that utilizes Sony's Blu-ray technology. These products include but are not limited to the Sony PlayStation 3 console and Sony PlayStation 3 software distributed on Blu-ray discs.

The SCE America accused instrumentalities for the '870 patent, claims 3, 18 and 22 are each and every product that utilizes Sony's Blu-ray technology. These products include but are not limited to the Sony PlayStation 3 console and Sony PlayStation 3 software distributed on Blu-ray discs.

The Sony Electronics accused instrumentalities for the '870 patent, claims 3, 18 and 22 are each and every product that utilizes Sony's DTCP-enabled i.LINK™, DTCP-IP or Blu-ray technology. These products include but are not limited to Sony HES-V1000 Home Entertainment Server, Sony BDP-S1 Blu-ray disc player, Sony BDP-S2000ES Blu-ray disc player, Sony BDP-S500 Blu-ray disc player, Sony BDP-S300 Blu-ray disc player, Sony BWU-100A Blu-ray disc rewritable drive, Sony HT-SF2000 Blu-ray Disc Matching Component Home Theater, Sony HT-SS2000 Blu-ray Disc Matching Component Home Theater, Sony VAIO computers with i.LINK™ ports, DTCP-IP and/or Blu-ray drives, including but not limited to model number**s** VGN-AR690U**,** VGN-AR630E, VGN-AR390E, VGN-AR370, VGN-AR570, VGN-FZ190, VGN-FZ90, VGN-FZ190E/1, VGN-FZ190E/2, VGN-FZ180U/B, VGN-FZ285U/B, VGN-FZ280E/B, VGN-FZ290 and VGC-L19U, Sony KDL-32XBR950 television, Sony KDL-42XBR950 television, Sony KDF-60XBR950 television, Sony KDF-70XBR950 television, Sony KDP-51WS550 television, Sony KDP-57WS550 television, Sony KDP-65WS550 television, Sony KDE-42BR950 television, Sony KDE-50BR950 television, Sony KDE-61BR950 television, Sony KDS-R50XBR1 television, Sony KDS-60XBR1 television, Sony VAIO i.LINK DVD+/-R DL/DVD+/-RW Drive External, Sony RDR-GX330 DVD player, Sony DRD-VX555 DVD player, Sony DVP-NS9100ES/B DVD player, Sony HDW-D1800 (with HKDW-105 board) VTR, Sony STR-DA9000ES home theater receiver, Sony SCD-XA9000ES super audio CD player, Sony CXD 3204 chip, Sony CXD 3205 chip, Sony VGX-XL3 VAIO digital living system, and Sony VGX-TP1 VAIO living room PC.

The Sony Pictures accused instrumentalities for the '870 patent, claims 3, 18 and 22 are each and every product that utilizes Sony's Blu-ray technology. These products include, but are not limited to, motion pictures and television shows distributed on Blu-ray discs.

The Sony DADC accused instrumentalities for the '870 patent, claims 3, 18 and 22 are each and every product that utilizes Sony's Blu-ray technology. These products include, but are not limited to, Blu-ray discs.

III. PATENT RULE 3-1(c) DISCLOSURE

A. The '928 Patent

For the '928 patent, each accused instrumentality contains either one or more DTCP-enabled i.LINK™ ports along with its associated hardware and software or hardware and software implementing Sony's DTCP-IP technology. Each accused instrumentality operates in accordance with the Digital Content Protection Standard ("DTCP") specification to transmit encrypted data when connected to one or more additional DTCP-enabled device(s) (manufactured by Sony or a third party). Attached as Appendix A is a claim chart setting forth how the accused instrumentalities when connected to one or more additional DTCP-enabled device(s) (whether one of Defendants' devices or a device of a third party) and operating in conformance with the DTCP specification, infringe claim 61 of the '928 patent.

B. The '870 Patent

For the '870 patent, the accused instrumentalities can broken into two general categories: 1) accused instrumentalities that operate in accordance with the DTCP specification and 2) accused instrumentalities that operate in accordance with the Advanced Access Content System ("AACS") specification.

1. DTCP

The accused instrumentalities that operate in accordance with the DTCP specification include but are not limited to Sony VAIO computers with i.LINK™ ports and/or DTCP-IP, Sony KDL-32XBR950 television, Sony KDL-42XBR950 television, Sony KDF-60XBR950 television, Sony KDF-70XBR950 television, Sony KDP-51WS550 television, Sony KDP-57WS550 television, Sony KDP-65WS550 television, Sony KDE-42BR950 television, Sony KDE-50BR950 television, Sony KDE-61BR950 television, Sony KDS-R50XBR1 television, Sony KDS-60XBR1 television, Sony VAIO i.LINK DVD+/-R DL/DVD+/-RW Drive External, Sony RDR-GX330 DVD player, Sony DRD-VX555 DVD player, Sony DVP-NS9100ES/B DVD player, Sony HDW-D1800 (with HKDW-105 board) VTR, Sony STR-DA9000ES home theater receiver, Sony SCD-XA9000ES super audio CD player, Sony CXD 3204 chip, Sony CXD 3205 chip, Sony VGX-XL3 VAIO digital living system, and Sony VGX-TP1 VAIO living room PC. Each accused instrumentality that operates in accordance with the DTCP specification contains either one or more DTCP-enabled i.LINK™ port along with its associated hardware and software or hardware and software implementing Sony's DTCP-IP technology. These accused instrumentalities operate in accordance with the DTCP specification to transmit encrypted data when connected to one or more additional DTCP-enabled device(s) (manufactured by Sony or a third party). Attached as Appendix B is a claim chart setting forth how the accused instrumentalities when connected to one or more additional DTCP-enabled device(s) (whether one of Defendants' devices or a device of a third party) and operating in conformance with the DTCP specification, infringe claims 3, 18 and 22 of the '870 patent.

2. AACS

The accused instrumentalities that operate in accordance with the AACS specification include, but are not limited to, Sony HES-V1000 Home Entertainment Server, Sony BDP-S1 Blu-ray disc player, Sony BDP-S2000ES Blu-ray disc player, Sony BDP-S500 Blu-ray disc player, Sony BDP-S300 Blu-ray disc player, Sony BWU-100A Blu-ray disc rewritable drive, Sony HT-SF2000 Blu-ray Disc Matching Component Home Theater, Sony HT-SS2000 Blu-ray Disc Matching Component Home Theater, Sony VGX-XL3 VAIO digital living system, Sony PlayStation 3 console, Sony PlayStation 3 software distributed on Blu-ray discs, motion pictures and television shows distributed on Blu-ray discs, Blu-ray discs, including but not limited to VGhN-FZ180U/B 50GB BD-R Dual Layer Recordable discs, BNE-25AHF Rewritable discs and BNR-50AHE, BNR-25AHE Recordable discs, and Sony VAIO computers with Blu-ray drives, including but not limited to model number**s** VGN-AR690U**,** VGN-AR630E, VGN-AR390E, VGN-AR370, VGN-AR570, VGN-FZ190, VGN-FZ90, VGN-FZ190E/1, VGN-FZ190E/2, VGN-FZ180U/B, VGN-FZ285U/B, VGN-FZ280E/B, VGN-FZ290 and VGC-L19U. Each accused instrumentality that operates in accordance with the AACS specification contains either a Blu-ray drive or a Blu-ray disc. For the accused instrumentalities that contain a Blu-ray drive, including but not limited to, Sony HES-V1000 Home Entertainment Server, Sony BDP-S1 Blu-ray disc player, Sony BDP-S2000ES Blu-ray disc player, Sony BDP-S500 Blu-ray disc player, Sony BDP-S300 Blu-ray disc player, Sony BWU-100A Blu-ray disc rewritable drive, Sony HT-SF2000 Blu-ray Disc Matching Component Home Theater, Sony HT-SS2000 Blu-ray Disc

Matching Component Home Theater, Sony VGX-XL3 VAIO digital living system, Sony PlayStation 3 console and Sony VAIO computers with Blu-ray drives, including but not limited to model numbers VGN-AR690U, VGN-AR630E, VGN-AR390E, VGN-AR370, VGN-AR570, VGN-FZ190, VGN-FZ90, VGN-FZ190E/1, VGN-FZ190E/2, VGN-FZ180U/B, VGN-FZ285U/B, VGN-FZ280E/B, VGN-FZ290 and VGC-L19U, encrypted data is transmitted in accordance with the AACS specification when a Blu-ray disc (manufactured by Sony or a third party) is inserted into the accused instrumentality's Blu-ray drive. In addition, each accused instrumentality that contains a Blu-ray drive contains one or more of: 1) a signed drive certificate; or 2) a signed host certificate. Each accused instrumentality therefore contains at least one ECDSA signature created at Sony's request by AACS Licensing Authority (AAC-LA), of which Sony is a founder, in accordance with the AACS specification. For the accused instrumentalities that contain a Blu-ray disc, including but not limited to, Sony PlayStation 3 software distributed on Blu-ray discs, motion pictures and television shows distributed on Blu-ray discs, Blu-ray discs, including but not limited to VGhN-FZ180U/B 50GB BD-R Dual Layer Recordable discs, BNE-25AHF Rewritable discs and BNR-50AHE, BNR-25AHE Recordable discs, encrypted data is transmitted in accordance with the AACS specification when the accused instrumentality is inserted into a Blu-ray drive (manufactured by Sony or a third party). In addition Sony places on each accused instrumentality that is a Blu-ray disc one or more of: 1) a signed Content Certificate (using a message hash produced by Sony); 2) a signed Certificate Revocation List (CRL); 3) a signed Host Revocation List (HRL); 4) a signed Drive Revocation List (DRL); or 5) a signed End of Media Key Block (MKB). Each signed Blu-ray disc therefore contains at least one ECDSA signature created at Sony's request by AACS Licensing Authority (AAC-LA), of which Sony is a founder, in accordance with the AACS specification. Attached as

Appendix C is a claim chart setting forth how the accused instrumentalities that operate in accordance with AACS specification infringe claims 3, 18 and 22 of the ‘870 patent when either an accused instrumentality that contains a Blu-ray drive has a Blu-ray disc (whether one of Defendants’ discs or a disc of a third party) inserted in it or an accused instrumentality that contains a Blu-ray disc is inserted into a Blu-ray drive (whether one of Defendants’ drives or a drive of a third party).

IV. PATENT RULE 3-1(d) DISCLOSURE

Certicom asserts that each element of each asserted claim is literally present in each accused instrumentality. To the extent Defendants may assert that there are any differences between the accused products’ operation and an asserted claim those alleged difference are necessarily insubstantial and the accused products would infringe under the doctrine of equivalents. Pursuant to P.R. 3-1(h), Certicom state that each asserted claim contains at least one software limitation. Accordingly, Certicom will supplement its P.R. 3-1(d) disclosure within 30 days after Sony produces the source code for each accused instrumentality.

V. PATENT RULE 3-1(e) DISCLOSURE

Claim 61 of the ‘928 patent is entitled to a priority date of May 18, 1995. Claims 3, 18 and 22 of the ‘870 patent are entitled to a priority date of April 16, 1996.

VI. PATENT RULE 3-1(f) DISCLOSURE

Certicom’s Security Builder® Crypto™ products (versions 1.x to 5.x) and various customer-specific security systems designed by Certicom incorporate claims 3, 18 and 22 of the ‘870 patent.

Dated: May __, 2008

ROPES & GRAY LLP

By:___________________________

Robert C. Morgan (admitted *pro hac vice*)
Laurence S. Rogers (admitted *pro hac vice*)
Matthew A. Traupman (admitted *pro hac vice*)
1211 Avenue of the Americas
New York, New York 10036-8704
Telephone: (212) 596-9000
Facsimile: (212) 596-9090

THE ROTH LAW FIRM
Carl R. Roth
Texas Bar No. 17312000
Brendan C. Roth
Texas Bar No. 24040132
Amanda A. Abraham
Texas Bar No. 24055077
115 N. Wellington, Suite 200
Marshall, Texas 75670
Telephone: (903) 935-1665
Facsimile: (903) 935-1797

Attorneys for Plaintiffs Certicom Corp. and Certicom Patent Holding Corp.

APPENDIX A

References

[1] *Advanced Access Content System (AACS): Introduction and Common Cryptographic Elements*, Rev. 0.91, Intel Corporation et al., February 17, 2006.

[2] *Digital Transmission Content Protection (DTCP) Specification*, Revision 1.4, February 28, 2005.

[3] *ANSI X9.62- 1998, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, January 7, 1999.

Definitions

As used herein, "Source Device" refers to the device that can send a stream of content. A "Sink Device" is one that can receive a stream of content. Multifunction devices such as PCs and record/playback devices such as digital VCRs can be both source and sink devices. *See* [2] [p. 12]

U.S. Patent No. 6,563,928

- filed April 1, 1999
- continuation of US 5,933,504, filed on May 17, 1996.
- priority to GB 9510035, filed on May 18, 1995.

a. Infringement of Claim 61

Claim 61	DTCP[2]
53. A method of establishing a session key for encryption of data between a pair of correspondents comprising the steps of one of said correspondents selecting a finite group G, establishing a subgroup S having an order q of the group G,	Each accused device identified in Section III.A can act as a Source Device, a Sink Device or both. When connected to one or more additional DTCP-enabled device(s) (manufactured by Sony or a third party), each accused device identified in Section III.B.1 operates in the following manner: Source Devices [A] and Sink Devices [B] of [2] establish Kauth (shared secret derived from DTCP authentication and ECDH key exchange) that is used as a session key for encryption of Kx into Ksx, which is sent from the Source Device [A] to the Sink Device [B] [2, Sect. 6.3.1, p. 37] Each of Defendants' Source Devices [A] and Sink Devices [B] of [2] select a finite group E. The group E is a composite group and, therefore, must have multiple subgroups, each of which may have an order q [2, Sect. 4.2.1.1, p. 22].

Claim 61	DTCP[2]
	Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
determining an element α of the subgroup S to generate greater than a predetermined number of the q elements of the subgroup S and	Each of Defendants' Source Devices [A] and Sink Devices [B] of [2] determine G of [2] which is α of claim 53. The basepoint G of [2] is a generator that generates r elements of at least one subgroup of the finite group where r is greater than a predetermined number [2, Sect. 4.2.1.1, p. 22]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
utilising said element α to generate a session key at said one correspondent.	Each of Defendants' Source Devices [A] and Sink Devices [B] of [2] utilize the basepoint G, i.e., α, to generate a session key, where the session key = x-coordinate of X_kY_v or Y_kX_v , which is the shared secret generated by the elliptic curve Diffie-Hellman (EC-DH) procedure of [2] [2, Sect. 4.4.3.2, p. 28]. The value X_k of [2] is combined with the generator G to obtain the value $X_v = X_k$ G. X_v is the first phase value sent from the Source Device [A] to the Sink Device [B] as shown in step 3a of Fig. 4.5.1 of [2] [2, Sect. 4.4.3.2, P. 28]. The first phase value, which is obtained by utilizing the generator basepoint G, is used by the Sink Device [B] to generate the session key. The value Y_k of [2] is combined with the generator G to obtain the value $Y_v = Y_k$ G. Y_v is the first phase value sent from the Sink Device [B] to the Source Device [A] as shown in step 3b of Fig. 4.5.1 of [2] [2, Sect. 4.4.3.2, P. 28]. The first phase value, which is obtained by utilizing the generator basepoint G, is used by the Source Device [A] to generate the session key. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
61. A method according to claim 53 wherein said subgroup is selected to have an order that is to be a function of the product of a pair of primes r, r' and said element α is a generator of a subgroup of an order of one of said primes r, r'.	Each accused device identified in Section III.A can act as a Source Device, a Sink Device or both. When connected to one or more additional DTCP-enabled device(s) (manufactured by Sony or a third party), each accused device identified in Section III.B.1 operates in the following manner: Each of Defendants' Source Devices [A] and Sink Devices [B] of [2] use a finite group that includes three subgroups of prime order, namely r', r'', and r'''. The finite group has an order r'r''r''', and accordingly is a function of a product of a pair of primes. One of those subgroups that has a prime order is generated by the basepoint G of [2]. Thus, a subgroup is selected to have an order that is to be a function of the product of a pair of primes and the element G of [2] is a generator of a subgroup of an order of one of the primes. Accordingly, each of Defendants' Source Devices [A]

Claim 61	DTCP[2]
	and Sink Devices [B] infringe this claim. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.

APPENDIX B

References

[1] *Advanced Access Content System (AACS): Introduction and Common Cryptographic Elements*, Rev. 0.91, Intel Corporation et al., February 17, 2006.

[2] *Digital Transmission Content Protection (DTCP) Specification*, Revision 1.4, February 28, 2005.

[3] *ANSI X9.62- 1998*, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, January 7, 1999.

Definitions

As used herein, "Source Device" refers to the device that can send a stream of content. A "Sink Device" is one that can receive a stream of content. Multifunction devices such as PCs and record/playback devices such as digital VCRs can be both source and sink devices. *See* [2] [p. 12]

U.S. Patent No. 6,704,870

- filed August 29, 2001
- priority to US 5,999,626, filed on April 16, 1996.

a. Infringement of Claim 3

Claim 3	DTCP[2]
1. A method of generating a signature on a message m in an elliptic curve cryptographic system having a seed point P on an elliptic curve of order e over a finite field, said method comprising the steps of: i) selecting as a session key an integer k and computing representation of a corresponding point kP;	Each accused device identified in Section III.B.1 can act as a Source Device, a Sink Device or both. When connected to one or more additional DTCP-enabled device(s) (manufactured by Sony or a third party), each accused device identified in Section III.B.1 operates in the following manner: Source Devices [A] and Sink Devices [B], generate a message signature using EC-DSA [2, Sect. 4.5.1, p. 29; Fig. 9]. The basepoint G of [2] is a seed point on the elliptic curve E of order e [2, Sect. 4.2.11, p. 22 and Sect. 4.4.3, p. 26] . "E denotes the elliptic curve over the finite field GF(p) of p elements" [2, Sect. 4.2.1.1, p. 22 and Sect. 4.4.3, p. 26]. Step 1 of Section 4.4.3.1 of [2] includes generating "a random value, u, satisfying $0 < u < r$. A new value for u is generated for every signature..." Thus, u of [2] is k of claim 1 and is a session key for "every signature" [2, Sect. 4.4.3.1, Signature, Algorithm, Step 1, p. 27] .

Claim 3	DTCP[2]
	Step 1 of Section 4.4.3.1 of [2] includes calculating "the elliptic curve point, V = uG." This is kP of claim 1 [2, Sect. 4.4.3.1, Signature, Algorithm, Step 1, p. 27] Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
ii) deriving from said representation a first signature component, r, independent of said message, m;	Step 2 of Section 4.4.3.1 of [2] includes calculating "c = x_v mod r (the x-coordinate of V reduced modulo r)." c of [2] is r of claim 1 [2, Sect. 4.4.3.1, Signature, Algorithm, Step 2, p. 27]. c of [2] is derived independent of the message M of [2] [2, Sect. 4.4.3.1, Signature Input and Verification Input, p. 27]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
iii) combining said first signature component, r, with a private key, a, a value derived from said message, m, and said session key, k, to obtain a second signature component, s, containing said private key, a, and said session key, k, such that extraction of either is inhibited even when said signature components, r,s, are made public;	Steps 3-5 of Section 4.4.3.1 of [2] include calculating the EC-DSA signature components c and d [2, p. 27]. Section 4.4.3.1 of [2] defines X^{-1} as "the private key of the signing device (must be kept secret)." This is the "private key, a," of claim 1 [2, Sect. 4.4.3.1, Signature, Input, p. 27] Step 3 of Section 4.4.3.1 of [2] includes the calculation of "f = [SHA-1(M)]." This is "a value derived from said message, m, " of claim 1 [2, Sect. 4.4.3.1, Signature, Algorithm, Step 3, p. 27]. Step 4 of Section 4.4.3.1 of [2] includes the calculation of "d = $[u^{-1}(f + cX^{-1})]$ mod r" where "$u^{-1}$is the modular inverse of u mod r ". d is the "second signature component" obtained by "combining said first signature component, r," which is c of [2],"with the private key, a," which is X^{-1} of [2], "a value derived from said message," which is f of [2], "and said session key, k," which is u of [2] [2, Sect. 4.4.3.1, Signature, Algorithm, Step 4, p. 27]. The signature components c and d of [2] are r and s of claim 1. The signature components c and d are represented as c || d = S_X^{-1}[M] [2, Sect. 4.4.3.1, Signature, Algorithm, Step 5, p. 27]. Using this form of signature, the extraction of either u or X^{-1} of [2] is inhibited even when the signature components c and d are made public. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
and iv) utilizing said signature components r, s, in the signature of the message, m.	Each of Defendants' source and sink devices use a message signature... [2, Sect. 4.5.1, Step 3, p. 29]. c || d of [2] are r, s of claim 1 [2, Sect. 4.4.3.1, Signature, Algorithm, Step 5, p. 27] Step 3 of Section 4.5.1 of [2] indicates that the message M of [2, Sect. 4.4.3.1, p. 27] includes "the EC-DH key

Claim 3	DTCP[2]
	exchange first-phase value, Renewability message Version Number and Generation of the system renewability message store by the device" and "the other device's random challenge" [2, Sect. 4.5.1, Step 3, p. 29] which is m of claim 1. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
2. A method according to claim 1 wherein said value derived from said message, m, is obtained by applying a hash function to said message.	Each accused device identified in Section III.B.1 can act as a Source Device, a Sink Device or both. When connected to one or more additional DTCP-enabled device(s) (manufactured by Sony or a third party), each accused device identified in Section III.B.1 operates in the following manner: Step 3 of Section 4.4.3.1 of [2] includes the calculation of "f = [SHA-1(M)]" which is "a value derived from said message, m, " of claim 1 [2, Sect. 4.4.3.1, Signature, Algorithm, Step 3, p. 27]. Section 4.4 states that "SHA-1 is the algorithm used to generate a message digest...calculated from message" [2, Sect. 4.4.1, SHA-1 (Secure Hash Algorithm, revision 1), p. 25]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
3. A method according to claim 2 wherein said second signature component, s, is of the form $s=k^{-1}\{h(m)+ar\}$ mod q, where q is a divisor of the order, e, of said elliptic curve and h(m) is said value derived by applying a hash function to said message.	Each accused device identified in Section III.B.1 can act as a Source Device, a Sink Device or both. When connected to one or more additional DTCP-enabled device(s) (manufactured by Sony or a third party), each accused device identified in Section III.B.1 operates in the following manner: Step 4 of Section 4.4.3.1 of [2] includes the calculation of "$d = [u^{-1}(f + cX^{-1})]$ mod r" where "$u^{-1}$is the modular inverse of u mod r ". [2, Sect. 4.4.3.1, Signature, Algorithm, Step 4, p. 27]. d of [2] is the "second signature component, s" of claim 3. c of [2] is r of claim 3. X^{-1} of [2] is a of claim 3. f of [2] is h(m) of claim 3. u of [2] is k of claim 3. r of [2] is q of claim 3 [4, Sect. 7.1.1, p. 27] [2, Sect. 4.2.1.1, p. 22]. Each of Defendants' Source Devices [A] and Sink Devices [B] of [2] use an elliptic curve having an order of the elliptic curve, which is e of claim 3, that includes three subgroups of prime order of a finite group. One of the elliptic curve's subgroups of prime order is generated by the basepoint G of [2] that has a prime order r, which

Claim 3	DTCP[2]
	is q of claim 3, resulting in r being a divisor of the order of the elliptic curve [2, Sect. 4.2.1.1, p. 22]. Accordingly, each of Defendants' Source Devices [A] and Sink Devices [B] infringe this claim. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.

b. Infringement of Claim 18

Claim 18	DTCP[2]
1. A method of generating a signature on a message m in an elliptic curve cryptographic system having a seed point P on an elliptic curve of order e over a finite field, said method comprising the steps of: i) selecting as a session key an integer k and computing representation of a corresponding point kP;	Each accused device identified in Section III.B.1 can act as a Source Device, a Sink Device or both. When connected to one or more additional DTCP-enabled device(s) (manufactured by Sony or a third party), each accused device identified in Section III.B.1 operates in the following manner: Each of Defendants' Source Devices [A] and Sink Devices [B], generate a message signature using EC-DSA [2, Sect. 4.5.1, p. 29; Fig. 9]. The basepoint G of [2] is a seed point on the elliptic curve E of order e [2, Sect. 4.2.11, p. 22 and Sect. 4.4.3, p. 26] . "E denotes the elliptic curve over the finite field GF(p) of p elements" [2, Sect. 4.2.1.1, p. 22 and Sect. 4.4.3, p. 26]. Step 1 of Section 4.4.3.1 of [2] includes generating "a random value, u, satisfying $0 < u < r$. A new value for u is generated for every signature..." Thus, u of [2] is k of claim 1 and is a session key for "every signature" [2, Sect. 4.4.3.1, Signature, Algorithm, Step 1, p. 27] . Step 1 of Section 4.4.3.1 of [2] includes calculating "the elliptic curve point, V = uG." This is kP of claim 1 [2, Sect. 4.4.3.1, Signature, Algorithm, Step 1, p. 27] Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
ii) deriving from said representation a first signature component, r, independent of said message,m;	Step 2 of Section 4.4.3.1 of [2] includes calculating "c = x_v mod r (the x-coordinate of V reduced modulo r)." c of [2] is r of claim 1 [2, Sect. 4.4.3.1, Signature, Algorithm, Step 2, p. 27]. c of [2] is derived independent of the message M of [2] [2, Sect. 4.4.3.1, Signature Input and Verification Input, p. 27]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
iii) combining said first signature component, r, with a private key, a, a value derived from said message, m,	Steps 3-5 of Section 4.4.3.1 of [2] include calculating the EC-DSA signature components c and d [2, p. 27]. Section 4.4.3.1 of [2] defines X^{-1} as "the private key of

Claim 18	DTCP[2]
and said session key, k, to obtain a second signature component, s, containing said private key, a, and said session key, k, such that extraction of either is inhibited even when said signature components, r,s, are made public;	the signing device (must be kept secret)." This is the "private key, a," of claim 1 [2, Sect. 4.4.3.1, Signature, Input, p. 27] Step 3 of Section 4.4.3.1 of [2] includes the calculation of "f = [SHA-1(M)]." This is "a value derived from said message, m, " of claim 1 [2, Sect. 4.4.3.1, Signature, Algorithm, Step 3, p. 27]. Step 4 of Section 4.4.3.1 of [2] includes the calculation of "d = [u^{-1}(f + cX^{-1})] mod r" where "$u^{-1}$is the modular inverse of u mod r ". d is the "second signature component" obtained by "combining said first signature component, r," which is c of [2],"with a private key, a," which is X^{-1} of [2], a "value derived from said message, m," which is h(m) of [2], and "said session key, k," which is u of [2] [2, Sect. 4.4.3.1, Signature, Algorithm, Step 4, p. 27]. The signature components c and d of [2] are r and s of claim 1. The signature components c and d are represented as c || d = S_X^{-1}[M] [2, Sect. 4.4.3.1, Signature, Algorithm, Step 5, p. 27]. Using this form of signature, the extraction of either u or X^{-1} of [2] is inhibited even when the signature components c and d are made public. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
and iv) utilizing said signature components r,s, in the signature of the message, m.	Each of Defendants' source devices and sink devices use a message signature... [2, Sect. 4.5.1, Step 3, p. 29]. c || d of [2] are r, s of claim 1 [2, Sect. 4.4.3.1, Signature, Algorithm, Step 5, p. 27] Step 3 of Section 4.5.1 of [2] indicates that the message M of [2, Sect. 4.4.3.1, p. 27] includes "the EC-DH key exchange first-phase value, Renewability message Version Number and Generation of the system renewability message stored by the device" and "the other device's random challenge" [2, Sect. 4.5.1, Step 3, p. 29] which is m of claim 1. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
18. A method according to claim 1 wherein said second signature component s has a value corresponding to $\mathbf{s}=k^{-1}\ \{h(m)+ar\}$ mod q.	Each accused device identified in Section III.B.1 can act as a Source Device, a Sink Device or both. When connected to one or more additional DTCP-enabled device(s) (manufactured by Sony or a third party), each accused device identified in Section III.B.1 operates in the following manner: Step 4 of Section 4.4.3.1 of [2] includes the calculation of the second signature component d where "d = [u^{-1}(f + cX^{-1})] mod r" where "$u^{-1}$is the modular inverse of u mod r ". [2, Sect. 4.4.3.1, Signature, Algorithm, Step 4, p.

Claim 18	DTCP[2]
	27]. d of [2] is the "second signature component s" of claim 18. c of [2] is r of claim 18. X^{-1} of [2] is a of claim 18. f of [2] is h(m) of claim 18. u of [2] is k of claim 18. r of [2] is q of claim 18 [2, Sect. 4.2.1.1, p. 22]. Accordingly, each of Defendants' Source Devices [A] and Sink Devices [B] infringe this claim. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.

c. Infringement of Claim 22

Claim 22	DTCP[2]
21. A method of generating a digital signature r, s, of a message m using an elliptic curve cryptosystem employing an elliptic curve of order e, said method comprising the steps of: i) selecting an integer k and determining a corresponding point kP where P is point on the curve;	Each accused device identified in Section III.B.1 can act as a Source Device, a Sink Device or both. When connected to one or more additional DTCP-enabled device(s) (manufactured by Sony or a third party), each accused device identified in Section III.B.1 operates in the following manner: Each of Defendants' Source Devices [A] and Sink Devices [B], generate a message signature using EC-DSA [2, Sect. 4.5.1, p. 29; Fig. 9]. Each device uses a message signature... [2, Sect. 4.5.1, Step 3, p. 29]. c || d of [2] are r, s of claim 21 [2, Sect. 4.4.3.1, Signature, Algorithm, Step 5, p. 27] The basepoint G of [2] is a seed point on the elliptic curve E of order e. G of [2] is the point P of claim 21 [2, Sect. 4.2.11, p. 22 and Sect. 4.4.3, p. 26] . Step 1 of Section 4.4.3.1 of [2] includes generating "a random value, u, satisfying 0 < u < r. A new value for u is generated for every signature..." Thus, u of [2] is k of claim 21 and is an integer session key for "every signature" [2, Sect. 4.4.3.1, Signature, Algorithm, Step 1, p. 27] . Step 1 of Section 4.4.3.1 of [2] includes calculating "the elliptic curve point, V = uG" which is kP of claim 21 [2, Sect. 4.4.3.1, Signature, Algorithm, Step 1, p. 27] Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
ii) selecting a coordinate (x) of the	Step 2 of Section 4.4.3.1 of [2] includes calculating "c =

Claim 22	DTCP[2]
point kP;	x_v mod r (the x-coordinate of V reduced modulo r)." c of [2] is r of claim 21 [2, Sect. 4.4.3.1, Signature, Algorithm, Step 2, p. 27]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
iii) reducing the coordinate mod q where q is a known divisor of e, to obtain a first component r; and	Step 2 of Section 4.4.3.1 of [2] states that c is "the x-coordinate of V reduced modulo r," c of [2] is r of claim 21 [2, Sect. 4.4.3.1, Signature, Algorithm, Step 2, p. 27]. r of [2] is q of claim 21 [2, Sect. 4.2.1.1, p. 22]. Each of Defendants' Source Devices [A] and Sink Devices [B] of [2] use an elliptic curve having an order of the elliptic curve, which is e of claim 3, that includes three subgroups of prime order of a finite group. One of the elliptic curve's subgroups of prime order is generated by the basepoint G of [2] that has a prime order r, which is q of claim 3, resulting in r being a divisor of the order of the elliptic curve [2, Sect. 4.2.1.1, p. 22]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
iv) combining said first component, r, with a long-term private key a and said integer k to obtain a second signature component s, such that extraction of either said long term private key a or said integer k is inhibited even when said signature r,s, are made public.	Steps 3-5 of Section 4.4.3.1 of [2] include calculating the EC-DSA "signature" components c and d [2, p. 27]. These are r and s of claim 21. Section 4.4.3.1 of [2] defines X^{-1} as "the private key of the signing device (must be kept secret)." This is the "long-term private key a" of claim 21 [2, Sect. 4.4.3.1, Signature, Input, p. 27] Step 4 of Section 4.4.3.1 of [2] includes the calculation of "$d = [u^{-1}(f + cX^{-1})]$ mod r" where "$u^{-1}$is the modular inverse of u mod r ". d is the "second signature component" obtained by "combining said first component, r," which is c of [2]," with the "long-term private key a," which is $X^{-1}$of [2], and "said integer k," which is u of [2] [2, Sect. 4.4.3.1, Signature, Algorithm, Step 4, p. 27]. The signature components c and d of [2] are r and s of claim 21. The signature components c and d are represented as c || d = $S_X^{-1}[M]$ [2, Sect. 4.4.3.1, Signature, Algorithm, Step 5, p. 27]. Using this form of signature, the extraction of either u or X^{-1} of [2] is inhibited even when the signature components c and d of [2] are made public. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
22. A method according to claim 21 wherein said second signature component s has the form $s=k^{-1}$ {h(m)+ar} mod q, where h(m) is a	Each accused device identified in Section III.B.1 can act as a Source Device, a Sink Device or both. When connected to one or more additional DTCP-enabled device(s) (manufactured by Sony or a third party), each accused device identified in Section III.B.1 operates in

Claim 22	**DTCP[2]**
hash of the message m.	the following manner: Step 4 of Section 4.4.3.1 of [2] includes the calculation of "d = [u^{-1}(f + cX^{-1})] mod r" where "$u^{-1}$is the modular inverse of u mod r ". [2, Sect. 4.4.3.1, Signature, Algorithm, Step 4, p. 27]. d of [2] is the "second signature component s" of claim 22. c of [2] is r of claim 22. X^{-1} of [2] is a of claim 22. f of [2] is h(m) of claim 22. u of [2] is k of claim 22. r of [2] is q of claim 22 [2, Sect. 4.2.1.1, p. 22]. Step 3 of Section 4.5.1 of [2] indicates that the message M of [2, Sect. 4.4.3.1, p. 27] includes "the EC-DH key exchange first-phase value, Renewability message Version Number and Generation of the system renewability message stored by the device" and "the other device's random challenge" [2, Sect. 4.5.1, Step 3, p. 29] which is m of claim 22. Accordingly, each of Defendants' Source Devices [A] and Sink Devices [B] infringe this claim. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.

APPENDIX C

References

[1] *Advanced Access Content System (AACS): Introduction and Common Cryptographic Elements*, Rev. 0.91, Intel Corporation et al., February 17, 2006.

[2] *Digital Transmission Content Protection (DTCP) Specification*, Revision 1.4, February 28, 2005.

[3] *ANSI X9.62- 1998*, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, January 7, 1999.

[4] *Advanced Access Content System (AACS): Pre-recoded Video Book*, Rev. 092, Intel Corporation et al., November 29, 2007.

[5] *Advanced Access Content System (AACS): Blu-ray Disk Pre-recoded Book*, Rev. 0912, Intel Corporation et al., July 27, 2006.

[6] *Advanced Access Content System (AACS): Blu-ray Disk Recordable Book*, Rev. 092, Intel Corporation et al., July 24, 2006.

U.S. Patent No. 6,704,870

- filed August 29, 2001
- priority to US 5,999,626, filed on April 16, 1996.

a. Infringement of Claim 3

Claim 3	AACS [1]
1. A method of generating a signature on a message m in an elliptic curve cryptographic system having a seed point P on an elliptic curve of order e over a finite field, said method comprising the steps of: i) selecting as a session key an integer k and computing representation of a corresponding point kP;	Section 2.3 of [1] states "All digital signatures in AACS utilize the ECDSA digital signature scheme" in [3] [1, Sect. 2.3, p. 10]. Each accused device identified in Section III.B.2 contains either a Blu-ray disc or it contains a Blu-ray drive. When an accused device containing a Blu-ray disk is inserted into a Blu-ray drive (whether one of Sony's drive or a drive of a third party) or when an accused device that contains a Blu-ray drive has a Blu-ray disc (whether one of Sony's discs or a disc of a third party) inserted in it, each accused device identified in Section III.B.2 operates in the following manner: Each of the AACS Optical Drive and Host generate signatures D_{sig} and H_{sig} [1, p. 32; Fig. 4-6].

Claim 3	AACS [1]
	The Base Point G of [1] is the seed point P of claim 1 "on an elliptic curve" of order e "defined over GF(p)" [1, Table 2-1, p. 10 and p. 33, step 19] . Step 18 of Section 4.3 of [1] refers to the generation of a session key for the drive and states "the drive generates 160 bits random number as D_K" [1, p. 33, step 18]. D_K is the session key integer k of claim 1. Step 23 of Section 4.3 of [1] refers to the generation of a session key for the host and states "the host generates 160 bits random number as H_K" [1, p. 33, step 23]. H_K is the session key integer k of claim 1. Step 19 of Section 4.3 of [1] states "the drive calculates a point on the elliptic curve D_V" such that "$D_V = D_K$ G where G is the base point of the elliptic curve" [1, p. 33, step 19]. Dv of [1] is kP of claim 1. Step 24 of Section 4.3 of [1] states "the host calculates a point on the elliptic curve H_V" such that "$H_V = H_K$ G where G is the base point of the elliptic curve" [1, p. 33, step 24]. Hv of [1] is kP of claim 1. Each accused instrumentality that contains a Blu-ray drive includes at least one of a signed Drive Certificate and signed Host Certificate [4, p. 30]. Each Blu-ray disc includes at least one of a signed Content Certificate, a signed Certificate Revocation List (CRL), a signed Host Revocation List (HRL), a signed Drive Revocation List (DRL) [4, p. 5, Fig. 2-1], and a signed End of Media Key Block (MKB) Record [1, p. 25, Table 3-10] [5, p. 6-12] [6, p.7-9, Sect.2]. Each of the signed Drive Certificate, Host Certificate, Content Certificate, CRL, HRL, DRL, and End of MKB Record include an ECDSA signature. “k” and “kP” are generated [3, p. 28-29, Sect. 5.3]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
ii) deriving from said representation a first signature component, r, independent of said message, m;	Section 2.3 of [1] states "All digital signatures in AACS utilize the ECDSA digital signature scheme" in [3] [1, Sect. 2.3, p. 10]. Step 2 of Section 5.3.2 of [3] states "Compute the elliptic curve point $(x_1, y_1) = kG$" [3, Sect. 5.3.3, p. 29]. Step 1 of Section 5.3.3 of [3] states "Convert the field element x_1 into an integer x_1." Step 2 of Section 5.3.3 of [3] states "Set $r = x_1 \bmod n$" [3, Sect. 5.3.3, p. 29]. Steps 1 and 2 of [3] include deriving the first signature component r of [3] from x_1 of [3], which is derived from the elliptic curve point for kG of [3] and is also independent of a message M [3, Sect. 5.3, p. 28]. The message M of [3, Sect. 5.3, p. 28] includes Hn || Dv or Dn || Hv of [1, Fig. 4-6, p. 32]. This is m of claim 1. Each ECDSA signature on Blu-ray drive or a Blu-ray disc includes a first signature component r and a message

Claim 3	AACS [1]
	M (one or more of the content hash, Host Certificate, Drive Certificate, CRL, HRL, DRL or MKB) [3, p. 28-29, Sect. 5.3]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
iii) combining said first signature component, r, with a private key, a, a value derived from said message, m, and said session key, k, to obtain a second signature component, s, containing said private key, a, and said session key, k, such that extraction of either is inhibited even when said signature components, r, s, are made public;	Section 2.3 of [1] states "All digital signatures in AACS utilize the ECDSA digital signature scheme" in [3] [1, Sect. 2.3, p. 10]. Section 2.3 refers to "K_{priv} (a scalar value satisfying $0 < k_{priv} < r$)." Each of the AACS_Drive$_{priv}$ of [1, Sect. 4.3, step 20, p. 33], AACS_Host$_{priv}$ of [1, Sect. 4.3, step 25, p. 33], and d of [3, Sect. 5.3.3, p. 29] is the "private key, a" of claim 1. Section 5.3.1 of [3] states "Compute the hash value e = H(M) using the hash function SHA-1" e of [3] is "a value derived from said message, m, " of claim 1. Step 4 of Section 5.3.3 of [3] includes the calculation of "$s = k^{-1}(e + dr) \bmod n$" [3, Sect. 5.3.3, p. 29]. s is the "second signature component" obtained by "combining said first signature component, r," which is r of [3],"with the private key, a," which is d of [3], "a value derived from said message, m," which is e of [3], "and said session key, k," which is k of [3]. The signature components r and s of [3] are S of [1, Sect. 2.3, p. 10]. These are r and s of claim 1. Using this form of signature, the extraction of either k or d of [3] is inhibited even when the signature components r and s are made public. Each ECDSA signature on a Blu-ray drive or a Blu-ray disc includes a second signature component, s, that contains a private key and a session key k [3, p. 28-29, Sect. 5.3]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
and iv) utilizing said signature components r, s, in the signature of the message, m.	D_{sig} or H_{sig} of [1, Sect. 4.3, steps 20 and 25, p. 33] is S of [1, p. 10]. S is a signature of a message that includes r and s of [3, Sect. 5.3.3, p. 29]. These are r and s of claim 1. The Drive utilizes D_{sig} of a message from the Drive. The Host utilizes H_{sig} of a message from the Host. [1, Fig. 4-6, p.32] [1, Sect. 4.3, Steps 20-21, Steps 25-26, pp. 33-34]. The message M of [3, Sect. 5.3, p. 28] is D of [1, p. 10]. D of [1] includes Hn || Dv or Dn || Hv of [1, Fig. 4-6, p. 32]. This is m of claim 1. Each ECDSA signature on a Blu-ray drive or a Blu-ray disc utilizes the signature components r and s in the signature of the message [3, p. 28-29, Sect. 5.3].

Claim 3	**AACS [1]**
	Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
2. A method according to claim 1 wherein said value derived from said message, m, is obtained by applying a hash function to said message.	Each accused device identified in Section III.B.2 contains either a Blu-ray disc or it contains a Blu-ray drive. When an accused device containing a Blu-ray disk is inserted into a Blu-ray drive (whether one of Sony's drive or a drive of a third party) or when an accused device that contains a Blu-ray drive has a Blu-ray disc (whether one of Sony's discs or a disc of a third party) inserted in it, each accused device identified in Section III.B.2 operates in the following manner: Section 5.3.1 of [3] states "Compute the hash value e = H(M) using the hash function SHA-1." e of [3] is "a value derived from said message, m, " of claim 2 [3, Section 5.3.1, p. 28]. Each ECDSA signature on a Blu-ray drive or a Blu-ray disc utilizes the hash of the message M in the second signature component, s [3, p. 28-29, Sect. 5.3]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
3. A method according to claim 2 wherein said second signature component, s, is of the form s=k^{-1} {h(m)+ar} mod q, where q is a divisor of the order, e, of said elliptic curve and h(m) is said value derived by applying a hash function to said message.	Each accused device identified in Section III.B.2 contains either a Blu-ray disc or it contains a Blu-ray drive. When an accused device containing a Blu-ray disk is inserted into a Blu-ray drive (whether one of Sony's drive or a drive of a third party) or when an accused device that contains a Blu-ray drive has a Blu-ray disc (whether one of Sony's discs or a disc of a third party) inserted in it, each accused device identified in Section III.B.2 operates in the following manner: Step 4 of Section 5.3.3 of [3] includes the calculation of "s = k^{-1}(e + dr) mod n" [3, Sect. 5.3.3, p. 29]. s of [3] is s of claim 3. r of [3] is r of claim 3. d of [3] is a of claim 3. e of [3] is h(m) of claim 3. k of [3] is k of claim 3. Section 2.2 of [3] defines n as "The order of the base point G" [3, Sect. 2.2, p. 8]. n of [3] is r of [1] which is "Order of Base Point" [1, Table 2-1, p. 10]. This is q of claim 3. u = #E(Fq) of [3] is the number of points on the curve corresponding to e of claim 3. n is selected according to appendix A.3.1 of [3] such that u = hn. Accordingly, h= u/n and n, which is q of claim 3, is a divisor of the order e of the curve of claim 3. Section 5.3.1 of [3] states "Compute the hash value e = H(M) using the hash function SHA-1" [3, Section 5.3.1, p. 28].

Claim 3	AACS [1]
	Accordingly, each of Defendants' AACS Optical Drives and Hosts infringe this claim. Each ECDSA signature on a Blu-ray drive or a Blu-ray disc utilizes a second signature component in the form of $s = k^{-1}(e + dr) \bmod q$ [3, p. 28-29, Sect. 5.3]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.

b. Infringement of Claim 18

Claim 18	AACS[1]
1. A method of generating a signature on a message m in an elliptic curve cryptographic system having a seed point P on an elliptic curve of order e over a finite field, said method comprising the steps of: i) selecting as a session key an integer k and computing representation of a corresponding point kP;	Section 2.3 of [1] states "All digital signatures in AACS utilize the ECDSA digital signature scheme" in [3] [1, Sect. 2.3, p. 10]. Each accused device identified in Section III.B.2 contains either a Blu-ray disc or it contains a Blu-ray drive. When an accused device containing a Blu-ray disk is inserted into a Blu-ray drive (whether one of Sony's drive or a drive of a third party) or when an accused device that contains a Blu-ray drive has a Blu-ray disc (whether one of Sony's discs or a disc of a third party) inserted in it, each accused device identified in Section III.B.2 operates in the following manner: Each of the AACS Optical Drive and Host generate signatures D_{sig} and H_{sig} [1, p. 32; Fig. 4-6]. Section 2.3 of [1] states "All digital signatures in AACS utilize the ECDSA digital signature scheme" in [3] [1, Sect. 2.3, p. 10] The Base Point G of [1] is the seed point P of claim 1 "on an elliptic curve" of order e "defined over GF(p)" [1, Table 2-1, p. 10 and p. 33, step 19] . Step 18 of Section 4.3 of [1] refers to the generation of a session key for the drive and states "the drive generates 160 bits random number as D_K" [1, p. 33, step 18]. D_K is the session key integer k of claim 1. Step 23 of Section 4.3 of [1] refers to the generation of a session key for the host and states "the drive generates 160 bits random number as H_K" [1, p. 33, step 23]. H_K is the session key integer k of claim 1. Step 19 of Section 4.3 of [1] states "the drive calculates a point on the elliptic curve D_V" such that "$D_V = D_K$ G where G is the base point of the elliptic curve" [1, p. 33, step 19]. Dv of [1] is kP of claim 1. Step 24 of Section 4.3 of [1] states "the host calculates a point on the elliptic curve H_V" such that "$H_V = H_K$ G where G is the base point of the elliptic curve" [1, p. 33,

Claim 18	AACS[1]
	step 24]. Hv of [1] is kP of claim 1. Each accused instrumentality that contains a Blu-ray drive includes at least one of a signed Drive Certificate and signed Host Certificate [4, p. 30]. Each Blu-ray disc includes at least one of a signed Content Certificate, a signed Certificate Revocation List (CRL), a signed Host Revocation List (HRL), a signed Drive Revocation List (DRL) [4, p. 5, Fig. 2-1], and a signed End of Media Key Block (MKB) Record [1, p. 25, Table 3-10] [5, p. 6-12] [6, p.7-9, Sect.2]. Each of the signed Drive Certificate, Host Certificate, Content Certificate, CRL, HRL, DRL, and End of MKB Record include an ECDSA signature. “k” and “kP” are generated [3, p. 28-29, Sect. 5.3]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
ii) deriving from said representation a first signature component, r, independent of said message, m;	Section 2.3 of [1] states "All digital signatures in AACS utilize the ECDSA digital signature scheme" in [3] [1, Sect. 2.3, p. 10]. Step 2 of Section 5.3.2 of [3] states "Compute the elliptic curve point $(x_1, y_1) = kG$" [3, Sect. 5.3.3, p. 29]. Step 1 of Section 5.3.3 of [3] states "Convert the field element x_1 into an integer x_1." Step 2 of Section 5.3.3 of [3] states "Set $r = x_1 \bmod n$" [3, Sect. 5.3.3, p. 29]. Steps 1 and 2 of [3] include deriving the first signature component r of [3] from x_1 of [3], which is derived from the elliptic curve point for kG of [3] and is also independent of a message M [3, Sect. 5.3, p. 28]. The message M of [3, Sect. 5.3, p. 28] includes Hn || Dv or Dn || Hv of [1, Fig. 4-6, p. 32]. This is m of claim 1. Each ECDSA signature on a Blu-ray drive or a Blu-ray disc includes a first signature component r and a message M (one or more of the content hash, Drive Certificate, Host Certificate, CRL, HRL, DRL or MKB) [3, p. 28-29, Sect. 5.3]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
iii) combining said first signature component, r, with a private key, a, a value derived from said message, m, and said session key, k, to obtain a second signature component, s, containing said private key, a, and said session key, k, such that extraction of either is inhibited even when said signature components, r, s, are made public;	Section 2.3 of [1] states "All digital signatures in AACS utilize the ECDSA digital signature scheme" in [3] [1, Sect. 2.3, p. 10]. Section 2.3 refers to "K_{priv} (a scalar value satisfying $0 < k_{priv} < r$)." Each of the AACS_Drive$_{priv}$ of [1, Sect. 4.3, step 20, p. 33], AACS_Host$_{priv}$ of [1, Sect. 4.3, step 25, p. 33] and d of [3, Sect. 5.3.3, p. 29] is the "private key, a" of claim 1. Section 5.3.1 of [3] states "Compute the hash value e = H(M) using the hash function SHA-1." e of [3] is "a value derived from said message, m, " of claim 1. Step 4 of Section 5.3.3 of [3] includes the calculation of

Claim 18	AACS[1]
	"s = k^{-1}(e + dr) mod n" [3, Sect. 5.3.3, p. 29]. s of [3] is the "second signature component, s" of claim 1 which is obtained by "combining said first signature component, r," which is r of [3],"with the private key, a," which is d of [3], "a value derived from said message, m," which is e of [3], "and said session key, k," which is k of [3]. The signature components r and s of [3] are S of [1, Sect. 2.3, p. 10]. These are r and s of claim 1. Using this form of signature, the extraction of either k or d of [3] is inhibited even when the signature components r and s are made public. Each ECDSA signature on a Blu-ray drive or a Blu-ray disc includes a second signature component, s, that contains a private key a and a session key k [3, p. 28-29, Sect. 5.3]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
and iv) utilizing said signature components r, s, in the signature of the message, m.	D_{sig} or H_{sig} of [1, Sect. 4.3, steps 20 and 25, p. 33] is S of [1, p. 10]. S is a signature of a message that includes r and s of [3, Sect. 5.3.3, p. 29]. These are r and s of claim 1. The Drive utilizes D_{sig} of a message from the Drive. The Host utilizes H_{sig} of a message from the Host. [1, Fig. 4-6, p.32] [1, Sect. 4.3, Steps 20-21, Steps 25-26, pp. 33-34]. The message M of [3, Sect. 5.3, p. 28] is D of [1, p. 10] which includes Hn || Dv or Dn || Hv of [1, Fig. 4-6, p. 32]. This is m of claim 1. Each ECDSA signature on a Blu-ray drive or a Blu-ray disc utilizes the signature components r and s in the signature of the message [3, p. 28-29, Sect. 5.3]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
18. A method according to claim 1 wherein said second signature component s has a value corresponding to **s**=k^{-1} {h(m)+ar} mod q.	Each accused device identified in Section III.B.2 contains either a Blu-ray disc or it contains a Blu-ray drive. When an accused device containing a Blu-ray disk is inserted into a Blu-ray drive (whether one of Sony's drive or a drive of a third party) or when an accused device that contains a Blu-ray drive has a Blu-ray disc (whether one of Sony's discs or a disc of a third party) inserted in it, each accused device identified in Section III.B.2 operates in the following manner: Step 4 of Section 5.3.3 of [3] includes the calculation of "s = k^{-1}(e + dr) mod n" [3, Sect. 5.3.3, p. 29]. s of [3] is s of claim 18. r of [3] is r of claim 18. d of [3] is a of claim 18.

Claim 18	AACS[1]
	e of [3] is h(m) of claim 18. k of [3] is k of claim 18. Section 2.2 of [3] defines n as "The order of the base point G" [3, Sect. 2.2, p. 8]. n of [3] is r of [1] which is "Order of Base Point" [1, Table 2-1, p. 10]. This is q of claim 18. Accordingly, each of Defendants' AACS Optical Drives and Hosts infringe this claim. Each ECDSA signature on a Blu-ray drive or a Blu-ray disc utilizes a second signature component in the form of $s = k^{-1}(e + dr) \bmod q$ [3, p. 28-29, Sect. 5.3]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.

c. Infringement of Claim 22

Claim 22	AACS[1]
21. A method of generating a digital signature r, s, of a message m using an elliptic curve cryptosystem employing an elliptic curve of order e, said method comprising the steps of: i) selecting an integer k and determining a corresponding point kP where P is point on the curve;	Section 2.3 of [1] states "All digital signatures in AACS utilize the ECDSA digital signature scheme" in [3] [1, Sect. 2.3, p. 10]. Each accused device identified in Section III.B.2 contains either a Blu-ray disc or it contains a Blu-ray drive. When an accused device containing a Blu-ray disk is inserted into a Blu-ray drive (whether one of Sony's drive or a drive of a third party) or when an accused device that contains a Blu-ray drive has a Blu-ray disc (whether one of Sony's discs or a disc of a third party) inserted in it, each accused device identified in Section III.B.2 operates in the following manner: Each of the AACS Optical Drive and Host generate signatures D_{sig} and H_{sig} [1, p. 32; Fig. 4-6]. Section 2.3 of [1] states "All digital signatures in AACS utilize the ECDSA digital signature scheme" in [3] [1, Sect. 2.3, p. 10]. The Base Point G of [1] is the seed point P of claim 21 "on an elliptic curve" of order e "defined over GF(p)" [1, Table 2-1, p. 10 and p. 33, step 19] . Step 18 of Section 4.3 of [1] refers to the generation of a session key for the drive and states "the drive generates 160 bits random number as D_K" [1, p. 33, step 18]. D_K is the session key integer k of claim 21. Step 23 of Section 4.3 of [1] refers to the generation of a session key for the host and states "the drive generates 160 bits random number as H_K" [1, p. 33, step 23]. H_K is the session key integer k of claim 21.

Claim 22	AACS[1]
	Step 19 of Section 4.3 of [1] states "the drive calculates a point on the elliptic curve D_V" such that "$D_V = D_K$ G where G is the base point of the elliptic curve" [1, p. 33, step 19]. Dv of [1] is kP of claim 21. Step 24 of Section 4.3 of [1] states "the host calculates a point on the elliptic curve H_V" such that "$H_V = H_K$ G where G is the base point of the elliptic curve" [1, p. 33, step 24]. Hv of [1] is kP of claim 21. Each accused instrumentality that contains a Blu-ray drive includes at least one of a signed Drive Certificate and signed Host Certificate [4, p. 30]. Each Blu-ray disc includes at least one of a signed Content Certificate, a signed Certificate Revocation List (CRL), a signed Host Revocation List (HRL), a signed Drive Revocation List (DRL) [4, p. 5, Fig. 2-1], and a signed End of Media Key Block (MKB) Record [1, p. 25, Table 3-10] [5, p. 6-12] [6, p.7-9, Sect.2]. Each of the signed Host Certificate, Drive Certificate, Content Certificate, CRL, HRL, DRL, and End of MKB Record include an ECDSA signature. "k" and "kP" are generated [3, p. 28-29, Sect. 5.3]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
ii) selecting a coordinate (x) of the point kP;	Section 2.3 of [1] states "All digital signatures in AACS utilize the ECDSA digital signature scheme" in [3] [1, Sect. 2.3, p. 10]. Step 2 of Section 5.3.2 of [3] states "Compute the elliptic curve point (x_1, y_1) = kG" [3, Sect. 5.3.3, p. 29]. Step 1 of Section 5.3.3 of [3] states "Convert the field element x_1 into an integer x_1." Each ECDSA signature on a Blu-ray drive or a Blu-ray disc includes the step of selecting a coordinate (x) of the point kP [3, p. 28-29, Sect. 5.3]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
iii) reducing the coordinate mod q where q is a known divisor of e, to obtain a first component r; and	Section 2.3 of [1] states "All digital signatures in AACS utilize the ECDSA digital signature scheme" in [3] [1, Sect. 2.3, p. 10]. Step 2 of Section 5.3.3 of [3] states "Set $r = x_1$ mod n" [3, Sect. 5.3.3, p. 29]. Steps 1 and 2 of [3] include deriving the first signature component r of [3] from x_1 of [3], which is derived from the elliptic curve point for kG of [3] [3, Sect. 5.3, p. 28]. Section 2.2 of [3] defines n as "The order of the base point G" [3, Sect. 2.2, p. 8]. n of [3] is r of [1] which is "Order of Base Point" [1, Table 2-1, p. 10]. This is q of claim 21. u = #E(Fq) of [3] is the number of points on the curve corresponding to e of claim 21. n is selected according to appendix A.3.1 of [3] such that u = hn. Accordingly, h= u/n and n. which is q of claim 21, is a

Claim 22	**AACS[1]**
	divisor of the order e of the curve of claim 21. Each ECDSA signature on a Blu-ray drive or a Blu-ray disc includes the step of reducing the coordinate mod q to obtain a first component r [3, p. 28-29, Sect. 5.3]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
iv) combining said first component, r, with a long-term private key a and said integer k to obtain a second signature component s, such that extraction of either said long term private key a or said integer k is inhibited even when said signature r, s, are made public.	Section 2.3 of [1] states "All digital signatures in AACS utilize the ECDSA digital signature scheme" in [3] [1, Sect. 2.3, p. 10]. Section 2.3 refers to "K$_{priv}$ (a scalar value satisfying 0 < k$_{priv}$ <r)." Each of AACS_Drive$_{priv}$ of [1, Sect. 4.3, step 20, p. 33], AACS_Host$_{priv}$ of [1, Sect. 4.3, step 25, p. 33] and d of [3, Sect. 5.3.3, p. 29] is the "long-term private key a" of claim 21. Step 4 of Section 5.3.3 of [3] includes the calculation of "s = k^{-1}(e + dr) mod n" [3, Sect. 5.3.3, p. 29]. s of [3] is the "second signature component s" of claim 21 which is obtained by "combining said first signature component, r," which is r of [3],"with a long-term private key a," which is d of [3], "and said integer k," which is k of [3]. The signature components r and s of [3] are S of [1, Sect. 2.3, p. 10]. These are r and s of claim 21. Using this form of signature, the extraction of either k or d of [3] is inhibited even when the signature components r and s are made public. Each ECDSA signature on a Blu-ray drive or a Blu-ray disc includes a second signature component, s, that contains a private key and a session k [3, p. 28-29, Sect. 5.3]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.
22. A method according to claim 21 wherein said second signature component s has the form s=k^{-1} {h(m)+ar} mod q, where h(m) is a hash of the message m.	Section 2.3 of [1] states "All digital signatures in AACS utilize the ECDSA digital signature scheme" in [3] [1, Sect. 2.3, p. 10]. Each accused device identified in Section III.B.2 contains either a Blu-ray disc or it contains a Blu-ray drive. When an accused device containing a Blu-ray disk is inserted into a Blu-ray drive (whether one of Sony's drive or a drive of a third party) or when an accused device that contains a Blu-ray drive has a Blu-ray disc (whether one of Sony's discs or a disc of a third party) inserted in it, each accused device identified in Section III.B.2 operates in the following manner: Step 4 of Section 5.3.3 of [3] includes the calculation of "s = k^{-1}(e + dr) mod n" [3, Sect. 5.3.3, p. 29]. s of [3] is s of claim 22.

Claim 22	**AACS[1]**
	r of [3] is r of claim 22. d of [3] is a of claim 22. e of [3] is h(m) of claim 22. k of [3] is k of claim 22. n of [3] is q of claim 22. Section 5.3.1 of [3] states "Compute the hash value e = H(M) using the hash function SHA-1." e of [3] is "h(m)...a hash of the message m" of claim 22. Accordingly, each of Defendants' AACS Optical Drives and Hosts infringe this claim. Each ECDSA signature on a Blu-ray drive or a Blu-ray disc utilizes a second signature component in the form of $s = k^{-1}(e + dr) \bmod q$ [3, p. 28-29, Sect. 5.3]. Pursuant to P.R. 3-1(h), Certicom asserts that this claim element is, at least partially, a software limitation.