

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

MEDIA CONTENT PROTECTION
LLC,

Plaintiff,

v.

MEDIATEK INC., and MEDIATEK
USA INC.,

Defendants.

C.A. No.: 20-CV-1246-CFC

JURY TRIAL DEMANDED

SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Media Content Protection LLC (“MCP” or “Plaintiff”) brings this action for patent infringement under 35 U.S.C. § 271 against MediaTek Inc. and MediaTek USA Inc. (collectively, “MediaTek” or “Defendants”), and alleges as follows:

THE PARTIES

1. Plaintiff Media Content Protection LLC (“MCP”) is a limited liability company duly organized and existing under the laws of the State of Delaware with its principal place of business at 533 Congress Street, Portland, ME 04101.

2. Defendant MediaTek Inc. is a corporation duly organized and existing under the laws of the Taiwan with a principal place of business located at No. 1 Dusing Road 1, Hsinchu Science Park, Hsinchu City 30078, Taiwan.

3. Defendant MediaTek USA, Inc. is a corporation duly organized and existing under the laws of the State of Delaware with a principal place of business at 2840 Junction Avenue, San Jose, California 95134. Defendant MediaTek USA is a wholly owned subsidiary of MediaTek Inc.

4. Defendants, either themselves and/or through the activities of their subsidiaries, affiliates, or intermediaries (including distributors, retailers, and others), make, use, sell, offer for sale, and/or import throughout the United States, including within the District of Delaware (this “District”), products, such as digital video-capable integrated circuits and associated firmware that infringe the Asserted Patent, defined below. Defendants make, use, sell, offer for sale, and/or import digital video-capable integrated circuits, that they or their customers incorporate into digital video-capable devices that are made, used, sold, offered for sale, and/or imported throughout the United States, including within this District. These digital video-capable devices may include, but are not limited to, televisions, set top boxes, BLU-RAY/DVD players, laptops, desktops, all-in-one PCs, thin clients, tablets, smartphones, convertible PCs, workstations, servers, monitors, displays, projectors, video adapters, and/or video hubs.

5. Upon information and belief, Defendant MediaTek USA Inc. acts on Defendant MediaTek Inc.’s behalf in conducting business within this District and the United States.¹ Upon further information and belief, Defendants share overlapping officers and directors, methods of financing, and represents itself as a single entity under the MediaTek brand.

THE ASSERTED PATENT

U.S. Patent No. 10,298,564

6. United States Patent No. 10,298,564 (the “’564 Patent”) is entitled “Secure Authenticated Distance Measurement” and issued on May 21, 2019 to inventor Franciscus L. A. J. Kamperman. The ’564 Patent issued from United States Patent Application No. 16/117,019 filed on August 30, 2018. A copy of the ’564 Patent is attached hereto as Exhibit A.

¹ *MediaTek | 2019 Annual Report* at 105, F-103-104, F-223, F-228-30, retrieved from <https://cdn-www.mediatek.com/posts/2019-MediaTek-Annual-Report.pdf>.

7. By way of assignment, MCP owns all rights, title, and interest to the '564 Patent (the "Asserted Patent").

8. The Asserted Patent is valid and enforceable.

JURISDICTION AND VENUE

9. This is a civil action for patent infringement arising under the Patent Act, 35 U.S.C. § 1 *et seq.*

10. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

11. Venue in this District is proper pursuant to 28 U.S.C. §§ 1391(b), (c) and 1400(b) because Defendant MediaTek USA Inc. is incorporated and resides in the State of Delaware, Defendant MediaTek Inc. not a resident of the United States and may be sued in any judicial district, and both Defendants have committed acts of infringement in this District.

12. This Court has personal jurisdiction over Defendants. Defendant MediaTek USA Inc. is a resident of this District. Defendant MediaTek Inc. is not subject to jurisdiction in any state's courts of general jurisdiction and the exercise of personal jurisdiction over it is consistent with the United States Constitution and laws. Defendants have and do conduct business within the State of Delaware. Defendants, directly or through subsidiaries, affiliates, or intermediaries (including distributors, retailers, and others), ship, distribute, make, use, offer for sale, import and/or advertise (including by providing an interactive web page) their products and/or services in the United States and this District, and/or contribute to and actively induce their customers to ship, distribute, make, use, offer for sale, sell, import, and/or advertise (including the provision of interactive web pages) infringing products and/or services in the United States and this District. Defendants, directly or through subsidiaries, affiliates, or intermediaries (including distributors, retailers, and others), have purposefully and voluntarily placed one or more of their infringing

products, as described below, into the stream of commerce with the expectation that those products will be purchased, used, and/or incorporated into digital video-capable devices made, used, sold, offered for sale, and/or imported into the United States by customers and/or consumers in this District.

BACKGROUND

13. MCP incorporates the allegations of all of the foregoing paragraphs as if fully restated herein.

14. Koninklijke Philips N.V. (formerly known as Koninklijke Philips Electronics N.V.) (“Philips N.V.”) and Philips North America LLC (formerly known as Philips Electronics North America Corporation) (“Philips North America”) (collectively, “Philips”) is a world-renowned company that engages in research and development in numerous fields. One of these fields pertains to digital video-capable devices for delivering and displaying content to users. Exemplary products in this field include televisions, set top boxes, BLU-RAY/DVD players, laptops, desktops, all-in-one PCs, thin clients, tablets, smartphones, convertible PCs, workstations, servers, monitors, displays, projectors, video adapters, and/or video hubs. The Asserted Patent derives from Philips’s efforts in this field and claim protection for, among other things, delivering and displaying content to users.

15. Defendants made, used, sold, offered for sale, imported, tested, designed, and/or marketed in the United States digital video-capable integrated circuits and associated firmware for delivering and displaying content to users that infringe the Asserted Patent. Such digital video-capable integrated circuits and associated firmware are incorporated into digital video-capable devices made, used, sold, offered for sale or imported into the United States by companies, including but not limited to, Hisense Co. Ltd., TCL Industries Holdings Co., Dell Technologies Inc. and HP, Inc., and/or their affiliates, subsidiaries or intermediaries (the “Exemplary Customers”).

16. Defendants have actual notice of the Asserted Patent and of their infringement. Defendants received actual notice of the Asserted Patent at least as early as September 17, 2020 by way of a letter to Defendants dated September 17, 2020. That letter included allegations of infringement of the Asserted Patent. Additionally, the filing of the original Complaint and the First Amended Complaint also constitutes notice in accordance with 35 U.S.C. § 287.

17. With actual notice of the Asserted Patent, Defendants have directly infringed, and continue to directly infringe the Asserted Patent under 35 U.S.C. § 271(a) and (g) by one or more of making, using, selling and/or offering to sell, in this District and elsewhere in the United States, and importing into this District and elsewhere in the United States, certain infringing digital video-capable integrated circuits and associated firmware that infringe the Asserted Patent (the “Accused Products”), as further described in detail in Count I *infra*.

18. The Accused Products include, but are not limited to, all digital video-capable integrated circuits and associated firmware designed to facilitate digital video-capable playback supporting the HDCP 2.0 protocol and above (referred to hereafter as “HDCP 2+”) that Defendants, either themselves and/or through the activities of their subsidiaries, affiliates, including without limitation Mstar,² or intermediaries (including distributors, retailers, and others), make, use, sell, offer for sale, and/or import throughout the United States, including, but not limited to, the following products and/or product lines, their associated firmware/software, and/or any development boards or printed circuit board assemblies containing the same: MediaTek Dimensity; MediaTek Helio G, P, A, and X; MT5596; MT5597;

² MediaTek 2020 Annual Report at F-27, ¶ 1 (“For the purpose of reorganization, MStar Semiconductor, Inc. was dissolved due to the merger with MediaTek Inc. on January 1, 2019. Subsidiaries previously owned by MStar Semiconductor, Inc., were transferred to MediaTek Inc.”) retrieved from <https://cdn-www.mediatek.com/posts/2019-MediaTek-Annual-Report.pdf> on Sept. 16, 2020.

MT5598; MT8XXX; MT9XXX; MT5XXX; MT8XXX; MT9675; MT9686; MT9950; later generation products; and Mstar connected TV, Smart TV, and Set-Top Box Series including without limitation, MSD6886,³ MSDURN180, MST9U13V4; MST9U11H1. This list of Defendants' currently known digital video-capable integrated circuits and associated firmware is exemplary and, on information and belief, many other of Defendants' digital video-capable integrated circuits and associated firmware infringe the Asserted Patent.

19. Defendants have also indirectly infringed, and continue to indirectly infringe the Asserted Patent under 35 U.S.C. § 271(b) and (c). Defendants knew and intended to induce and contribute to the infringement of the Asserted Patent. The Accused Products have no substantial non-infringing use, are a material part of the invention of the Asserted Patent, especially made or especially adapted for use in an infringement of the Asserted Patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

20. Upon information and belief, Defendants possessed knowledge of the Asserted Patent and of their infringement even before the September 17, 2020 date of the original Complaint in this action.

21. For example, upon information and belief, Defendants possessed knowledge of the Asserted Patent, their infringement thereof, and their customers' infringement thereof on or shortly after February 12, 2020 when Philips N.V. filed a complaint for patent infringement against TTE Technology, Inc., TCL Corp., TCL Electronics Holdings Ltd., TCL King Electrical Appliances (Huizhou) Co. Ltd., TCL Moka Int'l Ltd., TCL Overseas Marketing Ltd., and TCL Industries Holdings Co., Ltd. ("TCL") in the United States District Court for the Central District of California, Western Division (C.A. No. 1:20-cv-1406), and specifically identified

³ See, e.g., <https://www.scribd.com/document/455690219/MSD6886-Europe-Service-Manual-V1-0-2018-12-07-0-pdf>.

“HDCP 2.x” technology as infringing of the ’564 Patent. Upon information and belief, TCL is Defendants’ customer that incorporates Defendants’ HDCP 2+-capable products into TCL’s products such as televisions. Upon information and belief, Defendants were notified of the Asserted Patent, their infringement thereof, and their customer’s infringement thereof as a result of the filing of such complaint, for example, including by way of Defendants’ own monitoring efforts as adopters and providers of the HDCP 2+ technology, or by way of notice from a third party such as Defendants’ customer TCL.

22. Upon information and belief, Defendants were again notified of the Asserted Patent, their infringement thereof, and their customers’ infringement thereof on or shortly after February 20, 2020, when Philips sent a letter to LG Electronics, Inc. and its affiliates (“LG”), notifying LG that its products incorporating HDCP 2+ technology infringed of the ’564 Patent. Upon information and belief, LG is Defendants’ customer that incorporates Defendants’ HDCP 2+-capable products into LG’s products such as televisions and computer monitors. Upon information and belief, Defendants received notice of the Asserted Patent and their infringement thereof from LG as a result of such letter.

23. Upon information and belief, Defendants were again notified of the Asserted Patent, their infringement thereof, and their customers’ infringement thereof on or shortly after July 12, 2020, when Philips filed a first amended complaint against Defendants’ customer TCL in the above-identified patent infringement lawsuit in the United States District Court for the Central District of California, Western Division (C.A. No. 1:20-cv-1406), again specifically identifying “HDCP 2.x” technology as infringing the ’564 Patent. Upon information and belief, Defendants were again notified of the Asserted Patent, their infringement thereof, and their customer’s infringement thereof as a result of the filing of such amended complaint, for example, including by way of Defendants’ own monitoring efforts as

adopters and providers of the HDCP 2+ technology, or by way of notice from a third party such as their customer TCL.

24. Defendants are adopters and providers of the HDCP 2+ technology and are large technology corporations that make, use, sell, and/or offer for sale in the United States, import into the United States, and/or sell for importation into the United States, products that provide HDCP 2+ technology. To the extent Defendants failed to investigate their infringement upon learning of the '564 Patent, and/or upon learning of the above-identified patent infringement lawsuit in the United States District Court for the Central District of California, Western Division (C.A. No. 1:20-cv-1406), upon information and belief Defendants were willfully blind to their infringement of the '564 Patent.

25. Upon information and belief, Defendants upon learning of the Asserted Patent and their infringement thereof did not possess a good-faith belief of non-infringement. For example, upon information and belief, before the September 17, 2020 date of the original Complaint in this case, Defendants became aware that Philips had successfully licensed their patents, including the Asserted Patent, to a number of large, multinational electronics companies through high-profile patent litigation. As a result, Defendants lacked a good-faith belief at that time that they did not need to license the Asserted Patent.

26. Upon information and belief, Intel Corporation also published Errata to the specifications for the infringing HDCP 2.3 technology on July 1, 2021 ("Errata") in an effort to design around the Asserted Patent, which further demonstrates that Defendants lacked a good-faith belief of noninfringement with regard to the Asserted Patent before that date. In any event, on September 22, 2021, Philips sent letters to Defendants' customers of HDCP 2+ technology, including TCL, Hisense, HP, and Dell, notifying each such customer of its continuing infringement notwithstanding the Errata. Upon information and belief, each such customer, in

turn, notified Defendants of their continuing infringement and thus Defendant continued to lack a good-faith belief of noninfringement notwithstanding the Errata.

27. Upon information and belief, Defendants lack a good faith belief of noninfringement of the Asserted Patent when the claims of the Asserted Patent are properly construed.

28. After receiving actual notice of the Asserted Patent, Defendants continued to actively induce, and materially contribute to, their customers' infringement of the Asserted Patent by making, using, selling, offering for sale, marketing, advertising, and/or importing digital video-capable integrated circuits and associated firmware that are incorporated into Defendants' digital video-capable devices that infringe the Asserted Patent, and instructing customers to infringe the Asserted Patent.

29. For example, Defendants specifically intended and advertised that their digital video-capable integrated circuits and associated firmware for use within digital video-capable devices such as smart televisions.⁴ Such digital video-capable integrated circuits and associated firmware are advertised as supporting "HDMI 2.0/1.4 with HDCP 2.2" interfaces. Thus, Defendants induce their customers to infringe the Asserted Patent by advertising and/or instructing their customers regarding infringing uses of the Accused Products. On information and belief, Defendants did so with the specific intent to bring about infringement in the United States knowing that, among others, at least the Exemplary Customers would incorporate Defendants' digital-video capable integrated circuits and associated firmware in digital-video capable devices made, used, sold, offered for sale or imported into the United States.

⁴ <https://www.mediatek.com/products/digitalTv/mt5596>.

30. As another example, Defendants contribute to the same infringement by selling digital video-capable integrated circuits and associated firmware to customers who incorporate said digital video-capable integrated circuits and associated firmware into their infringing digital video-capable devices. On information and belief, Defendants had knowledge that digital video-capable integrated circuits and associated firmware were especially made or especially adapted for use in an infringement of the Asserted Patent by practicing HDCP 2+, and were not a staple article or commodity of commerce suitable for substantial non-infringing use. Upon information and belief, Defendants were aware, and continue to be aware, that there is no way to comply with HDCP 2+ and not infringe the Asserted Patent.

31. Thus, Defendants have indirectly infringed, and continue to indirectly infringe, the Asserted Patent under 35 U.S.C. § 271(b) by actively inducing their customers to infringe the Asserted Patent by making, using, selling, offering for sale, marketing, advertising, and/or importing the Accused Products to their customers and by instructing customers to infringe the Asserted Patent, as described in detail in Count I *infra*. Additionally, Defendants have indirectly infringed, and continue to indirectly infringe the Asserted Patent under 35 U.S.C. § 271(c) by materially contributing to their own customers' infringement of the Asserted Patent by making, using, selling, offering for sale, advertising, marketing, and/or importing the Accused Products to their customers and instructing customers to infringe the Asserted Patent, as described in detail in Count I *infra*.

32. Defendants' acts of infringement have caused damage to MCP. MCP is entitled to recover from Defendants the damages incurred by MCP as a result of Defendants' wrongful acts.

COUNT I

Defendants' Infringement of the '564 Patent

33. MCP incorporates the allegations of all of the foregoing paragraphs as if fully restated herein.

34. Defendants have directly infringed, and continue to directly infringe, the '564 Patent by making, using, selling, offering for sale, or importing throughout the United States products and/or methods covered by one or more claims of the '564 Patent including, but not limited to, digital video-capable integrated circuits and associated firmware for inclusion in digital video-capable devices. The products that infringe one or more claims of the '564 Patent include, but are not limited to, at least the Accused Products. Further discovery may reveal additional infringing products and/or models.

35. For example and without limitation, the Accused Products infringe claim 1 of the '564 Patent.

36. Attached hereto as Exhibit B, and incorporated into this Second Amended Complaint, is a claim chart showing where in the Mstar-branded MSD6886NQHT integrated circuit and associated firmware incorporated into the Hisense, H65 Series Android TV, Model 43H6570G each limitation of claim 1 is met. This claim chart is exemplary and, on information and belief, many other products provided by Defendants and/or Defendants' customers infringe the '564 Patent.

37. Defendants have, and continue to, indirectly infringe the '564 Patent by actively inducing and contributing to the infringement of the '564 Patent by others, such as customers, resellers, and retailers. These others include, but are not limited to the Exemplary Customers, who, for example, sell, offer for sale, and/or import throughout the United States, including within this District, digital video-capable devices incorporating the Accused Products.

38. Defendants specifically intended others, such as customers, resellers, and retailers, to infringe the '564 Patent and knew that these others perform acts that constituted direct infringement. For example, Exhibit B shows that an exemplary product, the Mstar-branded MSD6886NQHT integrated circuit and associated firmware incorporated into the Hisense H65G Series 4K UHD Android Smart TV, Model No. 43H6570G, which is sold by Best Buy Co., Inc., infringes the '564 Patent. Defendants designed the Accused Products such that they would each infringe the '564 Patent as described in Exhibit B if made, used, sold, offered for sale, or imported throughout the United States. Defendants provided, directly or indirectly, Accused Products to others, such as, but not limited to, customers, knowing and intending that those others would use, sell, offer for sale, and/or import the Accused Products throughout the United States, thereby directly infringing one or more claims of the '564 Patent.

39. In addition, upon information and belief, Defendants provide instructions, user guides, and/or other documentation to the infringing others regarding the use and operation of the Accused Products. When others follow such instructions, user guides, and/or other documentation, they directly infringe one or more claims of the '564 Patent. By providing such instructions, user guides, and/or other documentation, Defendants know and intend that others will follow those instructions, user guides, and other documentation, and thereby directly infringe one or more claims of the '564 Patent. Thus, Defendants know that their actions actively induce infringement.

40. The Accused Products have no substantial non-infringing uses and are a material part of the invention. As described in Exhibit B, any manufacture, use, sale offer for sale or importation throughout the United States of an Accused Product, or incorporation of any of the Accused Products in digital video-capable devices infringes the '564 Patent. Thus, the Accused Products have no substantial

non-infringing uses.

41. MCP is entitled to recover damages under 35 U.S.C. § 284 to adequately compensate for Defendants' infringement of the '564 Patent.

DAMAGES

42. Defendants have refused to compensate MCP for their infringement of the Asserted Patent. MCP is entitled to monetary damages adequate to compensate MCP for Defendants' infringement in an amount no less than a reasonable royalty for the use made of the patented inventions by Defendants. The precise amount of damages will be determined through discovery in this action and proven at trial.

MARKING

43. MCP and its licensees of the Asserted Patent have complied with 35 U.S.C. § 287, and relative to its licensees, MCP has taken reasonable steps to ensure compliance with marking.

PRAYER FOR RELIEF

WHEREFORE, MCP respectfully asks the Court for an order granting the following relief:

- a) A judgment that the Asserted Patent is valid and enforceable;
- b) A judgment that Defendants have infringed, directly and indirectly, either literally or under the Doctrine of Equivalents, one or more claims of the '564 Patent;
- c) A judgment awarding MCP all appropriate damages under 35 U.S.C. § 284 for Defendants' past infringement, and any continuing or future infringement of the Asserted Patent, including pre and post judgment interest, costs, and disbursements pursuant to 35 U.S.C. § 284;
- d) An accounting for infringing sales not presented at trial and an award by the Court of additional damages for any such infringing sales;
- e) A finding that this case is exceptional within the meaning of 35 U.S.C.

§ 285 and that MCP be awarded its reasonable attorneys' fees against Defendants incurred in prosecuting this action;

- f) An award of reasonable attorneys' fees, costs, and expenses incurred by MCP in connection with prosecuting this action; and
- g) Any and all other relief as the Court finds just, equitable, and proper under the circumstances.

DEMAND FOR JURY TRIAL

Pursuant to Fed. R. Civ. P. 38, MCP hereby respectfully demands trial by jury on all claims and issues so triable.

Dated: September 20, 2024

Respectfully submitted,

FARNAN LLP

/s/ Brian E. Farnan

Brian E. Farnan (Bar No. 4089)
Michael J. Farnan (Bar No. 5165)
919 N. Market St., 12th Floor
Wilmington, DE 19801
Phone: (302) 777-0300
Fax: (302) 777-0301
bfarnan@farnanlaw.com
mfarnan@farnanlaw.com

Michael T. Renaud (admitted *pro hac vice*)
Adam S. Rizk (admitted *pro hac vice*)
Catherine Xu (admitted *pro hac vice*)
Timothy J. Rousseau (admitted *pro hac vice*)
Courtney P. Herndon (admitted *pro hac vice*)
Williams S. Dixon (admitted *pro hac vice*)
MINTZ LEVIN COHN FERRIS
GLOVSKY & POPEO PC
One Financial Center
Boston, Massachusetts 02111
Phone: 617) 542-6000

Fax: (617) 542-2241
MTRenaud@mintz.com
ARizk@mintz.com
CXu@mintz.com
TJRousseau@mintz.com
CHerndon@mintz.com
WSDixon@mintz.com

Peter F. Snell (admitted *pro hac vice*)
Brad M. Scheller (admitted *pro hac vice*)
MINTZ LEVIN COHN FERRIS
GLOVSKY & POPEO PC
919 Third Avenue
New York, NY 10022
Phone: (212) 935-3000
Fax: (212) 983-3115
PFSnell@mintz.com
BMScheller@mintz.com

Attorneys for Plaintiff
Media Content Protection LLC

EXHIBIT A



US10298564B2

(12) **United States Patent**
Kamperman

(10) **Patent No.:** **US 10,298,564 B2**
(45) **Date of Patent:** ***May 21, 2019**

(54) **SECURE AUTHENTICATED DISTANCE MEASUREMENT**

(71) Applicant: **KONINKLIJKE PHILIPS N.V.**,
Eindhoven (NL)

(72) Inventor: **Franciscus L. A. J. Kamperman**,
Geldrop (NL)

(73) Assignee: **KONINKLIJKE PHILIPS N.V.**,
Eindhoven (NL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/117,019**

(22) Filed: **Aug. 30, 2018**

(65) **Prior Publication Data**

US 2019/0014106 A1 Jan. 10, 2019

Related U.S. Application Data

(63) Continuation of application No. 15/352,646, filed on Nov. 16, 2016, now Pat. No. 10,091,186, which is a (Continued)

(30) **Foreign Application Priority Data**

Jul. 26, 2002 (EP) 02078076

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 9/14 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC **H04L 63/0823** (2013.01); **G06F 21/10** (2013.01); **H04L 9/14** (2013.01);
(Continued)

(58) **Field of Classification Search**

CPC H04L 63/0823; H04L 9/14; H04L 63/107;
H04L 63/062; H04L 43/16;
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,438,824 A 3/1984 Mueller-Schloer
4,688,036 A 8/1987 Hirano et al.
(Continued)

FOREIGN PATENT DOCUMENTS

EP 1100035 A1 5/2001
JP H04306760 A 10/1992
(Continued)

OTHER PUBLICATIONS

Ikeno et al "Modern Cryptography Theory" Japan, Institute of Electronics, Information and Communication Engineers, Nov. 15, 1997, p. 175-177.

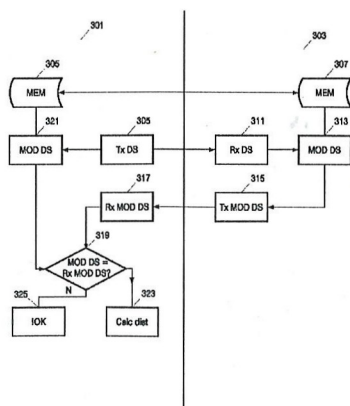
(Continued)

Primary Examiner — Darren B Schwartz

(57) **ABSTRACT**

The invention relates to a method for a first communication device to perform authenticated distance measurement between the first communication device and a second communication device, wherein the first and the second communication device share a common secret and the common secret is used for performing the distance measurement between the first and the second communication device. The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device. Moreover, the invention relates to a communication device for performing authenticated distance measurement to a second communication device. The invention also relates to an apparatus for playing back multimedia content comprising a communication device.

53 Claims, 3 Drawing Sheets



US 10,298,564 B2

Page 2

Related U.S. Application Data

continuation of application No. 15/229,207, filed on Aug. 5, 2016, now Pat. No. 9,590,977, which is a continuation of application No. 14/538,493, filed on Nov. 11, 2014, now Pat. No. 9,436,809, which is a continuation of application No. 10/521,858, filed as application No. PCT/IB03/02932 on Jun. 27, 2003, now Pat. No. 8,886,939.

- (51) **Int. Cl.**
H04L 12/26 (2006.01)
H04L 9/32 (2006.01)
G06F 21/10 (2013.01)
H04L 9/30 (2006.01)
H04W 24/00 (2009.01)
H04W 12/06 (2009.01)
- (52) **U.S. Cl.**
 CPC *H04L 9/30* (2013.01); *H04L 9/3263* (2013.01); *H04L 43/0852* (2013.01); *H04L 43/16* (2013.01); *H04L 63/062* (2013.01); *H04L 63/107* (2013.01); *G06F 2221/07* (2013.01); *G06F 2221/2111* (2013.01); *H04L 63/0428* (2013.01); *H04L 2463/101* (2013.01); *H04W 12/06* (2013.01); *H04W 24/00* (2013.01)
- (58) **Field of Classification Search**
 CPC *H04L 43/0852*; *H04L 9/3263*; *H04L 9/30*; *H04L 63/0428*; *H04L 2463/101*; *G06F 21/10*; *G06F 2221/07*; *G06F 2221/2111*; *H04W 24/00*; *H04W 12/06*
 See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,926,480	A	5/1990	Chaum	
5,126,746	A	6/1992	Gritton	
5,596,641	A	1/1997	Ohashi et al.	
5,602,917	A	2/1997	Mueller	
5,659,617	A	8/1997	Fischer	
5,723,911	A	3/1998	Glehr	
5,778,071	A	7/1998	Caputo et al.	
5,937,065	A	8/1999	Simon et al.	
5,949,877	A	9/1999	Traw et al.	
5,983,347	A	11/1999	Brinkmeyer et al.	
6,085,320	A	7/2000	Kaliski	
6,088,450	A	7/2000	Davis et al.	
6,151,676	A	11/2000	Cuccia et al.	
6,208,239	B1	3/2001	Muller et al.	
6,346,878	B1	2/2002	Pohlman et al.	
6,351,235	B1	2/2002	Stilp	
6,442,690	B1	8/2002	Howard, Jr.	
6,484,948	B1	11/2002	Sonoda	
6,493,825	B1	12/2002	Blumenau et al.	
6,526,598	B1	3/2003	Horn	
6,550,011	B1 *	4/2003	Sims, III	G06F 21/10 365/52
7,200,233	B1	4/2007	Keller et al.	
7,242,766	B1	7/2007	Lyle	
7,516,325	B2	4/2009	Willey	
7,787,865	B2	8/2010	Willey	
7,898,977	B2	3/2011	Roose	
8,068,610	B2	11/2011	Moroney	
8,107,627	B2	1/2012	Epstein	
8,352,582	B2	1/2013	Epstein	
8,997,243	B2	3/2015	Epstein	
2001/0008558	A1	7/2001	Hirafuji	
2001/0043702	A1	11/2001	Elteto et al.	
2001/0044786	A1	11/2001	Ishibashi	
2001/0050990	A1 *	12/2001	Sudia	G06Q 20/02 380/286

2002/0007452	A1 *	1/2002	Traw	G06F 21/10 713/152
2002/0026424	A1	2/2002	Akashi	
2002/0026576	A1	2/2002	Das-Purkayastha et al.	
2002/0035690	A1	3/2002	Nakano	
2002/0061748	A1	5/2002	Nakakita et al.	
2002/0078227	A1	6/2002	Kronenberg	
2002/0166047	A1	11/2002	Kawamoto	
2003/0021418	A1	1/2003	Arakawa et al.	
2003/0030542	A1	2/2003	Von Hoffmann	
2003/0051151	A1	3/2003	Asano	
2003/0065918	A1	4/2003	Willey	
2003/0070092	A1	4/2003	Hawkes et al.	
2003/0112978	A1	6/2003	Rodman et al.	
2003/0174838	A1 *	9/2003	Bremer	H04L 63/0428 380/270
2003/0184431	A1	10/2003	Lundkvist	
2003/0220765	A1	11/2003	Overy et al.	
2004/0015693	A1	1/2004	Kitazumi	
2004/0025018	A1 *	2/2004	Haas	H04L 45/26 713/168
2004/0080426	A1	4/2004	Fraenkel	
2005/0114647	A1	5/2005	Epstein	
2005/0265503	A1	12/2005	Rofheart et al.	
2006/0294362	A1	12/2006	Epstein	

FOREIGN PATENT DOCUMENTS

JP	H0619948	A	1/1994
JP	H08234658	A	9/1996
JP	9170364	A	6/1997
JP	H09170364	A	6/1997
JP	11101035	A	4/1999
JP	11208419	A	8/1999
JP	2000357156	A	12/2000
JP	2001249899	A	9/2001
JP	2001257672	A	9/2001
JP	2002124960	A	4/2002
JP	2002189966	A	7/2002
WO	9739553	A1	10/1997
WO	9949378	A	9/1999
WO	0152234	A1	7/2001
WO	0193434	A1	12/2001
WO	0233887	A2	4/2002
WO	0235036	A1	5/2002
WO	02054353	A1	7/2002

OTHER PUBLICATIONS

Modern Cryptography Theory (1986) Chapter 9, ISBN: 4-88552-064-9 (Japanese).

Hayashi et al Encryption and Authentication Program Module , Technical Paper (Japanese) NTT R&D vol. 44, No. 10 Oct. 1, 1995.

Stefan Brands and Devid Chaum "Distance Bounding Protocols" Eurocrypt '93, (1993) p. 344-359.

Tim Kindber & Kan Zhang "Context Authention Using Constrained Channels" pp. 1-8 , Apr. 16, 2001.

Hitachi Ltd., 5C Digital Transmission Content Protection White Paper Rev. 1.0 Jul. 14, 1998, p. 1013.

Boyd et al "Protocols for Authention and Key Establishment" Spring-Verlag, Sep. 17, 2003, p. 116-120, 195, 305.

High Bandwidth Digital Content Protection System Feb. 17, 2000.

High Bandwidth Digital Content Protection System Revision 1.0 Erratum Mar. 1, 2001.

Digital Transmission Content Protection Specification vol. 1 Hitachi Ltd. Revision 1.0 Apr. 12, 1999.

Digital Transmission Content Protection Specification vol. 1 (Informational Version) Hitachi Ltd. Revision 1.2A Feb. 25, 2002.

SmartRight™ Certification for FCC Approval for Use with the Broadcast Flag, Mar. 1, 2004.

SmartRight™ Copy Protection for System for Digital Home Networks, Deployment Process, CPTWG, Nov. 28, 2001.

SmartRight™ Copy Protection System for Digital Home Networks, CPTWG, May 24, 2001.

SmartRight™ Digital Broadcast Content Protection, Presentation to FCC, Apr. 2, 2004 (cited in litigation).

US 10,298,564 B2

Page 3

(56)

References Cited

OTHER PUBLICATIONS

SmartRight™ Technical White Paper, Version 1.7, Jan. 2003 (“White Paper”) (cited in litigation).

Internet Security Association and Key Management Protocol (ISAKMP), Request for Comments 2408 (“RFC 2408”)—cited in litigation, Nov. 1998.

International Standard ISO/IEC 11770-3 (1st ed.) (“ISO 11770-3”), Nov. 1, 1999.

Scott Crosby, et al., “A Cryptanalysis of the High-bandwidth Digital Content Protection System” Computer and Communications Security, (2001).

SmartRight™ Specifications Sep. 26, 2001.

SmartRight™ Copy Protection System for Digital Home Networks, CPTWG, Jul. 11, 2001.

Bruce Schneier, Applied Cryptography (2d ed. 1996) (“Schneier”).

Steven M. Bellovin and Michael Merritt, “Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks”, 2002.

RFC 2463 Internet Control Message Protocol Dec. 1998.

RFC2246 the TLS Protocol, Jan. 1999.

Internet Security Association and Key Management Protocol (ISAKMP), Request for Comments 2408 (“RFC 2408”), Nov. 1998.

Declaration of William Rosenblatt, Microsoft Exhibit 1009, Dec. 8, 2017.

Supplemental Declaration of William Rosenblatt, Microsoft Exhibit 1015, Apr. 20, 2018.

Petition for Inter Parties Review of USP 8543819, Dec. 8, 2017.

Patent Owner’s Preliminary Response, Mar. 13, 2018.

Petitioners’ Reply to Patent Owner’s Preliminary Response, Apr. 20, 2018.

Patent Owner’s Sur-Reply to Petitioners’ Reply, May 4, 2018.

Petition for Inter Parties Review of USP 9436809, Dec. 8, 2017.

Markman Order Filed Jul. 11, 2017.

Internet Security Association and Key Management Protocol (ISAKMP), Request for Comments 2407 (“RFC 2407”), Nov. 1998.

Internet Security Association and Key Management Protocol (ISAKMP), Request for Comments 2409 (“RFC 2409”), Nov. 1998.

* cited by examiner

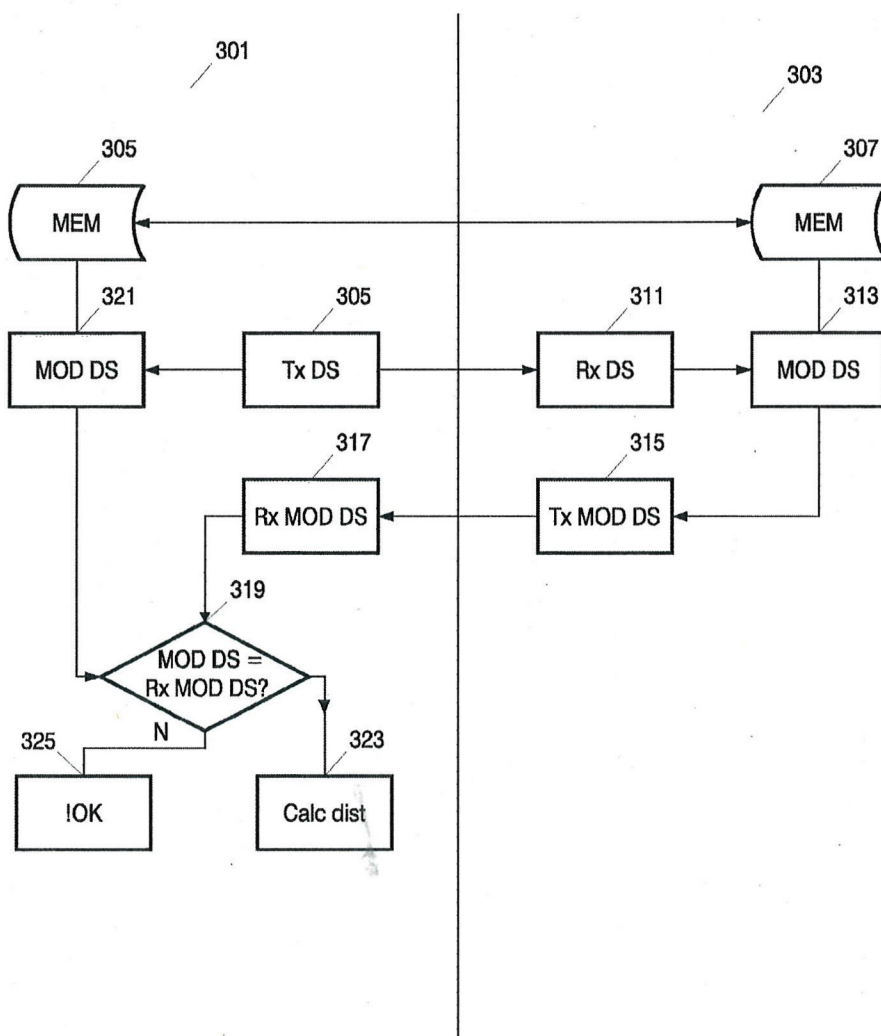


FIG. 3

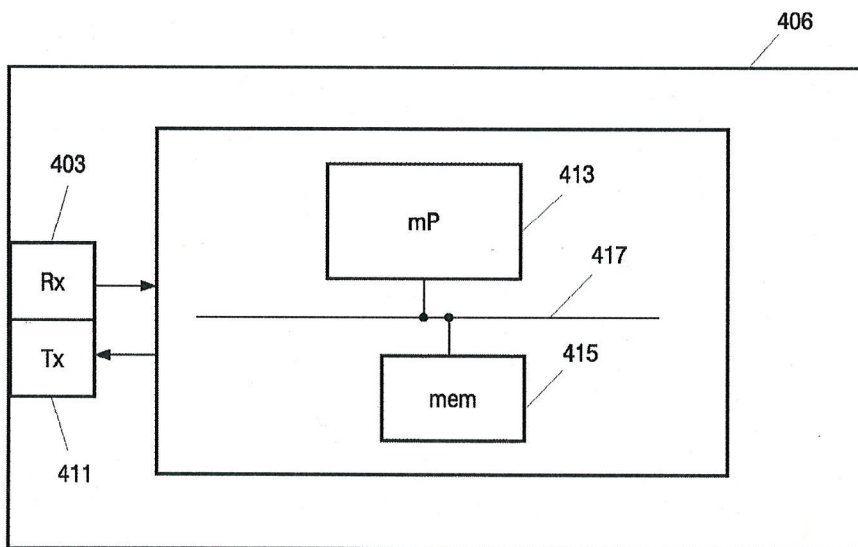


FIG. 4

US 10,298,564 B2

1

**SECURE AUTHENTICATED DISTANCE
MEASUREMENT**

This application is a continuation of the patent application entitled "Secure Authenticated Distance Measurement", filed on Nov. 16, 2016 and afforded Ser. No. 15/352,646 which is a continuation of the application filed Aug. 5, 2016 and afforded Ser. No. 15/229,207 which is a continuation of the application filed Nov. 11, 2014 and afforded Ser. No. 14/538,493 which claims priority pursuant to 35 USC 120, priority to and the benefit of the earlier filing date of, that patent application entitled "Secure Authenticated Distance Measurement", filed on Jan. 21, 2005 and afforded Ser. No. 10/521,858 (now U.S. Pat. No. 8,886,939), which claimed priority to and the benefit of the earlier filing date, as a National Stage Filing of that international patent application filed on Jun. 27, 2003 and afforded serial number PCT/IB2003/02932 (WO2004014037), which claimed priority to and the benefit of the earlier filing date of that patent application filed on Jul. 26, 2002 and afforded serial number EP 02078076.3, the contents of all of which are incorporated by reference, herein.

This application is further related to that patent application entitled "Secure authenticated Distance Measurement", filed on Jul. 24, 2009 and afforded Ser. No. 12/508,917 (now U.S. Pat. No. 8,543,819), issued Sep. 24, 2013), which claimed priority to and the benefit of the earlier filing date of that patent application entitled "Secure Authenticated Distance Measurement", filed on Jan. 21, 2005 and afforded Ser. No. 10/521,858 (now U.S. Pat. No. 8,886,939), the contents of which are incorporated by reference herein.

The invention relates to a method for a first communication device to performing authenticated distance measurement between a first communication device and a second communication device. The invention also relates to a method of determining whether data stored on a first communication device is to be accessed by a second communication device. Moreover, the invention relates to a communication device for performing authenticated distance measurement to a second communication device. The invention also relates to an apparatus for playing back multimedia content comprising a communication device.

Digital media have become popular carriers for various types of data information. Computer software and audio information, for instance, are widely available on optical compact disks (CDs) and recently also DVD has gained in distribution share. The CD and the DVD utilize a common standard for the digital recording of data, software, images, and audio. Additional media, such as recordable discs, solid-state memory, and the like, are making considerable gains in the software and data distribution market.

The substantially superior quality of the digital format as compared to the analog format renders the former substantially more prone to unauthorized copying and pirating, further a digital format is both easier and faster to copy. Copying of a digital data stream, whether compressed, uncompressed, encrypted or non-encrypted, typically does not lead to any appreciable loss of quality in the data. Digital copying thus is essentially unlimited in terms of multi-generation copying. Analog data with its signal to noise ratio loss with every sequential copy, on the other hand, is naturally limited in terms of multi-generation and mass copying.

The advent of the recent popularity in the digital format has also brought about a slew of copy protection and DRM systems and methods. These systems and methods use

2

technologies such as encryption, watermarking and right descriptions (e.g. rules for accessing and copying data).

One way of protecting content in the form of digital data is to ensure that content will only be transferred between devices if

the receiving device has been authenticated as being a compliant device, and the user of the content has the right to transfer (move, copy) that content to another device.

If transfer of content is allowed, this will typically be performed in an encrypted way to make sure that the content cannot be captured illegally in a useful format.

Technology to perform device authentication and encrypted content transfer is available and is called a secure authenticated channel (SAC). Although it might be allowed to make copies of content over a SAC, the content industry is very bullish on content distribution over the Internet. This results in disagreement of the content industry on transferring content over interfaces that match well with the Internet, e.g. Ethernet.

Further, it should be possible for a user visiting his neighbor to watch a movie, which he owns, on the neighbor's big television screen. Typically, the content owner will disallow this, but it might become acceptable if it can be proved that a license holder of that movie (or a device that the license holder owns) is near that television screen.

It is therefore of interest to be able to include an authenticated distance measurement when deciding whether content should be accessed or copied by other devices.

In the article by Stefan Brands and David Chaum, "Distance-Bounding protocols", Eurocrypt '93 (1993), Pages 344-359, integration of distance-bounding protocols with public-key identification schemes is described. Here distance measurement is described based on time measurement using challenge and response bits and with the use of a commitment protocol. This does not allow authenticated device compliancy testing and is not efficient when two devices must also authenticate each other.

It is an object of the invention to obtain a solution to the problem of performing a secure transfer of content within a limited distance.

This is obtained by a method for a first communication device to performing authenticated distance measurement between the first communication device and a second communication device, wherein the first and the second communication device share a common secret and the common secret is used for performing the distance measurement between the first and the second communication device.

Because the common secret is being used for performing the distance measurement, it can be ensured that when measuring the distance from the first communication device to the second communication device, it is the distance between the right devices that is being measured.

The method combines a distance measurement protocol with an authentication protocol. This enables authenticated device compliancy testing and is efficient, because a secure channel is anyhow needed to enable secure communication between devices and a device can first be tested on compliancy before a distance measurement is executed.

In a specific embodiment, the authenticated distance measurement is performed according to the following steps, transmitting a first signal from the first communication device to the second communication device at a first time t1, the second communication device being adapted for receiving the first signal, generating a second signal by modifying the received first signal

US 10,298,564 B2

3

according to the common secret and transmitting the second signal to the first device,
 receiving the second signal at a second time t_2 ,
 checking if the second signal has been modified according to the common secret,
 determining the distance between the first and the second communication device according to a time difference between t_1 and t_2 .

When measuring a distance by measuring the time difference between transmitting and receiving a signal and using a secret, shared between the first and the second communication device, for determining whether the returned signal really originated from the second communication device, the distance is measured in a secure authenticated way ensuring that the distance will not be measured to a third communication device (not knowing the secret). Using the shared secret for modifying the signal is a simple way to perform a secure authenticated distance measurement.

In a specific embodiment the first signal is a spread spectrum signal. Thereby a high resolution is obtained and it is possible to cope with bad transmission conditions (e.g. wireless environments with a lot of reflections).

In another embodiment the step of checking if the second signal has been modified according to the common secret is performed by the steps of,

generating a third signal by modifying the first signal according to the common secret,
 comparing the third signal with the received second signal.

This method is an easy and simple way of performing the check, but it requires that both the first communication device and the second communication device know how the first signal is being modified using the common secret.

In a specific embodiment the first signal and the common secret are bit words and the second signal comprises information being generated by performing an XOR between the bit words. Thereby, it is a very simple operation that has to be performed, resulting in demand for few resources by both the first and the second communication device when performing the operation.

In an embodiment the common secret has been shared before performing the distance measurement, the sharing being performed by the steps of,

performing an authentication check from the first communication device on the second communication device by checking whether the second communication device is compliant with a set of predefined compliance rules,

if the second communication device is compliant, sharing the common secret by transmitting the secret to the second communication device.

This is a secure way of performing the sharing of the secret, ensuring that only devices being compliant with compliance rules can receive the secret. Further, the shared secret can afterwards be used for generating a SAC channel between the two devices. The secret could be shared using e.g. key transport mechanisms as described in ISO 11770-3. Alternatively, a key agreement protocol could be used, which e.g. is also described in ISO 11770-3.

In another embodiment the authentication check further comprises checking if the identification of the second device is compliant with an expected identification. Thereby, it is ensured that the second device really is the device that it should be. The identity could be obtained by checking a certificate stored in the second device.

4

The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of performing a distance measurement between the first and the second communication device and checking whether the measured distance is within a predefined distance interval, wherein the distance measurement is an authenticated distance measurement according to the above. By using the authenticated distance measurement in connection with sharing data between devices, unauthorized distribution of content can be reduced.

In a specific embodiment the data stored on the first device is sent to the second device if it is determined that the data stored on the first device are to be accessed by the second device.

The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of performing a distance measurement between a third communication device and the second communication device and checking whether the measured distance is within a predefined distance interval, wherein the distance measurement is an authenticated distance measurement according to the above. In this embodiment, the distance is not measured between the first communication device, on which the data are stored, and the second communication device. Instead, the distance is measured between a third communication device and the second communication device, where the third communication device could be personal to the owner of the content.

The invention also relates to a communication device for performing authenticated distance measurement to a second communication device, where the communication device shares a common secret with the second communication device and where the communication device comprises means for measuring the distance to the second device using the common secret.

In an embodiment the device comprises:

means for transmitting a first signal to a second communication device at a first time t_1 , the second communication device being adapted for receiving the first signal, generating a second signal by modifying the received first signal according to the common secret and transmitting the second signal,

means for receiving the second signal at a second time t_2 ,
 means for checking if the second signal has been modified according to the common secret, and

means for determining the distance between the first and the second communication device according to a time difference between t_1 and t_2 .

The invention also relates to an apparatus for playing back multimedia content comprising a communication device according to the above.

In the following preferred embodiments of the invention will be described referring to the figures, wherein:

FIG. 1 illustrates authenticated distance measurement being used for content protection,

FIG. 2 is a flow diagram illustrating the method of performing authenticated distance measurement,

FIG. 3 illustrates in further detail the step of performing the authenticated distance measurement shown in FIG. 2,

FIG. 4 illustrates a communication device for performing authenticated distance measurement.

FIG. 1 illustrates an embodiment where authenticated distance measurement is being used for content protection. In the center of the circle 101 a computer 103 is placed. The computer comprises content, such as multimedia content

US 10,298,564 B2

5

being video or audio, stored on e.g. a hard disk, DVD or a CD. The owner of the computer owns the content and therefore the computer is authorized to access and present the multimedia content for the user. When the user wants to make a legal copy of the content to another device via e.g. a SAC, the distance between the other device and the computer **103** is measured and only devices within a predefined distance illustrated by the devices **105, 107, 109, 111, 113** inside the circle **101** are allowed to receive the content. Whereas the devices **115, 117, 119** having a distance to the computer **101** being larger than the predefined distance are not allowed to receive the content.

In the example a device is a computer, but it could e.g. also be a DVD drive, a CD drive or a Video, as long as the device comprises a communication device for performing the distance measurement.

In a specific example the distance might not have to be measured between the computer, on which the data are stored, and the other device, it could also be a third device e.g. a device being personal to the owner of the content which is within the predefined distance.

In FIG. 2 a flow diagram illustrates the general idea of performing authenticated distance measurement between two devices, **201** and **203** each comprising communication devices for performing the authenticated distance measurement. In the example the first device **201** comprises content which the second device **203** has requested. The authenticated distance measurement then is as follows. In step **205** the first device **201** authenticates the second device **203**; this could comprise the steps of checking whether the second device **203** is a compliant device and might also comprise the step of checking whether the second device **203** really is the device identified to the first device **201**. Then in step **207**, the first device **201** exchanges a secret with the second device **203**, which e.g. could be performed by transmitting a random generated bit word to second device **203**. The secret should be shared securely, e.g. according to some key management protocol as described in e.g. ISO 11770.

Then in step **209**, a signal for distance measurement is transmitted to the second device **203**; the second device modifies the received signal according to the secret and retransmits the modified signal back to the first device. The first device **201** measures the round trip time between the signal leaving and the signal returning and checks if the returned signal was modified according to the exchanged secret. The modification of the returned signal according to some secret will most likely be dependent on the transmission system and the signal used for distance measurement, i.e. it will be specific for each communication system (such as 1394, Ethernet, Bluetooth, IEEE 802.11, etc.).

The signal used for the distance measurement may be a normal data bit signal, but also special signals other than for data communication may be used. In an embodiment spread spectrum signals are used to be able to get high resolution and to be able to cope with bad transmission conditions (e.g. wireless environments with a lot of reflections).

In a specific example a direct sequence spread spectrum signal is used for distance measurement; this signal could be modified by XORing the chips (e.g. spreading code consisting of 127 chips) of the direct sequence code by the bits of the secret (e.g. secret consists also of 127 bits). Also, other mathematical operations as XOR could be used.

The authentication **205** and exchange of secret **207** could be performed using the protocols described in some known ISO standards ISO 9798 and ISO 11770. For example the first device **201** could authenticate the second device **203** according to the following communication scenario:

6

First device → Second device: $R_B || \text{Text 1}$

where R_B is a random number

Second device → First device: $\text{CertA} || \text{TokenAB}$

Where CertA is a certificate of A

$\text{TokenAB} = R_A || R_B || B || \text{Text3} || s_{S_A}(R_A || R_B || B || \text{Text2})$

R_A is a random number

Identifier B is an option

s_{S_A} is a signature set by A using private key S_A

If TokenAB is replaced with the token as specified in ISO 11770-3 we at the same time can do secret key exchange. We can use this by substituting Text2 by:

$\text{Text2} := e_{P_B}(A || K || \text{Text2}) || \text{Text3}$

Where e_{P_B} is encrypted with Public key B

A is identifier of A

K is a secret to be exchanged

In this case the second device **203** determines the key (i.e. has key control), this is also called a key transport protocol, but also a key agreement protocol could be used. This may be undesirable in which case it can be reversed, such that the first device determines the key. A secret key has now been exchanged according to step **207** in FIG. 2. Again, the secret key could be exchanged by e.g. a key transport protocol or a key agreement protocol.

After the distance has been measured in a secure authenticated way as described above content, data can be sent between the first and the second device in step **211** in FIG. 2.

FIG. 3 illustrates in further detail the step of performing the authenticated distance measurement. As described above the first device **301** and the second device **303** have exchanged a secret; the secret is stored in the memory **305** of the first device and the memory **307** of the second device. In order to perform the distance measurement, a signal is transmitted to the second device via a transmitter **309**. The second device receives the signal via a receiver **311** and **313** modifies the signal by using the locally stored secret. The signal is modified according to rules known by the first device **301** and transmitted back to the first device **301** via a transmitter **315**. The first device **301** receives the modified signal via a receiver **317** and in **319** the received modified signal is compared to a signal, which has been modified locally. The local modification is performed in **321** by using the signal transmitted to the second device in transmitter **309** and then modifying the signal using the locally stored secret similar to the modification rules used by the second device. If the received modified signal and the locally modified signal are identical, then the received signal is authenticated and can be used for determining the distance between the first and the second device. If the two signals are not identical, then the received signal cannot be authenticated and can therefore not be used for measuring the distance as illustrated by **325**. In **323** the distance is calculated between the first and the second device; this could e.g. be performed by measuring the time, when the signal is transmitted by the transmitter **309** from the first device to the second device and measuring when the receiver **317** receives the signal from the second device. The time difference between transmittal time and receive time can then be used for determining the physical distance between the first device and the second device.

In FIG. 4 a communication device for performing authenticated distance measurement is illustrated. The device **401** comprises a receiver **403** and a transmitter **411**. The device further comprises means for performing the steps described above, which could be by executing software using a micro-processor **413** connected to memory **415** via a communication bus **417**. The communication device could then be

US 10,298,564 B2

7

placed inside devices such as a DVD, a computer, a CD, a CD recorder, a television and other devices for accessing protected content.

The invention claimed is:

1. A second device for receiving delivery of a protected content from a first device, the second device comprising a processor circuit, the processor circuit arranged to execute instructions, the instructions arranged to:

provide a certificate to the first device prior to receiving a first signal, wherein the first signal is sent by the first device, wherein the certificate is associated with the second device;

receive the first signal when the certificate indicates that the second device is compliant with at least one compliance rule;

create a second signal, wherein the second signal is derived from a secret known by the second device;

provide the second signal to the first device after receiving the first signal, wherein the second signal is received by the first device; and

receive the protected content from the first device when the first device determines that the second signal is derived from the secret and a time between the sending of the first signal and the receiving of the second signal is less than a predetermined time.

2. The second device of claim 1, wherein the secret is securely provided to the second device by the first device.

3. The second device of claim 2, wherein determining that the second signal is derived from the secret comprises:

modifying the first signal, wherein the modifying requires the secret; and

determining that the modified first signal is identical to the second signal.

4. The second device of claim 2, wherein determining that the second signal is derived from the secret comprises: modifying the first signal; and

determining that the modified first signal is identical to the second signal.

5. The second device of claim 2, wherein the predetermined time is based on a communication system associated with the first device.

6. The second device of claim 2, further comprising instructions arranged to receive the secret from the first device.

7. The second device of claim 2, wherein the second signal comprises the first signal modified by the secret.

8. The second device of claim 2, wherein the secret comprises a random number.

9. The second device of claim 2, wherein the secret is encrypted with a public key.

10. The second device of claim 2, wherein the first signal comprises a random number.

11. The second device of claim 2, wherein the second signal comprises an XOR operation of the first signal with the secret.

12. The second device of claim 2, wherein determining that the second signal is derived from the secret comprises: modifying the second signal, wherein the modifying requires the secret; and

determining that the modified second signal is identical to the first signal.

13. The second device of claim 2, wherein determining that the second signal is derived from the secret comprises: modifying the second signal; and

determining that the modified second signal is identical to the first signal.

8

14. The second device of claim 2, wherein the secret is used for generating a secure channel between the first device and the second device.

15. The second device of claim 1, wherein determining that the second signal is derived from the secret comprises: modifying the first signal, wherein the modifying requires the secret; and

determining that the modified first signal is identical to the second signal.

16. The second device of claim 1, wherein determining that the second signal is derived from the secret comprises: modifying the first signal; and

determining that the modified first signal is identical to the second signal.

17. The second device of claim 1, wherein the predetermined time is based on a communication system associated with the first device.

18. The second device of claim 1, further comprising instructions arranged to receive the secret from the first device.

19. The second device of claim 1, wherein the second signal comprises the first signal modified by the secret.

20. The second device of claim 1, wherein the secret comprises a random number.

21. The second device of claim 1, wherein the secret is encrypted with a public key.

22. The second device of claim 1, wherein the first signal comprises a random number.

23. The second device of claim 1, wherein the second signal comprises an XOR operation of the first signal with the secret.

24. The second device of claim 1, further comprising instructions arranged to provide the secret to the first device.

25. The second device of claim 1, wherein the secret is used for generating a secure channel between the first device and the second device.

26. The second device of claim 1, wherein determining that the second signal is derived from the secret comprises: modifying the second signal, wherein the modifying requires the secret; and

determining that the modified second signal is identical to the first signal.

27. The second device of claim 1, wherein determining that the second signal is derived from the secret comprises: modifying the second signal; and

determining that the modified second signal is identical to the first signal.

28. The second device of claim 1, wherein the secret is known by the first device.

29. A method of receiving a protected content sent from a first device to a second device, the second device comprising a processor circuit, the processor circuit arranged to execute instructions implementing the method, the method comprising:

providing a certificate to the first device prior to receiving a first signal, wherein the first signal is sent by the first device, wherein the certificate is associated with the second device;

receiving the first signal from the first device when the certificate indicates that the second device is compliant with at least one compliance rule;

creating a second signal, wherein the second signal is derived from a secret known by the second device;

providing the second signal to the first device after receiving the first signal, wherein the second signal is received by the first device;

US 10,298,564 B2

9

receiving the protected content from the first device when the first device determines that the second signal is derived from the secret and a time between the sending of the first signal and the receiving of the second signal is less than a predetermined time.

30. The method of claim 29, wherein the secret is securely provided to the second device by the first device.

31. The method of claim 30, wherein determining that the second signal is derived from the secret comprises: modifying the first signal, wherein the modifying requires the secret; and determining that the modified first signal is identical to the second signal.

32. The method of claim 31, wherein the second signal comprises an XOR operation of the first signal with the secret.

33. The method of claim 31, wherein the secret comprises a first random number.

34. The method of claim 33, wherein the secret is used for generating a secure channel between the first device and the second device.

35. The method of claim 33, wherein the secret is encrypted with a public key.

36. The method of claim 35, wherein the first signal comprises a second random number.

37. The method of claim 30, wherein determining that the second signal is derived from the secret comprises: modifying the first signal; and determining that the modified first signal is identical to the second signal.

38. The method of claim 30, wherein the second signal comprises the first signal modified by the secret.

39. The method of claim 30, wherein determining that the second signal is derived from the secret comprises: modifying the second signal, wherein the modifying requires the secret; and determining that the modified second signal is identical to the first signal.

40. The method of claim 30, wherein determining that the second signal is derived from the secret comprises: modifying the second signal, wherein the modifying requires the secret; and determining that the modified second signal is identical to the first signal.

10

41. The method of claim 29, wherein determining that the second signal is derived from the secret comprises: modifying the first signal, wherein the modifying requires the secret; and determining that the modified first signal is identical to the second signal.

42. The method of claim 29, wherein determining that the second signal is derived from the secret comprises: modifying the first signal; and determining that the modified first signal is identical to the second signal.

43. The method of claim 29, wherein the predetermined time is based on a communication system associated with the first device.

44. The method of claim 29, further comprising receiving the secret from the first device.

45. The method of claim 29, wherein the second signal comprises the first signal modified by the secret.

46. The method of claim 29, wherein the secret comprises a random number.

47. The method of claim 29, wherein the secret is encrypted with a public key.

48. The method of claim 29, wherein the first signal comprises a random number.

49. The method of claim 29, wherein the second signal comprises an XOR operation of the first signal with the secret.

50. The method of claim 29, further comprising providing the secret to the first device.

51. The method of claim 29, wherein the secret is used for generating a secure channel between the first device and the second device.

52. The method of claim 29, wherein determining that the second signal is derived from the secret comprises: modifying the second signal, wherein the modifying requires the secret; and determining that the modified second signal is identical to the first signal.

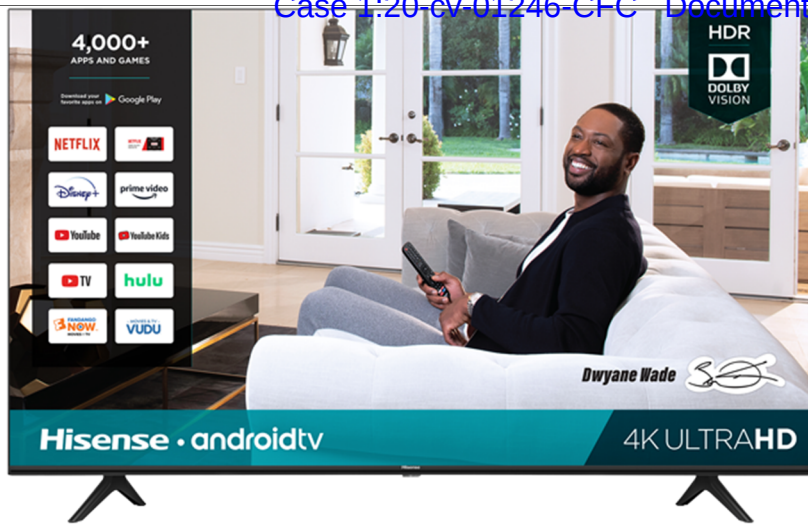
53. The method of claim 29, wherein determining that the second signal is derived from the secret comprises: modifying the second signal; and determining that the modified second signal is identical to the first signal.

* * * * *

EXHIBIT B

U.S. Patent No. 10,298,564

Hisense Product Containing MediaTek
Product
HDMI with HDCP 2.2



Hisense H65G Series 4K UHD Android Smart TV (Model # 43H6570G)
("Hisense Product")



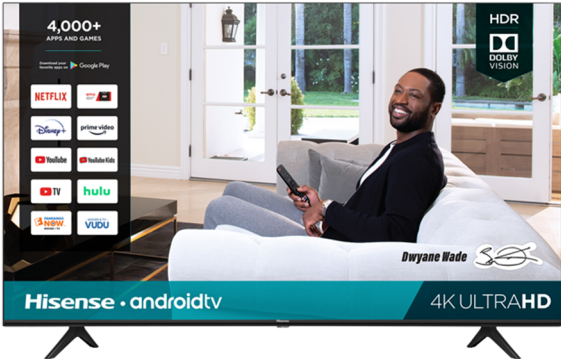
MediaTek video processing system and components thereof including MStar MSD6886NQHT Processor, main board hardware, integrated operating system, middleware, application program, video processing, and/or digital rights management ("DRM") software that runs on the Hisense Product ("MediaTek Product")

"1. A second device for receiving delivery of a protected content from a first device, the second device comprising a processor circuit, the processor circuit arranged to execute instructions, the instructions arranged to:"

1. A second device for receiving delivery of a protected content from a first device, the second device comprising a processor circuit, the processor circuit arranged to execute instructions, the instructions arranged to:

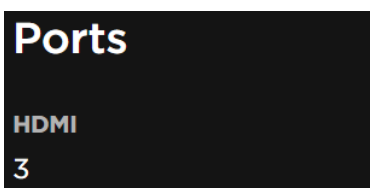
The Hisense H65G Series 4K UHD Android Smart TV (Model # 43H6570G) (the "Hisense Product") is a second device for receiving delivery of a protected content from a first device, the processor circuit arranged to execute instructions.

For example, the Hisense Product is an HDMI receiver with HDCP 2.2 for receiving delivery of protected content from another device, such as an HDMI transmitter with HDCP 2.2.



Hisense, 4K UHD HISENSE ANDROID SMART TV (2020), 43" Class- H65G Series, Model: 43H6570G, <https://www.hisense-usa.com/televisions/all-tvs/43H6570G-4k-uhd-hisense-android-smart-tv-2020>.

The Hisense Product includes three HDMI 2.0b ports that support HDCP 2.2.



Id.

"1. A second device for receiving delivery of a protected content from a first device, the second device comprising a processor circuit, the processor circuit arranged to execute instructions, the instructions arranged to:"



Hisense Product Image.

PORTS	
HDMI	3 (2.0b inputs)
Ethernet (LAN)	Yes
USB 2.0	2
RF Antenna	1
RCA Composite Video Input	1
L/R Audio Input for Composite	1

Hisense, H65 Series Android TV, Model 43H6570G, Specification Sheet, <https://assets.hisense-usa.com/assets/ProductDownloads/204/1cfe52f276/43H6570G-Spec-Sheet.pdf>.

"1. A second device for receiving delivery of a protected content from a first device, the second device comprising a processor circuit, the processor circuit arranged to execute instructions, the instructions arranged to:"

Inputs Specifications	
HDR10	Yes
HDR10+	No
Dolby Vision	Yes
HLG	Yes
3D	No
HDMI 2.0 Full Bandwidth	Yes (HDMI 1,2,3)
HDMI 2.1	No
CEC	Yes
HDCP 2.2	Yes (HDMI 1,2,3)
USB 3.0	No
Variable Analog Audio Out	Yes
Wi-Fi Support	Yes (2.4 GHz, 5 GHz)

RTINGS.com, Hisense H6570F TV Review, <https://www.rtings.com/tv/reviews/hisense/h6570f>. H6570F is a 2019 model of Hisense’s H65 Series Android TV and, upon information and belief, H6570G, the 2020 model of Hisense’s H65 Series Android TV, includes HDMI ports substantially similar to those of H6570F and is compatible with HDCP 2.2.

Upon information and belief, the Hisense Product is compliant with the High-bandwidth Digital Content Protection System Revision 2.2 (“HDCP 2.2”) protocol. The Hisense Product supports HDCP 2.2 for protecting content between devices.

For the purpose of this specification, it is assumed that the Audiovisual content is transmitted over a HDMI based wired display link. In an HDCP System, two or more HDCP Devices are interconnected through an HDCP-protected Interface. The Audiovisual Content flows from the Upstream Content Control Function into the HDCP System at the most upstream HDCP Transmitter. From there the Audiovisual Content encrypted by the HDCP System, referred to as HDCP Content, flows through a tree-shaped topology of HDCP Receivers over HDCP-protected Interfaces. This specification describes a content protection mechanism for: (1) authentication of HDCP Receivers to their immediate upstream connection (i.e., an HDCP Transmitter), (2) revocation of HDCP Receivers that are determined by the Digital Content Protection, LLC, to be invalid, and (3) HDCP Encryption of Audiovisual Content over the HDCP-protected Interfaces between HDCP Transmitters and their downstream HDCP Receivers. HDCP Receivers may render the HDCP Content in audio and visual form for human consumption. HDCP Receivers may be HDCP Repeaters that serve as downstream HDCP Transmitters emitting the HDCP Content further downstream to one or more additional HDCP Receivers.

"1. A second device for receiving delivery of a protected content from a first device, the second device comprising a processor circuit, the processor circuit arranged to execute instructions, the instructions arranged to:"

High-bandwidth Digital Content Protection System Mapping HDCP to HDMI, Rev. 2.2 (Feb. 13, 2013), available at https://www.digital-cp.com/sites/default/files/specifications/HDCP%20on%20HDMI%20Specification%20Rev2_2_Final1.pdf ("HDMI HDCP 2.2") at 5.

There are three elements of the content protection system. Each element plays a specific role in the system. First, there is the authentication protocol, through which the HDCP Transmitter verifies that a given HDCP Receiver is licensed to receive HDCP Content. The authentication protocol is implemented between the HDCP Transmitter and its corresponding downstream HDCP Receiver. With the legitimacy of the HDCP Receiver determined, encrypted HDCP Content is transmitted between the two devices based on shared secrets established during the authentication protocol. This prevents eavesdropping devices from utilizing the content. Finally, in the event that legitimate devices are compromised to permit unauthorized use of HDCP Content, renewability allows an HDCP Transmitter to identify such compromised devices and prevent the transmission of HDCP Content.

This document contains chapters describing in detail the requirements of each of these elements. In addition, a chapter is devoted to describing the cipher structure that is used in the encryption of HDCP Content.

Id. at 9.

The Hisense Product is an HDCP Device, and more specifically an HDCP 2.2-compliant Device, capable of functioning as an HDCP Receiver and that implements required functionality of HDMI HDCP 2.2 including the functions required by the HDCP Receiver State Diagram.

The state machines in this specification define the required behavior of HDCP Devices. The link-visible behavior of HDCP Devices implementing the specified state machines must be identical, even if implementations differ from the descriptions. The behavior of HDCP Devices implementing the specified state machines must also be identical from the perspective of an entity outside of the HDCP System.

Implementations must include all elements of the content protection system described herein, unless the element is specifically identified as informative or optional. Adopters must also ensure that implementations satisfy the robustness and compliance rules described in the technology license.

Id. at 5.

"1. A second device for receiving delivery of a protected content from a first device, the second device comprising a processor circuit, the processor circuit arranged to execute instructions, the instructions arranged to:"

HDCP 2.2-compliant Device. An HDCP Device that is designed in adherence to HDCP 2.2 is referred to as an *HDCP 2.2-compliant Device*.

Id. at 6.

HDCP Device. Any device that contains one or more HDCP-protected Interface Port and is designed in adherence to HDCP is referred to as an *HDCP Device*.

Id. at 7.

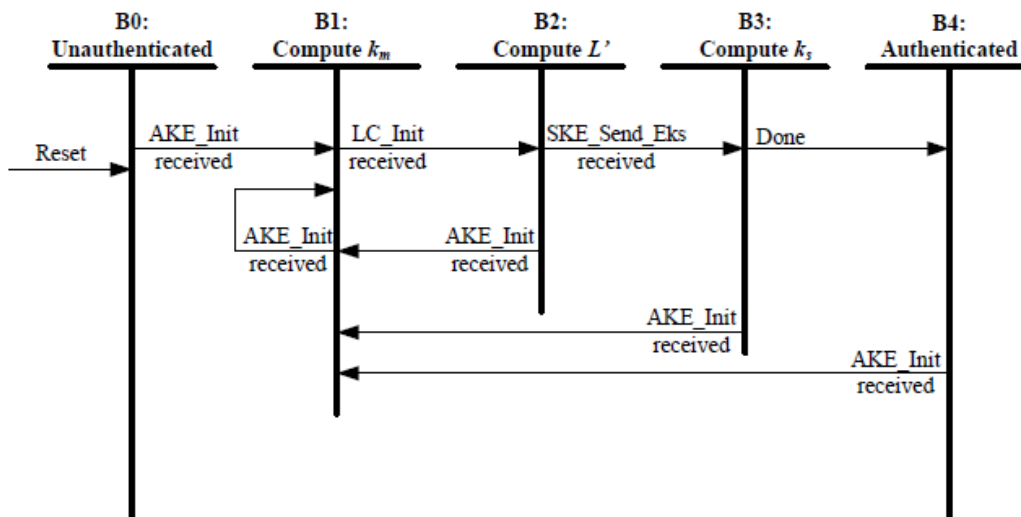


Figure 2.13. HDCP Receiver Authentication Protocol State Diagram

Id. at 31-32.

The Hisense Product includes, for example, a bit in its HDCP2Version register identifying the Hisense Product as HDCP 2 capable.

"1. A second device for receiving delivery of a protected content from a first device, the second device comprising a processor circuit, the processor circuit arranged to execute instructions, the instructions arranged to:"

State H1: Transmit Low-value Content. In this state, the transmitter reads the HDCP2Version register. The transmitter determines that the receiver is HDCP 2 capable by reading bit[2] in the receiver's HDCP2Version register. If this bit is set to 1, it indicates that the receiver is HDCP 2 capable. In this state the transmitter should begin sending an unencrypted signal with HDCP Encryption disabled. The transmitted signal can be a low value content or informative on-screen display. This will ensure that a valid video signal is displayed to the user before and during authentication.

Id. at 27.

The Hisense Product receives delivery of protected content from a first device.

2.1 Overview

The HDCP authentication protocol is an exchange between an HDCP Transmitter and an HDCP Receiver that affirms to the HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. It is comprised of the following stages

- Authentication and Key Exchange (AKE) – The HDCP Receiver's public key certificate is verified by the HDCP Transmitter. A Master Key k_m is exchanged.
- Locality Check – The HDCP Transmitter enforces locality on the content by requiring that the Round Trip Time (RTT) between a pair of messages is not more than 20 ms.
- Session Key Exchange (SKE) – The HDCP Transmitter exchanges Session Key k_s with the HDCP Receiver.
- Authentication with Repeaters – The step is performed by the HDCP Transmitter only with HDCP Repeaters. In this step, the repeater assembles downstream topology information and forwards it to the upstream HDCP Transmitter.

Successful completion of AKE and locality check stages affirms to the HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. At the end of the authentication protocol, a communication path is established between the HDCP Transmitter and HDCP Receiver that only Authorized Devices can access.

Id. at 11.

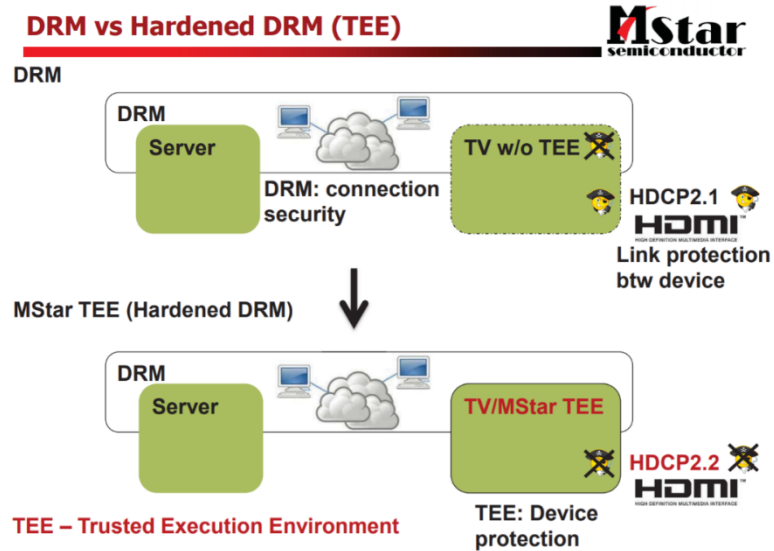
The Hisense Product comprises a processor circuit, the processor circuit arranged to execute instructions as set forth in the body of the claim. The Hisense Product includes the MStar MSD6886NQHT SoC (the "MStar SoC").

"1. A second device for receiving delivery of a protected content from a first device, the second device comprising a processor circuit, the processor circuit arranged to execute instructions, the instructions arranged to:"




Hisense Product Teardown (SoC).

The MStar SoC implements “Hardened DRM” – Mstar Trusted Execution Environment (TEE) that includes hardware support for HDCP 2.2.



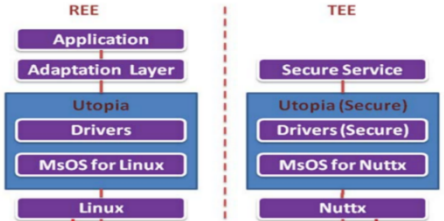
"1. A second device for receiving delivery of a protected content from a first device, the second device comprising a processor circuit, the processor circuit arranged to execute instructions, the instructions arranged to:"



MStar TEE (Global Platform)


MStar Security Platform

REE




Linux


TEE



Nuttx



1. Decrypted Contents/ Key are processed in secure zone
2. Only Secure HW IP or Secure Processor can access secure zone
3. Non-security-related items are not in secure zone. ex. MM/ PVR
4. All info from normal zone are not trusted
5. Secure boot



Security – TEE

Based on HW

- AESDMA / HDCP2.2

Key Protection

- Managed by secure Processor/HW
- Stored in HW(OTP/ROM)
- Secure Store

Security Boot

- Boot Code in HW (OTP/ROM)
- Secure Update/Debug
- Unique Device ID

Secure Video Path

- Secure Range w/o memory burden
- DRAM Scramble w/o performance impact
- Protect Decompressed content

Concurrent

- Secure Processor Performance

MStar Semiconductor, Security Evolution on TV/OTT (Jun. 2015), available at <https://ecfsapi.fcc.gov/file/60001077389.pdf>, at pp. 2, 5, 6.

On information and belief, the MStar SoC includes an ARM TrustZone-enabled Cortex-A CPU and Mali GPU, which provide hardware support for HDCP 2.2 and execute instructions.

"1. A second device for receiving delivery of a protected content from a first device, the second device comprising a processor circuit, the processor circuit arranged to execute instructions, the instructions arranged to:"

Cortex-A: Putting it All Together

21 © ARM 2015

ARM, Designing Security & Trust into Connected Devices (Nov. 10, 2015), available at https://community.arm.com/cfs-file/_key/telligent-evolution-components-attachments/01-2142-00-00-00-67-58/ARM-Techcon-Security-2015.pdf, at p. 21.

"provide a certificate to the first device prior to receiving a first signal, wherein the first signal is sent by the first device, wherein the certificate is associated with the second device;"

provide a certificate to the first device prior to receiving a first signal, wherein the first signal is sent by the first device, wherein the certificate is associated with the second device;

The instructions of the Hisense Product are arranged to provide a certificate, *e.g.*, $cert_{rx}$, to the first device (transmitter) as part of the Authentication and Key Exchange (AKE) stage of the HDCP 2.2 protocol and prior to receiving a first signal, *e.g.*, the LC_Init message including r_n , wherein the first signal is sent by the first device, and wherein the certificate is associated with the Hisense Product (second device).

The certificate, $cert_{rx}$, includes a Receiver ID for the Hisense Product, Receiver Public Key, and a cryptographic signature, amongst other information.

The HDCP Receiver is issued 1024-bit RSA public and private keys. The public key is stored in a Public Key Certificate issued by DCP LLC, denoted by $cert_{rx}$. Table 2.1 gives the fields contained in the certificate. All values are stored in big-endian format.

Name	Size (bits)	Bit position	Function
Receiver ID	40	4175:4136	Unique receiver identifier. It has the same format as an HDCP 1.x KSV i.e. it contains 20 ones and 20 zeroes
Receiver Public Key	1048	4135:3088	Unique RSA public key of HDCP Receiver denoted by $k_{pub_{rx}}$. The first 1024 bits is the big-endian representation of the modulus n and the trailing 24 bits is the big-endian representation of the public exponent e
Reserved2	4	3087:3084	Reserved for future definition. Must be 0x0 or 0x1.
Reserved1	12	3083:3072	Reserved for future definition. Must be 0x000
DCP LLC Signature	3072	3071:0	A cryptographic signature calculated over all preceding fields of the certificate. RSASSA-PKCS1-v1_5 is the signature scheme used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function

Table 2.1. Public Key Certificate of HDCP Receiver

HDMI HDCP 2.2 at 11.

Public Key Certificate. Each HDCP Receiver is issued a Public Key Certificate signed by DCP LLC, and contains the Receiver ID and RSA public key corresponding to the HDCP Receiver.

Id. at 8.

The Hisense Product provides the certificate to the transmitter as part of the AKE stage, irrespective of whether the transmitter has a Master Key k_m stored corresponding to the Receiver ID.

"provide a certificate to the first device prior to receiving a first signal, wherein the first signal is sent by the first device, wherein the certificate is associated with the second device;"

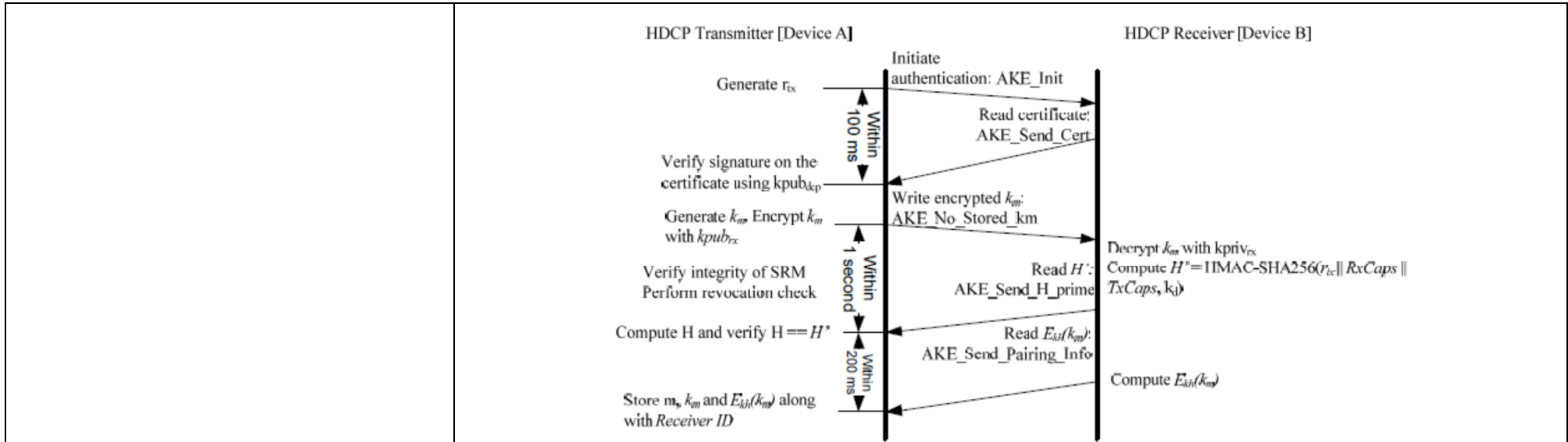


Figure 2.1. Authentication and Key Exchange (Without Stored k_m)

Id. at 12.

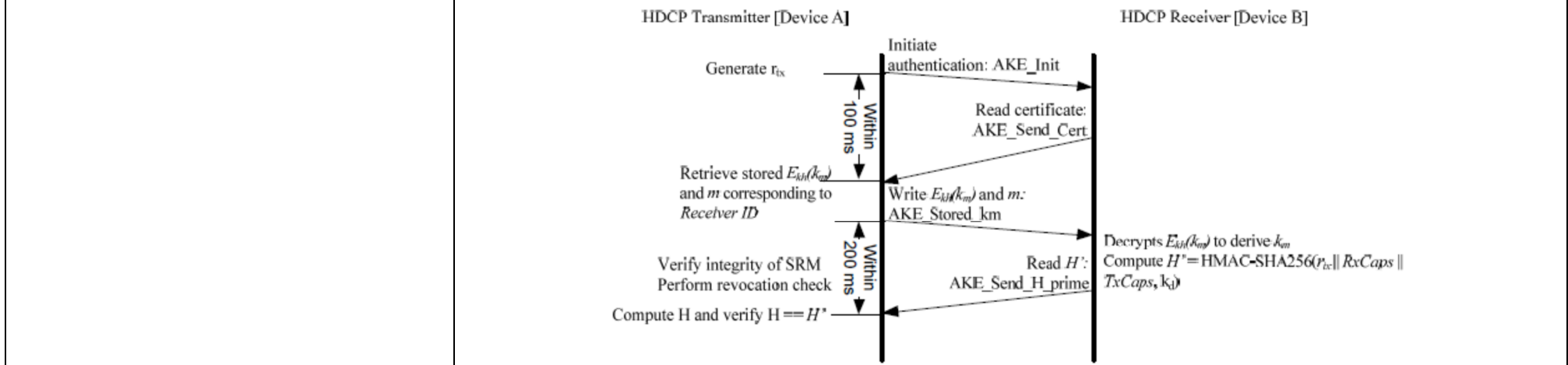


Figure 2.2. Authentication and Key Exchange (With Stored k_m)

"provide a certificate to the first device prior to receiving a first signal, wherein the first signal is sent by the first device, wherein the certificate is associated with the second device;"

Id.

The Hisense Product provides the certificate to the first device as part of the AKE_Send_Cert message.

The HDCP Receiver

- Makes available the AKE_Send_Cert message for the transmitter to read in response to AKE_Init. The AKE_Send_Cert message must be available for the transmitter to read within 100 ms from the time the transmitter finishes writing the AKE_Init message parameters to the HDCP Receiver.

Id. at 14.

Reads AKE_Send_Cert from the receiver containing $cert_{rx}$, a 64-bit pseudo-random value (r_{rx}) and $RxCaps$. REPEATER bit in $RxCaps$ indicates whether the connected receiver is an HDCP Repeater. If REPEATER is set to one, it indicates the receiver is an HDCP Repeater. If REPEATER is zero, the receiver is not an HDCP Repeater. The AKE_Send_Cert message must be available for the transmitter to read within 100 ms from the time the transmitter finishes writing the AKE_Init message parameters to the HDCP Receiver. If the AKE_Send_Cert message is not available for the transmitter to read within 100 ms, the transmitter aborts the authentication protocol.

Id. at 13.

4.2.2 AKE_Send_Cert (Read)

The HDCP Transmitter attempts to read AKE_Send_Cert beginning with $cert_{rx}$ within 100 ms after writing the AKE_Init message i.e. after the last byte of $TxCaps$ has been written.

Syntax	No. of Bytes
AKE_Send_Cert {	
msg_id (=3)	1
$cert_{rx}[4175..0]$	522
$r_{rx}[63..0]$	8
$RxCaps$	3
}	

Table 4.3. AKE_Send_Cert Format

Id. at 57.

"provide a certificate to the first device prior to receiving a first signal, wherein the first signal is sent by the first device, wherein the certificate is associated with the second device;"

The Hisense Product provides the certificate to the first device during the AKE stage prior to receiving the first signal, e.g., the LC_Init message including r_n , as part of a Locality Check.

2.3 Locality Check

Locality check is performed after AKE and pairing. The HDCP Transmitter initiates locality check by sending a 64-bit pseudo-random nonce r_n to the downstream receiver.

The HDCP Transmitter

- Initiates locality check by writing the LC_Init message containing a 64-bit pseudo-random nonce r_n to the HDCP Receiver.

Id. at 16.

See also:

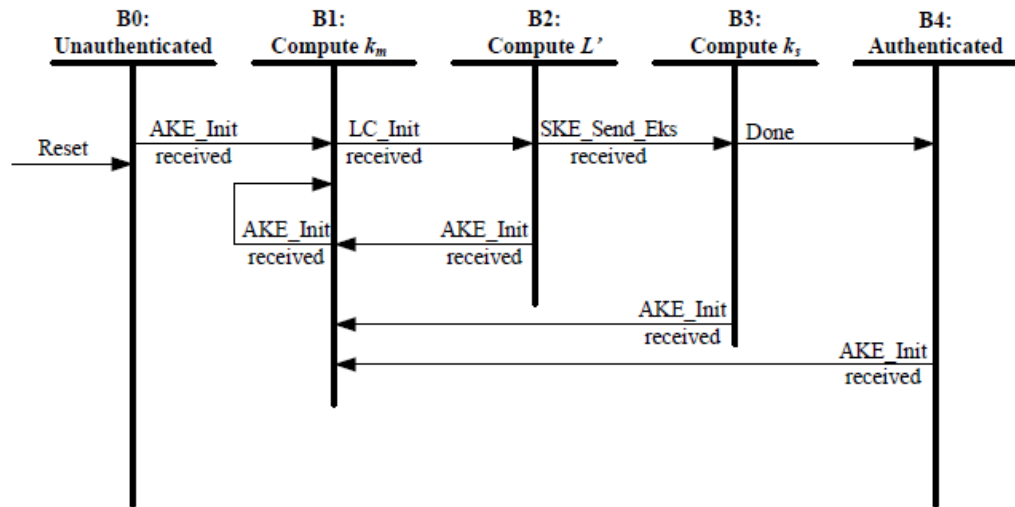


Figure 2.13. HDCP Receiver Authentication Protocol State Diagram

Id. at 31.

"provide a certificate to the first device prior to receiving a first signal, wherein the first signal is sent by the first device, wherein the certificate is associated with the second device;"

	<p>State B1: Compute k_m. In this state, the HDCP Receiver makes the AKE_Send_Cert message available for reading by the transmitter in response to AKE_Init. If AKE_No_Stored_km is received, the receiver decrypts k_m with $k_{priv_{rx}}$, calculates H'. It makes AKE_Send_H_prime message available for reading immediately after computation of H' to ensure that the message is received by the transmitter within the specified one second timeout at the transmitter.</p> <p><i>Id.</i></p>
--	--

"receive the first signal when the certificate indicates that the second device is compliant with at least one compliance rule;"

receive the first signal when the certificate indicates that the second device is compliant with at least one compliance rule;

The instructions of the Hisense Product are arranged to receive the first signal when the certificate indicates that the second device is compliant with at least one compliance rule.

The Hisense Product receives the LC_Init message including r_n when the certificate, $cert_{rx}$, indicates that the Hisense Product is compliant with at least one compliance rule. For example, the certificate, $cert_{rx}$, includes a Receiver ID, Receiver Public Key, and a cryptographic signature.

The HDCP Receiver is issued 1024-bit RSA public and private keys. The public key is stored in a Public Key Certificate issued by DCP LLC, denoted by $cert_{rx}$. Table 2.1 gives the fields contained in the certificate. All values are stored in big-endian format.

Name	Size (bits)	Bit position	Function
Receiver ID	40	4175:4136	Unique receiver identifier. It has the same format as an HDCP 1.x KSV i.e. it contains 20 ones and 20 zeroes
Receiver Public Key	1048	4135:3088	Unique RSA public key of HDCP Receiver denoted by $k_{pub_{rx}}$. The first 1024 bits is the big-endian representation of the modulus n and the trailing 24 bits is the big-endian representation of the public exponent e
Reserved2	4	3087:3084	Reserved for future definition. Must be 0x0 or 0x1.
Reserved1	12	3083:3072	Reserved for future definition. Must be 0x000
DCP LLC Signature	3072	3071:0	A cryptographic signature calculated over all preceding fields of the certificate. RSASSA-PKCS1-v1_5 is the signature scheme used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function

Table 2.1. Public Key Certificate of HDCP Receiver

HDMI HDCP 2.2 at 11.

2.3 Locality Check

Locality check is performed after AKE and pairing. The HDCP Transmitter initiates locality check by sending a 64-bit pseudo-random nonce r_n to the downstream receiver.

The HDCP Transmitter

- Initiates locality check by writing the LC_Init message containing a 64-bit pseudo-random nonce r_n to the HDCP Receiver.

Id. at 16.

"receive the first signal when the certificate indicates that the second device is compliant with at least one compliance rule;"

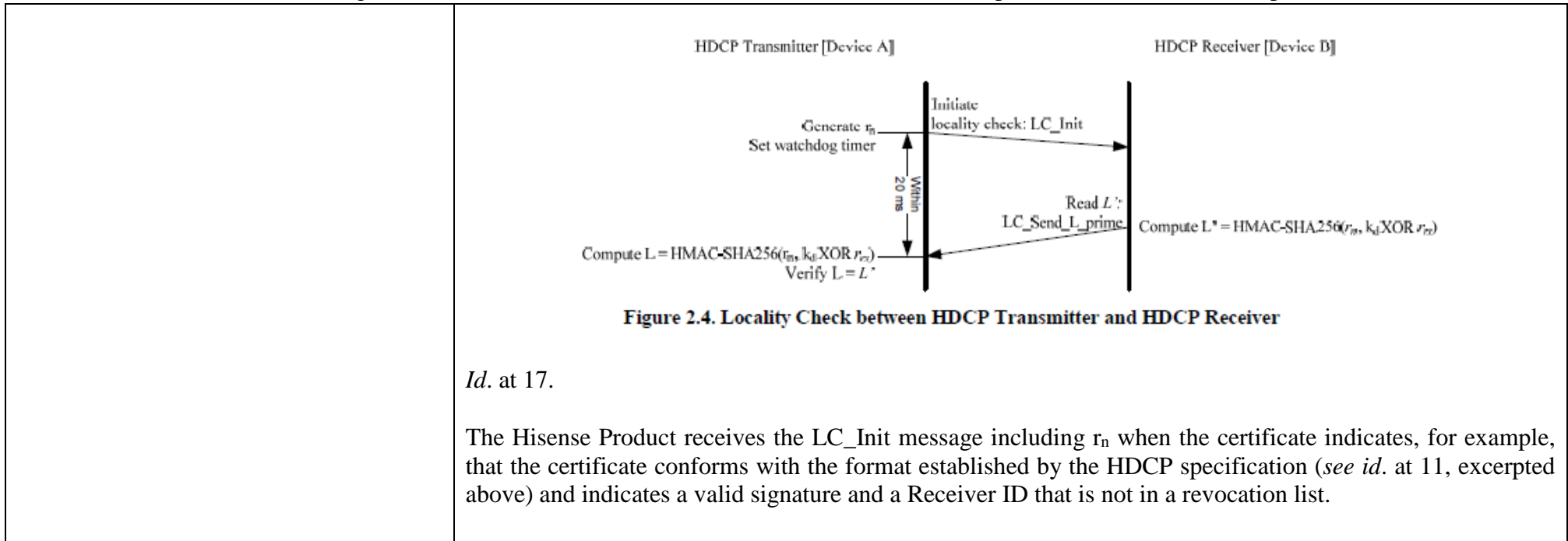


Figure 2.4. Locality Check between HDCP Transmitter and HDCP Receiver

Id. at 17.

The Hisense Product receives the LC_Init message including r_n when the certificate indicates, for example, that the certificate conforms with the format established by the HDCP specification (*see id.* at 11, excerpted above) and indicates a valid signature and a Receiver ID that is not in a revocation list.

"receive the first signal when the certificate indicates that the second device is compliant with at least one compliance rule;"

- Extracts *Receiver ID* from $cert_{rx}$
 - If the HDCP Transmitter does not have a 128-bit Master Key k_m stored corresponding to the *Receiver ID* (See Section 2.2.1)
 - Verifies the signature on the certificate using $k_{pub_{dcp}}$. Failure of signature verification constitutes an authentication failure and the HDCP Transmitter aborts the authentication protocol.
 - Generates a pseudo-random 128-bit Master Key k_m . Encrypts k_m with $k_{pub_{rx}}$ ($E_{k_{pub}}(k_m)$) and sends AKE_No_Stored_km message to the receiver containing the 1024-bit $E_{k_{pub}}(k_m)$. RSAES-OAEP encryption scheme must be used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function. The mask generation function used is MGF1 which uses SHA-256 as its underlying hash function.
 - Verifies integrity of the System Renewability Message (SRM). It does this by checking the signature of the SRM using $k_{pub_{dcp}}$. Failure of this integrity check constitutes an authentication failure and causes the HDCP Transmitter to abort authentication protocol.

The top-level HDCP Transmitter checks to see if the *Receiver ID* of the connected device is found in the revocation list. If the *Receiver ID* of the connected HDCP Device is found in the revocation list, authentication fails and the authentication protocol is aborted. SRM integrity check and revocation check are performed only by the top-level HDCP Transmitter.

Id. at 13.

A valid signature in the certificate indicates, for example, that the second device is compliant with a set of compliance rules of the HDCP specification.

1.9 “**Compliance Rules**” means the technical requirements set out in Exhibit C, as such exhibit may be amended by Licensor from time to time in accordance with the terms of this Agreement.

"receive the first signal when the certificate indicates that the second device is compliant with at least one compliance rule;"

HDCP License Agreement, March 6, 2017, at 2, available at https://digital-cp.com/sites/default/files/HDCP%20License%20Agreement_March%206%2C%202017_FOR%20REVIEW%20ONLY.pdf.

EXHIBIT C
COMPLIANCE RULES

Adopter agrees to comply with all terms and conditions of these Compliance Rules, which may be amended from time to time by Licensor in accordance with Section 5 of this Agreement.

Id. at Exhibit C.

See also:

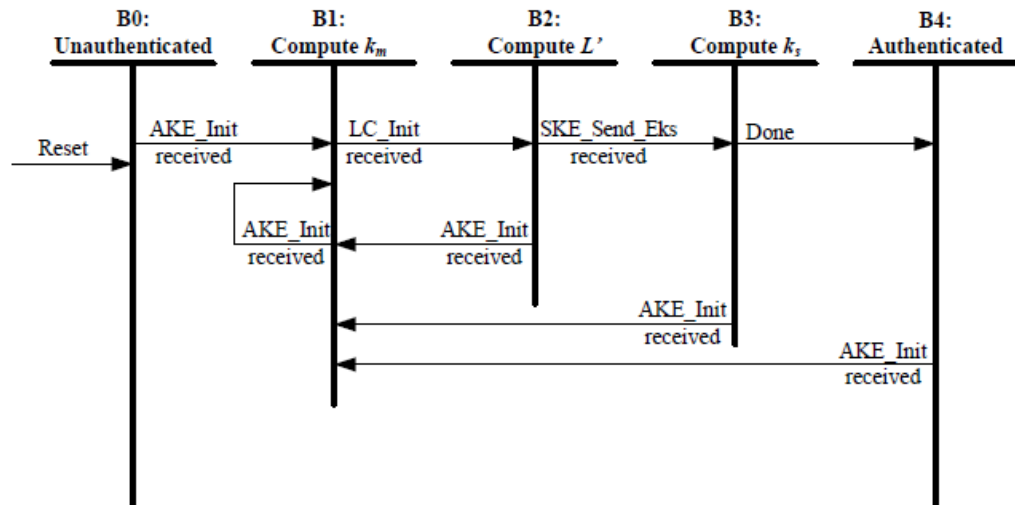


Figure 2.13. HDCP Receiver Authentication Protocol State Diagram

HDMI HDCP 2.2 at 31.

Transition B1: B2. The transition occurs when r_m is received as part of LC_Init message from the transmitter.

"receive the first signal when the certificate indicates that the second device is compliant with at least one compliance rule;"

	<i>Id.</i>
--	------------

"create a second signal, wherein the second signal is derived from a secret known by the second device;"

create a second signal, wherein the second signal is derived from a secret known by the second device;

The instructions of the Hisense Product are arranged to create a second signal, *e.g.*, L' .

The HDCP Receiver

- Computes a 256-bit value $L' = \text{HMAC-SHA256}(r_n, k_d \text{ XOR } r_{rx})$.
- Makes LC_Send_L_prime message containing 256-bit L' available for the transmitter to read immediately after computation of L' to ensure that the message is received by the transmitter within the specified 20 ms timeout at the transmitter.

HDMI HDCP 2.2 at 17.

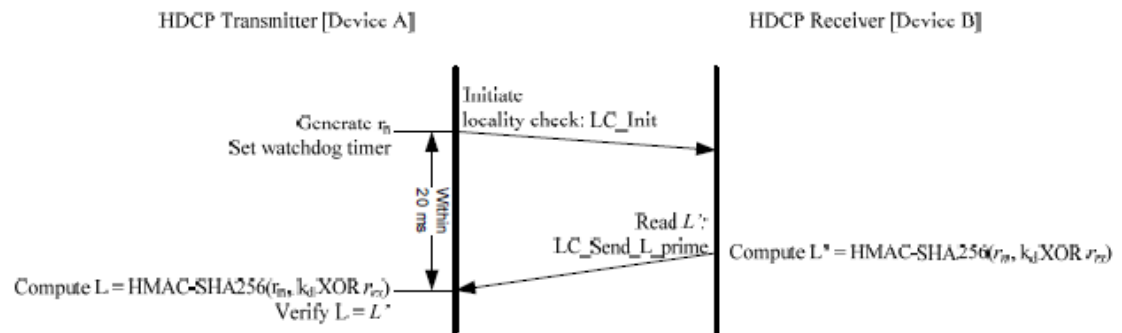


Figure 2.4. Locality Check between HDCP Transmitter and HDCP Receiver

Id.

The second signal is derived from a secret known by the Hisense Product (second device).

The value of L' is derived from k_d .

$$\text{Compute } L' = \text{HMAC-SHA256}(r_n, k_d \text{ XOR } r_{rx})$$

Id.

The value of k_d is based upon $dkey_0$ and $dkey_1$, each of which is derived from k_m , the Master Key.

"create a second signal, wherein the second signal is derived from a secret known by the second device;"

Performs key derivation as explained in Section 2.7 to generate 256-bit k_d . $k_d = dkey_0 \parallel dkey_1$, where $dkey_0$ and $dkey_1$ are derived keys generated when $ctr = 0$ and $ctr = 1$ respectively. $dkey_0$ and $dkey_1$ are in big-endian order.

Id. at 14-15.

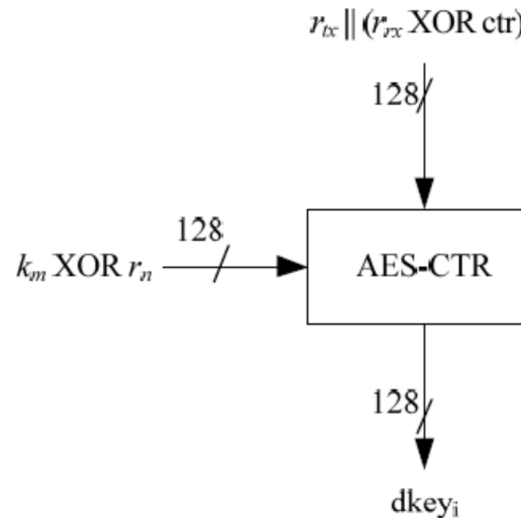


Figure 2.10. Key Derivation

Id. at 25.

Master Key. A 128-bit random, secret cryptographic key negotiated between the HDCP Transmitter and the HDCP Receiver during Authentication and Key Exchange and used to pair the HDCP Transmitter with the HDCP Receiver.

Id. at 8.

Each of k_m , k_d , $dkey_0$ and $dkey_1$ is a secret known by the Hisense Product.

"create a second signal, wherein the second signal is derived from a secret known by the second device;"

Value	Confidentiality Required [±] ?	Integrity Required [±] ?	Value used by Core Functions?	Core Function
k_m	Yes	Yes*	Yes	Handling of Master Key, during AKE (including Pairing) and Key Derivation, in plaintext form
k_d	Yes	Yes*	No	N/A
$dkey_0, dkey_1$	Yes	Yes*	No	N/A

Id. at 67 (abridged).

The Master Key, k_m , is received encrypted from the transmitter (first device) using the Hisense Product's public key, $k_{pub_{rx}}$. The Hisense Product decrypts k_m using the Hisense Product's private key, $k_{priv_{rx}}$, when the transmitter (first device) had not previously stored a k_m corresponding to the Hisense Product.

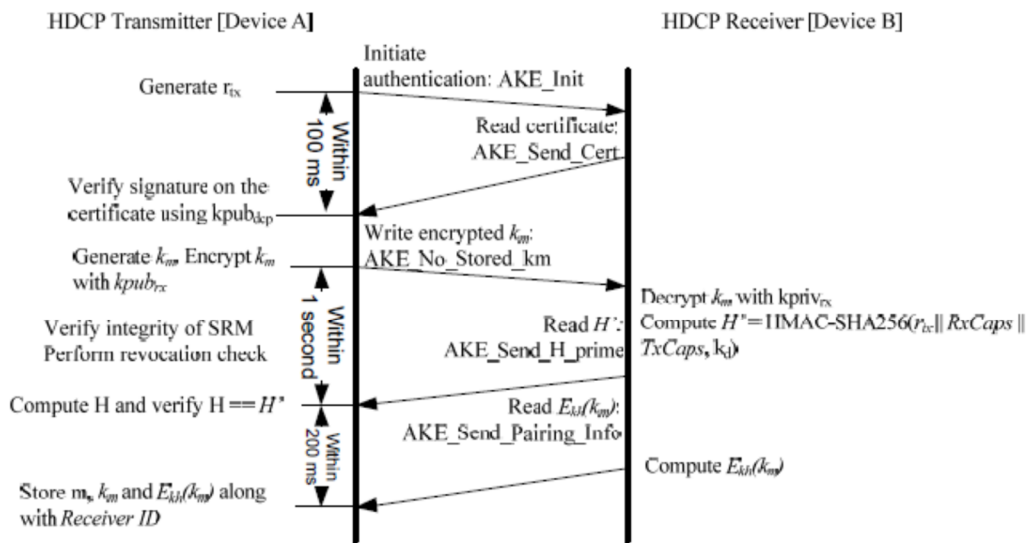


Figure 2.1. Authentication and Key Exchange (Without Stored k_m)

Id. at 12.

"create a second signal, wherein the second signal is derived from a secret known by the second device;"

- Generates a pseudo-random 128-bit Master Key k_m . Encrypts k_m with $k_{pub_{rx}}$ ($E_{k_{pub}}(k_m)$) and sends AKE_No_Stored_km message to the receiver containing the 1024-bit $E_{k_{pub}}(k_m)$. RSAES-OAEP encryption scheme must be used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function. The mask generation function used is MGF1 which uses SHA-256 as its underlying hash function.

Id. at 13.

- If AKE_No_Stored_km is received, the HDCP Receiver
 - Decrypts k_m with $k_{priv_{rx}}$ using RSAES-OAEP decryption scheme.
 - Performs key derivation as explained in Section 2.7 to generate 256-bit k_d . $k_d = dkey_0 \parallel dkey_1$, where $dkey_0$ and $dkey_1$ are derived keys generated when $ctr = 0$ and $ctr = 1$ respectively. $dkey_0$ and $dkey_1$ are in big-endian order.

Id. at 14.

The Hisense Product decrypts k_m using k_h when the transmitter (first device) previously stored a k_m corresponding to the Hisense Product.

"create a second signal, wherein the second signal is derived from a secret known by the second device;"

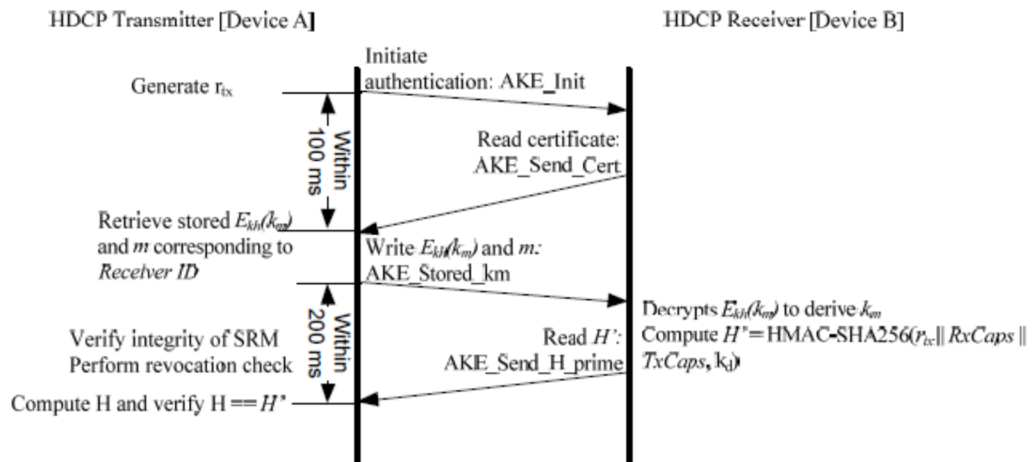


Figure 2.2. Authentication and Key Exchange (With Stored k_m)

Id. at 12.

- Sends AKE_Stored_km message to the receiver with the 128-bit $E_{kih}(k_m)$ and the 128-bit m corresponding to the *Receiver ID* of the HDCP Receiver

Id. at 14.

- If AKE_Stored_km is received, the HDCP Receiver
 - Computes 128-bit $k_h = \text{SHA-256}(k_{priv_{tx}})[127:0]$
 - Decrypts $E_{kih}(k_m)$ using AES with the received m as input and k_h as key in to the AES module as illustrated in Figure 2.3 to derive k_m .
 - Performs key derivation as explained in Section 2.7 to generate 256-bit k_d . $k_d = \text{dkey}_0 || \text{dkey}_1$, where dkey_0 and dkey_1 are derived keys generated when $\text{ctr} = 0$ and $\text{ctr} = 1$ respectively. dkey_0 and dkey_1 are in big-endian order.

Id. at 15.

"create a second signal, wherein the second signal is derived from a secret known by the second device;"

See also:

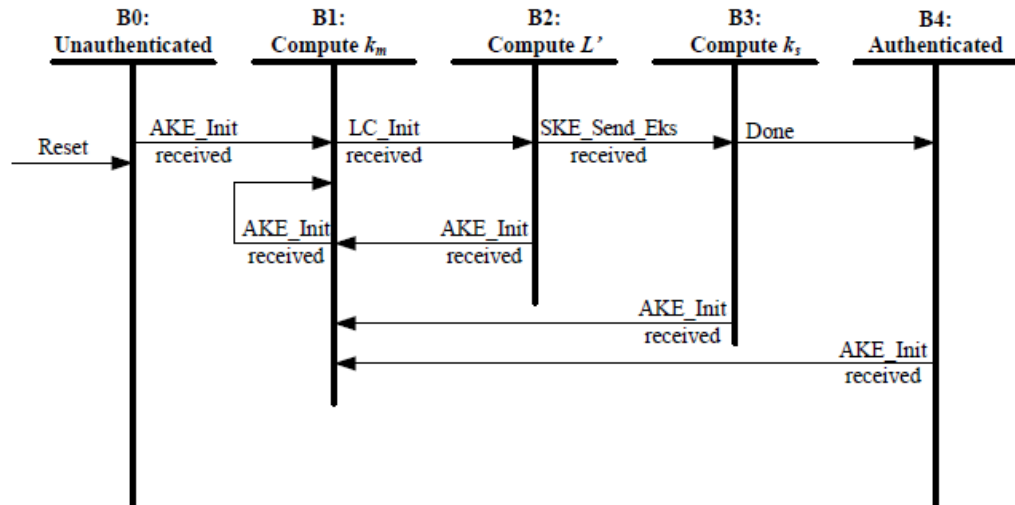


Figure 2.13. HDCP Receiver Authentication Protocol State Diagram

Id. at 31.

State B2: Compute L' . The HDCP Receiver computes L' required during locality check and makes the LC_Send_L_prime message available for reading by the transmitter.

Id.

"provide the second signal to the first device after receiving the first signal, wherein the second signal is received by the first device; and"

provide the second signal to the first device after receiving the first signal, wherein the second signal is received by the first device; and

The instructions of the Hisense Product are arranged to provide the second signal, *e.g.*, L' , to the first device (transmitter) after receiving the first signal, *e.g.*, the LC_Init message including r_n . The Hisense Product provides the second signal to the first device using, *e.g.*, the LC_Send_L_prime message, and the second signal is received by the first device.

2.3 Locality Check

Locality check is performed after AKE and pairing. The HDCP Transmitter initiates locality check by sending a 64-bit pseudo-random nonce r_n to the downstream receiver.

The HDCP Transmitter

- Initiates locality check by writing the LC_Init message containing a 64-bit pseudo-random nonce r_n to the HDCP Receiver.
- Sets its watchdog timer to 20 ms. The LC_Send_L_prime message must be received by the transmitter within 20 ms from the time the transmitter finishes writing the LC_Init message parameters to the HDCP Receiver. Locality check fails if the watchdog timer expires before the last byte of the LC_Send_L_prime message is received by the transmitter. The transmitter then aborts the authentication protocol.
- Computes $L = \text{HMAC-SHA256}(r_n, k_d \text{ XOR } r_{rx})$ where HMAC-SHA256 is computed over r_n and the key used for HMAC is $k_d \text{ XOR } r_{rx}$, where r_{rx} is XORed with the least-significant 64-bits of k_d .
- On reading LC_Send_L_prime message from the receiver, compares L and L' . Locality check fails if L is not equal to L' .

HDMI HDCP 2.2 at 16.

"provide the second signal to the first device after receiving the first signal, wherein the second signal is received by the first device; and"

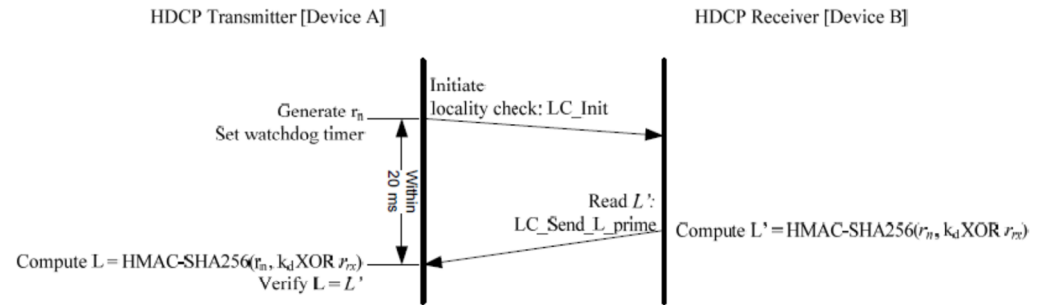


Figure 2.4. Locality Check between HDCP Transmitter and HDCP Receiver

The HDCP Receiver

- Computes a 256-bit value $L' = \text{HMAC-SHA256}(r_n, k_d \text{ XOR } r_{rx})$.
- Makes LC_Send_L_prime message containing 256-bit L' available for the transmitter to read immediately after computation of L' to ensure that the message is received by the transmitter within the specified 20 ms timeout at the transmitter.

Id. at 17.

4.2.8 LC_Send_L_prime (Read)

The LC_Send_L_prime message must be available for the transmitter to read within 20 ms from the time the transmitter finishes writing the LC_Init message parameters to the HDCP Receiver i.e. after the last byte of r_n has been written.

Syntax	No. of Bytes
LC_Send_L_prime{ msg_id (=10) L [255..0]	1 32
}	

Table 4.10. LC_Send_L_prime Format

Id. at 59.

See also:

"provide the second signal to the first device after receiving the first signal, wherein the second signal is received by the first device; and"

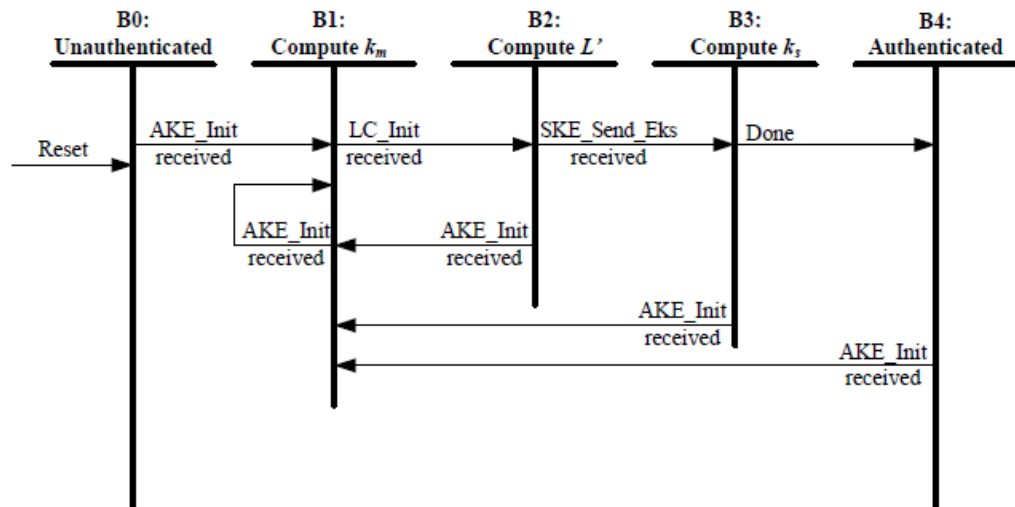


Figure 2.13. HDCP Receiver Authentication Protocol State Diagram

Id. at 31.

State B2: Compute L' . The HDCP Receiver computes L' required during locality check and makes the LC_Send_L_prime message available for reading by the transmitter.

Id.

"receive the protected content from the first device when the first device determines that the second signal is derived from the secret and a time between the sending of the first signal and the receiving of the second signal is less than a predetermined time."

receive the protected content from the first device when the first device determines that the second signal is derived from the secret and a time between the sending of the first signal and the receiving of the second signal is less than a predetermined time.

The instructions of the Hisense Product are arranged to receive the protected content from the first device when the first device determines that the second signal, *e.g.*, L' , is derived from the secret and a time between the sending of the first signal, *e.g.*, the LC_Init message including r_n , and the receiving of the second signal is less than a predetermined time.

The HDCP 2.2 Locality Check must be passed prior to session key exchange and establishment of a secure communications path for receipt of protected content by the Hisense Product.

The HDCP authentication protocol is an exchange between an HDCP Transmitter and an HDCP Receiver that affirms to the HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. It is comprised of the following stages

- Authentication and Key Exchange (AKE) – The HDCP Receiver's public key certificate is verified by the HDCP Transmitter. A Master Key k_m is exchanged.
- Locality Check – The HDCP Transmitter enforces locality on the content by requiring that the Round Trip Time (RTT) between a pair of messages is not more than 20 ms.
- Session Key Exchange (SKE) – The HDCP Transmitter exchanges Session Key k_s with the HDCP Receiver.
- Authentication with Repeaters – The step is performed by the HDCP Transmitter only with HDCP Repeaters. In this step, the repeater assembles downstream topology information and forwards it to the upstream HDCP Transmitter.

Successful completion of AKE and locality check stages affirms to the HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. At the end of the authentication protocol, a communication path is established between the HDCP Transmitter and HDCP Receiver that only Authorized Devices can access.

HDMI HDCP 2.2 at 11.

The Hisense Product receives protected content after the first device, as part of the Locality Check, determines that: the L' received via the LC_Send_L_prime message is derived from the secret (as determined by matching L' to value L which is derived from the secret (*e.g.*, L is computed based on k_d , which is based on $dkey_0$ and $dkey_1$, each of which is based on the Master Key, k_m)); and a time between the sending of the LC_Init message and receiving L' via the LC_Send_L_prime message is less than a predetermined time of 20 ms.

"receive the protected content from the first device when the first device determines that the second signal is derived from the secret and a time between the sending of the first signal and the receiving of the second signal is less than a predetermined time."

2.3 Locality Check

Locality check is performed after AKE and pairing. The HDCP Transmitter initiates locality check by sending a 64-bit pseudo-random nonce r_n to the downstream receiver.

The HDCP Transmitter

- Initiates locality check by writing the LC_Init message containing a 64-bit pseudo-random nonce r_n to the HDCP Receiver.
- Sets its watchdog timer to 20 ms. The LC_Send_L_prime message must be received by the transmitter within 20 ms from the time the transmitter finishes writing the LC_Init message parameters to the HDCP Receiver. Locality check fails if the watchdog timer expires before the last byte of the LC_Send_L_prime message is received by the transmitter. The transmitter then aborts the authentication protocol.
- Computes $L = \text{HMAC-SHA256}(r_n, k_d \text{ XOR } r_{rx})$ where HMAC-SHA256 is computed over r_n and the key used for HMAC is $k_d \text{ XOR } r_{rx}$, where r_{rx} is XORed with the least-significant 64-bits of k_d .
- On reading LC_Send_L_prime message from the receiver, compares L and L' . Locality check fails if L is not equal to L' .

Id. at 16.

"receive the protected content from the first device when the first device determines that the second signal is derived from the secret and a time between the sending of the first signal and the receiving of the second signal is less than a predetermined time."

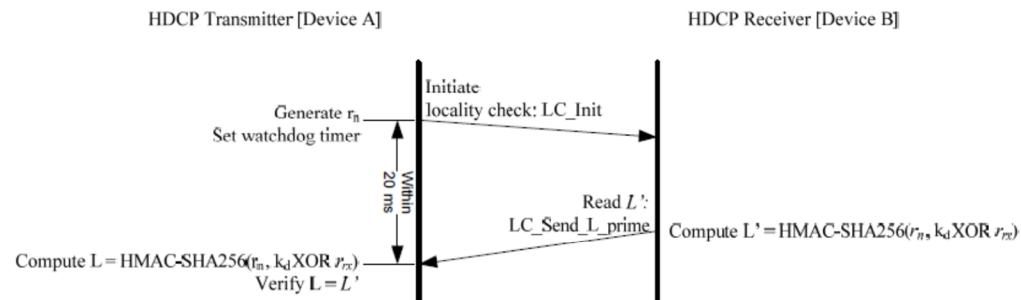


Figure 2.4. Locality Check between HDCP Transmitter and HDCP Receiver

The HDCP Receiver

- Computes a 256-bit value $L' = \text{HMAC-SHA256}(r_n, k_d \text{ XOR } r_n)$.
- Makes LC_Send_L_prime message containing 256-bit L' available for the transmitter to read immediately after computation of L' to ensure that the message is received by the transmitter within the specified 20 ms timeout at the transmitter.

In the case of a locality check failure due to expiration of the watchdog timer or due to mismatch of L and L' at the HDCP Transmitter, locality check may be reattempted by the HDCP Transmitter for a maximum of 1023 additional attempts (for a maximum allowed 1024 total trials) with the transmission of an LC_Init message containing a new r_n . Failure of locality check on the first attempt and subsequent zero or more reattempts results in an authentication failure and the authentication protocol is aborted.

Id. at 17.

The Hisense Product proceeds to session key exchange and receipt of the protected content after successful completion of the AKE stage and Locality Check.

2.4 Session Key Exchange

Successful completion of AKE and locality check stages affirms to HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. Session Key Exchange (SKE) is initiated by the HDCP Transmitter after a successful locality check. The HDCP Transmitter sends encrypted Session Key to the HDCP Receiver at least 200 ms before enabling HDCP Encryption and beginning the transmission of HDCP Content. HDCP Encryption may be enabled 200 ms after the transmission of the encrypted Session Key to the HDCP Receiver and at no time prior. Content encrypted with the Session Key k_s starts to flow between the HDCP Transmitter and HDCP Receiver. HDCP Encryption must be enabled only after successful completion of AKE, locality check and SKE stages.

"receive the protected content from the first device when the first device determines that the second signal is derived from the secret and a time between the sending of the first signal and the receiving of the second signal is less than a predetermined time."

Id.

3.1 Data Encryption

HDCP Encryption is applied at the input to the T.M.D.S. Encoder and decryption is applied at the output of the T.M.D.S. Decoder (Figure 3-1). HDCP Encryption consists of a bit-wise exclusive-or (XOR) of the HDCP Content with a pseudo-random data stream produced by the HDCP Cipher.

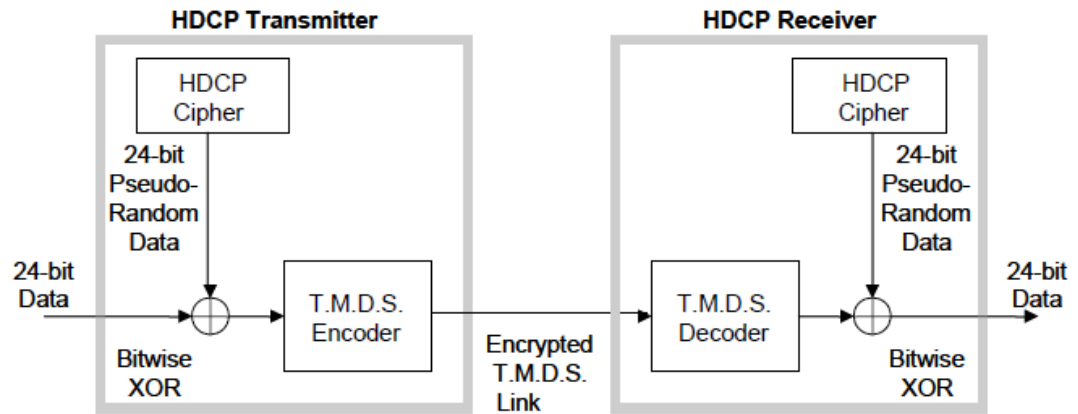


Figure 3-1. HDCP Encryption and Decryption

Id. at 50.

See also:

"receive the protected content from the first device when the first device determines that the second signal is derived from the secret and a time between the sending of the first signal and the receiving of the second signal is less than a predetermined time."

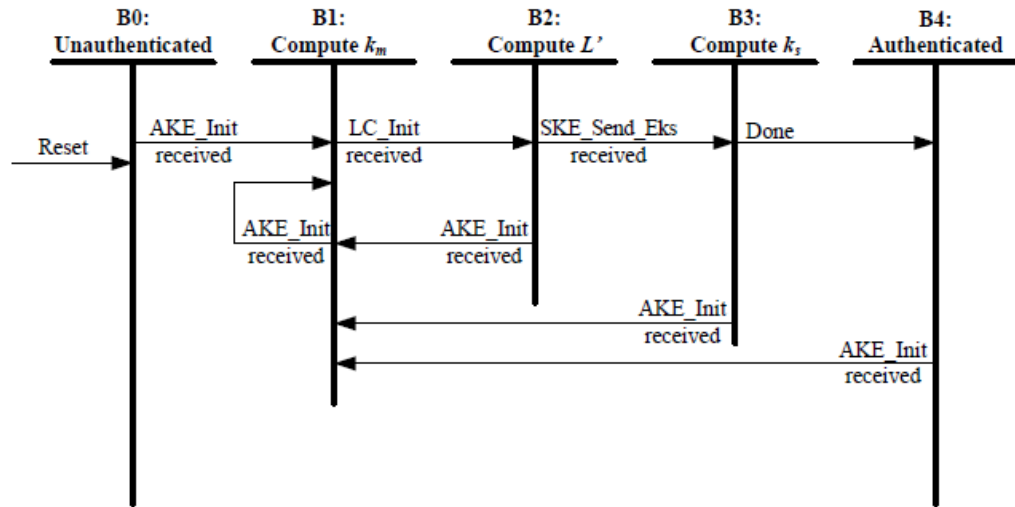


Figure 2.13. HDCP Receiver Authentication Protocol State Diagram

Id. at 31.

State B3: Compute k_s . The HDCP Receiver decrypts $E_{dk_0}(k_s)$ to derive k_s .

Transition B3: B1. Should the HDCP Transmitter write an AKE_Init while the HDCP Receiver is in State B3, the HDCP Receiver abandons intermediate results and restarts computation of k_m .

Transition B3: B4. Successful computation of k_s transitions the receiver into the authenticated state.

State B4: Authenticated. The HDCP Receiver has completed the authentication protocol. It must perform an ongoing link integrity check as described in Section 2.6. If the Receiver detects a synchronization mismatch between Transmitter and Receiver during the link integrity check, it must set the REAUTH_REQ bit in the *Rx>Status* register.

Id. at 32.