IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

DRM VECTORS, LLC, **Plaintiff,** **v.** **MICROSOFT CORPORATION,** **Defendant.**	**CIVIL ACTION NO.** **JURY TRIAL DEMANDED**

PLAINTIFF'S ORIGINAL COMPLAINT

Plaintiff DRM Vectors, LLC ("Plaintiff"), by and through its undersigned counsel, files this Original Complaint against Defendant Microsoft Corporation ("Defendant") as follows:

NATURE OF THE ACTION

1. This is a patent infringement action to stop Defendant's infringement of United States Patent No. 9,305,143 ("the '143 patent") entitled "Broadcasting of Electronic Documents Preserving Copyright and Permitting Private Copying". A true and correct copy of the '143 patent is attached hereto as Exhibit A. Plaintiff is the owner by assignment of the '143 patent. Plaintiff seeks monetary damages and injunctive relief.

PARTIES

2. Plaintiff is a limited liability company having a principal place of business located at 717 North Union St. Wilmington, DE 19805.

3. Upon information and belief, Defendant is a corporation organized and existing under the laws of the State of Washington with a principal place of business located at One Microsoft Way Redmond, WA 98052. Defendant can be served with process by serving the Corporation Service Company, 300 Deschutes Way SW STE 304, Tumwater, WA, 98501-7719.

JURISDICTION AND VENUE

4. This action arises under the Patent Laws of the United States, 35 U.S.C. § 1 *et seq.*, including 35 U.S.C. §§ 271, 281, 283, 284, and 285.

5. This Court has subject matter jurisdiction over this case for patent infringement under 28 U.S.C. §§ 1331 and 1338(a).

6. The Court has personal jurisdiction over Defendant because Defendant is present within or has minimum contacts within the State of Delaware and the District of Delaware; Defendant has purposefully availed itself of the privileges of conducting business in the State of Delaware and in the District of Delaware; Defendant has sought protection and benefit from the laws of the State of Delaware; Defendant regularly conducts business within the State of Delaware and within the District of Delaware; and Plaintiff's cause of action arises directly from Defendant's business contacts and other activities in the State of Delaware and in the District of Delaware. Further, this Court has personal jurisdiction over Defendant because it is incorporated in Delaware and has purposely availed itself of the privileges and benefits of the laws of the State of Delaware.

7. More specifically, Defendant, directly and/or through intermediaries, ships, distributes, uses, provides, offers for sale, sells, and/or advertises products and services in the United States, the State of Delaware, and the District of Delaware including but not limited to the Accused Instrumentalities as detailed below. Upon information and belief, Defendant has committed patent infringement in the State of Delaware and in the District of Delaware. Defendant solicits and has solicited customers in the State of Delaware and in the District of Delaware. Defendant has paying customers who are residents of the State of Delaware and the

District of Delaware and who each use and have used the Defendant's products and services in the State of Delaware and in the District of Delaware.

8. Venue is proper in the District of Delaware pursuant to 28 U.S.C. §§ 1400(b). On information and belief, Defendant is incorporated in this district, or has a regular and established business presence in this district and has transacted business in this district, and has directly and/or indirectly committed acts of patent infringement in this district.

COUNT I – PATENT INFRINGEMENT

9. Plaintiff refers to and incorporates herein the allegations of Paragraphs 1-8 above.

10. The '143 patent was duly and legally issued by the United States Patent and Trademark Office on April 5, 2016 after full and fair examination. Plaintiff is the owner by assignment of the '143 patent and possesses all rights of recovery under the '143 patent, including the exclusive right to sue for infringement and recover past damages and obtain injunctive relief.

11. Defendant owns, uses, operates, advertises, controls, sells, and otherwise provides systems, methods and apparatus that infringe the '143 patent. The '143 patent provides, among other things, "a method of broadcasting electronic documents allowing the protection of copyright and private copying including a network accessible control server taking customer orders, network accessible delivery and control servers, and equipment supporting a display for consulting the document."

Defendant has been and is now infringing the '143 patent in the State of Delaware, in this judicial district, and elsewhere in the United States, by, among other things, directly or through intermediaries, making, using, importing, testing, providing, supplying, distributing, selling, and/or offering for sale, methods (including, without limitation, the Defendant's products

including Microsoft PlayReady platform, content and copyright protection functionality identified herein as the "Accused Instrumentality") that provide methods for accessing an order server containing models of documents to distribute, an item database, a customer database with the emails of customers, an order database containing references of the works ordered, and digital rights associated with the works ordered, said digital rights comprising controlled consultation rights as constraints, and permanently acquired digital rights, the order server configured for handling an order received from the customer on the network accessing a delivery server via the network, the delivery server configured for generating a specific copy of a document ordered by a customer from the model of the document ordered, the order server sending order information to the delivery server, the order information comprising, at least the reference to the work, customer contact information, the controllable consultation rights,and other digital rights ordered, the delivery server creating a delivery record of the work ordered containing the unique identifier to control the said work ordered, the order server responding to the customer's order by sending the customer a URL link towards the delivery server, the URL link comprising, as a parameter, at least the unique identifier of the copy ordered; responsive to an activation of the URL link by the customer, the delivery server generating a specific copy of the work ordered, by a library used for creation of documents on the fly containing the unique identifier, a supervision agent for the document, and the other permanently acquired digital rights relating to the document, the supervision agent designed to verify the controlled digital rights of each copy of the ordered work; accessing a control server via the network, the control server configured to verify digital rights acquired by the customer using the unique identifier of the ordered document copy; when delivering the ordered document copy to the customer, the delivery server sending to the control server the controlled information containing at least the

unique identifier of the ordered document copy and the set of digital rights controlled; and operating a customer computing device, supporting a viewer, to allow the customer, via the viewer, to consult the ordered document, previously downloaded from the delivery server, said viewer designed to allow the customer to consult the ordered document; and a verification step comprising the sub-steps of when opening the specific copy on the customer computing device, the supervision agent of the specific copy causing the customer computing device to connect to the control server, and the supervision agent of the specific copy sending a query containing at least the unique identifier of the specific copy, in response to receiving the query, the control server returning a response comprised of one of i) an authorization to consult the specific copy, and ii) a consultation refusal, according to the specific copy's controlled digital rights as stored by the control server, and when the customer computing device receives the response from the control server, the supervision agent of the specific copy allowing the consultation of the specific copy when the response comprises the authorization to consult the specific copy and prohibiting the consultation of the specific copy when the response comprises the consultation refusal covered by at least claim 1 of the '143 patent to the injury of DRM Vectors, LLC. Defendant is directly infringing, literally infringing, and/or infringing the '143 patent under the doctrine of equivalents. Defendant is thus liable for infringement of the '143 patent pursuant to 35 U.S.C. § 271.

15. Defendant has induced and continues to induce infringement of the '143 patent by intending that others use, offer for sale, or sell in the United States, products and/or methods covered by one or more claims of the '143 patent, including, but not limited to, methods, and products comprising methods that broadcast electronic documents which preserve copyrights and premite private copying that infringe one or more claims of the '143 patent.

16. Defendant indirectly infringes the '143 patent by inducing infringement by others, such as resellers, customers and end-use consumers, in accordance with 35 U.S.C. § 271(b) in this District and elsewhere in the United States. Direct infringement is a result of the activities performed by the resellers, customers and end-use consumers of the broadcasting of electronic documents which preserve copyrights and permit private copying, including methods, and products comprising methods for broadcasting electronic documents which preserve copyrights and permit private copying.

17. Defendant received notice of the '143 patent at least as of the date this lawsuit was filed.

18. Defendant's affirmative acts of providing and/or selling the methods, and products comprising methods for broadcasting electronic documents which preserve copyrights and permit private copying, including manufacturing and distributing, and providing instructions for using the methods, and products comprising methods for broadcasting electronic documents which preserve copyrights and permit private copying in their normal and customary way to infringe one or more claims of the '143 patent. Defendant performs the acts that constitute induced infringement, and induce actual infringement, with the knowledge of the '143 patent and with the knowledge or willful blindness that the induced acts constitute infringement.

19. Defendant specifically intends for others, such as resellers, customers and end-use consumers, to directly infringe one or more claims of the '143 patent, or, alternatively, has been willfully blind to the possibility that its inducing acts would cause infringement. By way of example, and not as limitation, Defendant induces such infringement by its affirmative action by, among other things: (a) providing advertising on the benefits of using the Accused

Instrumentalities' functionality; (b) providing information regarding how to use the Accused Instrumentalities' functionality; (c) providing instruction on how to use the Accused Instrumentalities' functionality; and (d) providing hardware and/or software components required to infringe the claims of the '143 patent.

20. Accordingly, a reasonable inference is that Defendant specifically intends for others, such as resellers, customers and end-use consumers, to directly infringe one or more claims of the '143 patent in the United States because Defendant has knowledge of the '143 patent at least as of the date this lawsuit was filed and Defendant actually induces others, such as resellers, customers and end-use consumers, to directly infringe the '143 patent by using, selling, and/or distributing, within the United States, methods, and products comprising methods for broadcasting electronic documents which preserve copyrights and permit private copying.

21. As a result of Defendant's acts of infringement, Plaintiff has suffered and will continue to suffer damages in an amount to be proved at trial.

22. Defendant continues advising, encouraging, or otherwise inducing others to use the methods, and products comprising the methods claimed by the '143 patent to the injury of Plaintiff. Since at least the filing date of the Original Complaint, Defendant has had knowledge of the '143 patent, and by continuing the actions described above, has specific intent to induce infringement of the '143 patent pursuant to 35 U.S.C. § 271(b), and has further contributed to said infringement of the '143 patent by their customers by providing them with the Accused Instrumentalities so that their customers could directly infringe the '143 patent.

23. Claim 1 of the '143 patent, claims:

24. An electronic document creation method protecting copyrights and allowing private copying, comprising the steps of:

accessing an order server containing models of documents to distribute, an item database, a customer database with the emails of customers, an order database containing references of the works ordered, and digital rights associated with the works ordered, said digital rights comprising controlled consultation rights as constraints, and permanently acquired digital rights, the order server configured for handling an order received from the customer on the network;

accessing a delivery server via the network, the delivery server configured for generating a specific copy of a document ordered by a customer from the model of the document ordered, the order server sending order information to the delivery server, the order information comprising, at least the reference to the work, customer contact information, the controllable consultation rights,and other digital rights ordered;

the delivery server creating a delivery record of the work ordered containing the unique identifier to control the said work ordered;

the order server responding to the customer's order by sending the customer a URL link towards the delivery server, the URL link comprising, as a parameter, at least the unique identifier of the copy ordered;

responsive to an activation of the URL link by the customer, the delivery server generating a specific copy of the work ordered, by a library used for creation of documents on the fly containing the unique identifier, a supervision agent for the document, and the other permanently acquired digital rights relating to the document, the supervision agent designed to verify the controlled digital rights of each copy of the ordered work;

accessing a control server via the network, the control server configured to verify digital rights acquired by the customer using the unique identifier of the ordered document copy;

when delivering the ordered document copy to the customer, the delivery server sending to the control server the controlled information containing at least the unique identifier of the ordered document copy and the set of digital rights controlled; and

operating a customer computing device, supporting a viewer, to allow the customer, via the viewer, to consult the ordered document, previously downloaded from the delivery server, said viewer designed to allow the customer to consult the ordered document; and

a verification step comprising the sub-steps of

when opening the specific copy on the customer computing device, the supervision agent of the specific copy causing the customer computing device to connect to the control server, and the supervision agent of the specific copy sending a query containing at least the unique identifier of the specific copy;

in response to receiving the query, the control server returning a response comprised of one of i) an authorization to consult the specific copy, and ii) a consultation refusal, according to the specific copy's controlled digital rights as stored by the control server, and

when the customer computing device receives the response from the control server, the supervision agent of the specific copy allowing the consultation of the specific copy when the response comprises the authorization to consult the specific copy and prohibiting the consultation of the specific copy when the response comprises the consultation refusal.

25. An electronic document creation method protecting copyrights and allowing private copying, comprising the steps of:

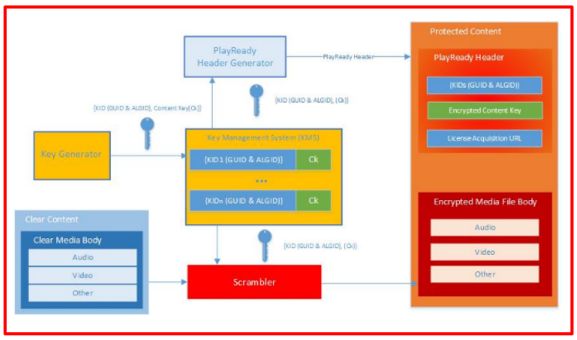
Microsoft

Microsoft PlayReady

Secure audio/video content against unauthorized use, and help monetize content

Microsoft PlayReady content access and protection technology is a set of technologies that can be used to distribute audio/video content more securely over a network, and help prevent the unauthorized use of this content. This technology is used for defining, incorporating, and enforcing rights for digital media. The service provider and content provider can control the expiration date, the number of times a user can play the content file, the resolution of the content that can be played on a screen, the type of screen that content is rendered to, and many other control settings. PlayReady technologies can be incorporated into media applications on televisions, set top boxes, mobile phones, tablets, personal computers, and other devices to enforce the content access rules defined by the content owners.

Source: https://docs.microsoft.com/en-us/playready/



Source:https://docs.microsoft.com/en-us/playready/overview/key-and-key-ids-kids

HTML5 platforms have leveraged PlayReady and many PlayReady endpoints now support MPEG-Dash. PlayReady in Action

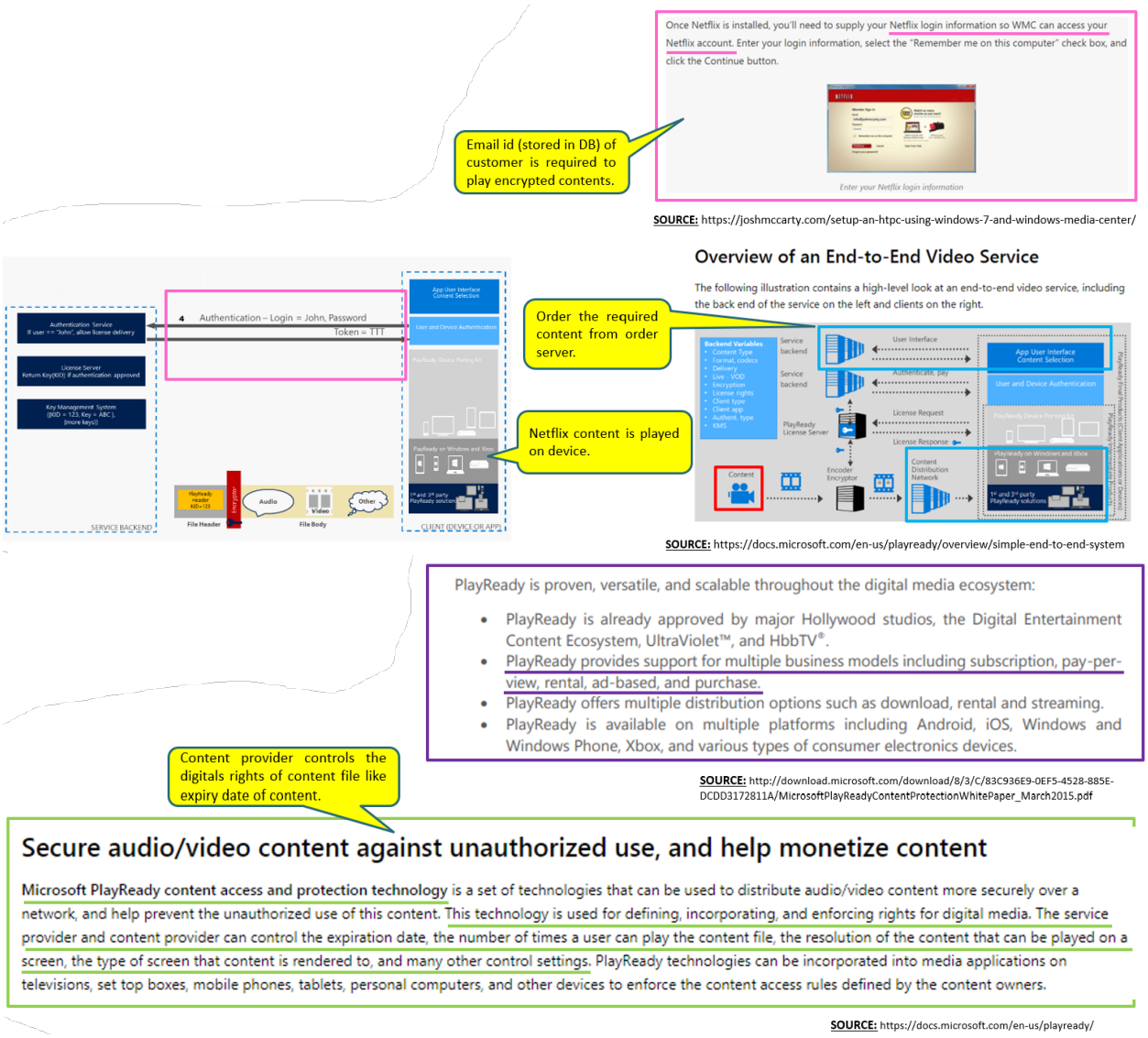
In general, content protection systems are designed to do the following:

1. Secure the distribution of digital content.
2. Allow rights to that content to be specified and enforced.

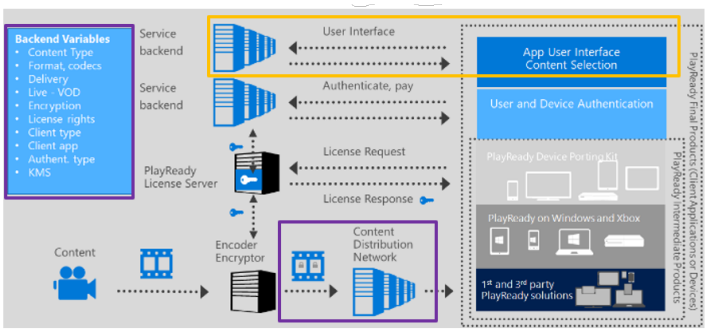
PlayReady secures content by encrypting data files. These encrypted files may be moved, archived, streamed, copied, or distributed without restrictions. In order to decrypt these data files, a digital *key* is required. This key is contained within a *license*. Each license also contains rights and policies that specify how the files may be used, and under what conditions.

Source: http://download.microsoft.com/download/8/3/C/83C936E9-0EF5-4528-885E-DCDD3172811A/MicrosoftPlayReadyContentProtectionWhitePaper_March2015.pdf

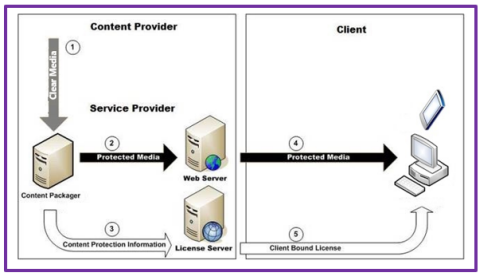
accessing an order server containing models of documents to distribute, an item database, a customer database with the emails of customers, an order database containing references of the works ordered, and digital rights associated with the works ordered, said digital rights comprising
controlled consultation rights as constraints, and permanently acquired digital rights, the order server configured for handling an order received from the customer on the network;



accessing a delivery server via the network, the delivery server configured for generating a specific copy of a document ordered by a customer from the model of the document ordered, the order server sending order information to the delivery server, the order information comprising, at least the reference to the work, customer contact information, the controllable consultation rights,and other digital rights ordered;



Delivery server provides copy of content sent to user device.



SOURCE: https://docs.microsoft.com/en-us/playready/overview/simple-end-to-end-system

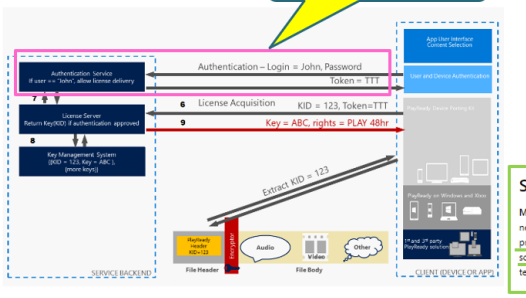
SOURCE: https://docs.microsoft.com/en-us/playready/overview/ecosystem

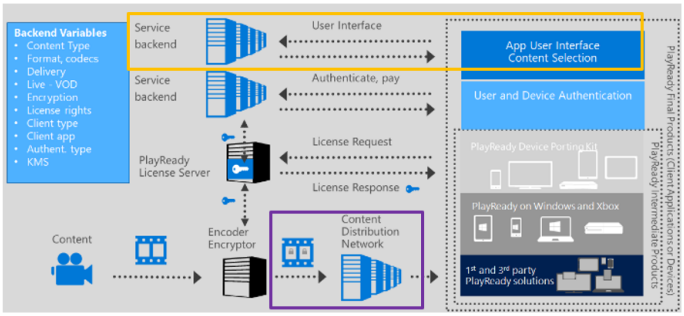
PlayReady is proven, versatile, and scalable throughout the digital media ecosystem:

- PlayReady is already approved by major Hollywood studios, the Digital Entertainment Content Ecosystem, UltraViolet™, and HbbTV®.
- PlayReady provides support for multiple business models including subscription, pay-per-view, rental, ad-based, and purchase.
- PlayReady offers multiple distribution options such as download, rental and streaming.
- PlayReady is available on multiple platforms including Android, iOS, Windows and Windows Phone, Xbox, and various types of consumer electronics devices.

SOURCE: http://download.microsoft.com/download/8/3/C/83C936E9-0EF5-4528-885E-DCDD3172811A/MicrosoftPlayReadyContentProtectionWhitePaper_March2015.pdf

Checking contact information through the server.





SOURCE: https://docs.microsoft.com/en-us/playready/overview/simple-end-to-end-system

SOURCE: https://docs.microsoft.com/en-us/playready/overview/simple-end-to-end-system

Secure audio/video content against unauthorized use, and help monetize content

Microsoft PlayReady content access and protection technology is a set of technologies that can be used to distribute audio/video content more securely over a network, and help prevent the unauthorized use of this content. This technology is used for defining, incorporating, and enforcing rights for digital media. The service provider and content provider can control the expiration date, the number of times a user can play the content file, the resolution of the content that can be played on a screen, the type of screen that content is rendered to, and many other control settings. PlayReady technologies can be incorporated into media applications on televisions, set top boxes, mobile phones, tablets, personal computers, and other devices to enforce the content access rules defined by the content owners.

SOURCE: https://docs.microsoft.com/en-us/playready

the delivery server creating a delivery record of the work ordered containing the unique identifier to control the said work ordered;

PlayReady Servers

PlayReady Servers prepare content for distribution, store and distribute content, manage licenses and domains, and meter content usage. PlayReady servers can be on-premises or located in the cloud.

Playready server receives the content request and then encrypt the ordered data having KeyID.

SOURCE: http://download.microsoft.com/download/8/3/C/83C936E9-0EF5-4528-885E-DCDD3172811A/MicrosoftPlayReadyContentProtectionWhitePaper_March2015.pdf

Next, the content is delivered to the client (for example, the client has begun downloading part of the data stream that makes up the content). The client then begins to parse this content and discovers that it is encrypted and uses a key that is unknown, but contains a KeyID.

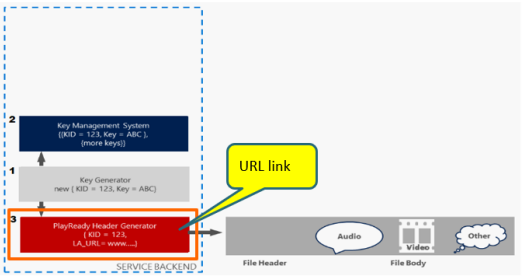
SOURCE: https://docs.microsoft.com/en-us/playready/overview/simple-end-to-end-system

the order server responding to the customer's order by sending the customer a URL link towards the delivery server, the URL link comprising, as a parameter, at least the unique identifier of the copy ordered;

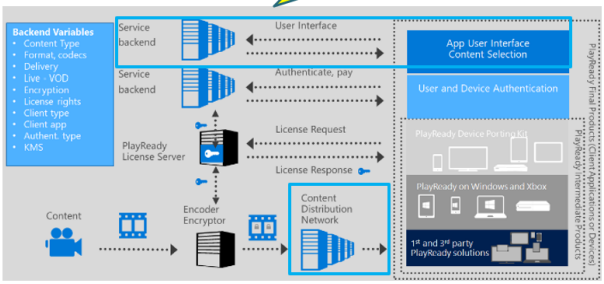
Next, the content is delivered to the client (for example, the client has begun downloading part of the data stream that makes up the content). The client then begins to parse this content and discovers that it is encrypted and uses a key that is unknown, but contains a KeyID.

SOURCE: https://docs.microsoft.com/en-us/playready/overview/simple-end-to-end-system

When the user request a file from the order server it provides customer a link to file which contains the encrypted key.

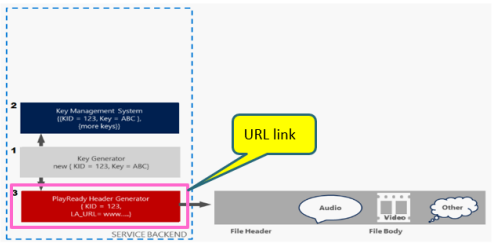


SOURCE: https://docs.microsoft.com/en-us/playready/overview/simple-end-to-end-system



SOURCE: https://docs.microsoft.com/en-us/playready/overview/simple-end-to-end-system

responsive to an activation of the URL link by the customer, the delivery server generating a specific copy of the work ordered, by a library used for creation of documents on the fly containing the unique identifier, a supervision agent for the document, and the other permanently acquired digital rights relating to the document, the supervision agent designed to verify the controlled digital rights of each copy of the ordered work;



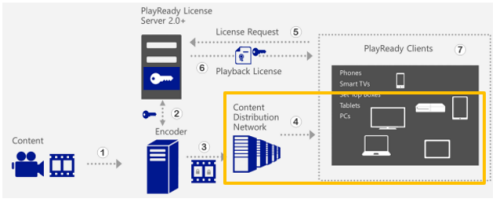
SOURCE: https://docs.microsoft.com/en-us/playready/overview/simple-end-to-end-system

On-the-fly PlayReady encryption using key files

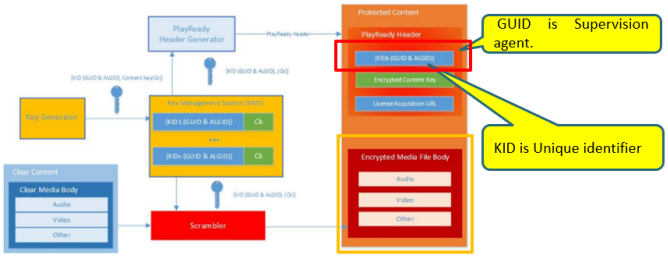
VOD and live content can be PlayReady encrypted on-the-fly using key files. When using this option, you'll need to provide your own PlayReady key server. Key files are text files that are located in the ***[install-dir]*/keys** folder that match the stream name of the stream you're playing with the addition of a **.key** extension. For example, if you're interested in protecting the live stream **myStream**, then you create a key file with the following path:

```
[install-dir]/keys/myStream.key
```

SOURCE: https://www.wowza.com/docs/how-to-secure-smooth-streaming-using-playready-drm-silverlight#on-the-fly-playready-encryption-using-key-files



SOURCE: http://download.microsoft.com/download/8/3/C/83C936E9-0EF5-4528-885E-DCDD3172811A/MicrosoftPlayReadyContentProtectionWhitePaper_March2015.pdf



SOURCE: https://docs.microsoft.com/en-us/playready/overview/key-and-key-ids-kids

Secure audio/video content against unauthorized use, and help monetize content

Microsoft PlayReady content access and protection technology is a set of technologies that can be used to distribute audio/video content more securely over a network, and help prevent the unauthorized use of this content. This technology is used for defining, incorporating, and enforcing rights for digital media. The service provider and content provider can control the expiration date, the number of times a user can play the content file, the resolution of the content that can be played on a screen, the type of screen that content is rendered to, and many other control settings. PlayReady technologies can be incorporated into media applications on televisions, set top boxes, mobile phones, tablets, personal computers, and other devices to enforce the content access rules defined by the content owners.

SOURCE: https://docs.microsoft.com/en-us/playready

accessing a control server via the network, the control server configured to verify digital rights acquired by the customer using the unique identifier of the ordered document copy;

Content and license flow

In PlayReady systems, a content packaging service encrypts content and stores it on a Web Server. Clients acquire this encrypted content through streaming or download. Clients also acquire a PlayReady license from a License Server, which contains the information needed to decrypt content for rendering.

Playready verifies digital rights using the encrypted keys, file if the verification is successful.

SOURCE: https://docs.microsoft.com/en-us/playready/overview/ecosystem

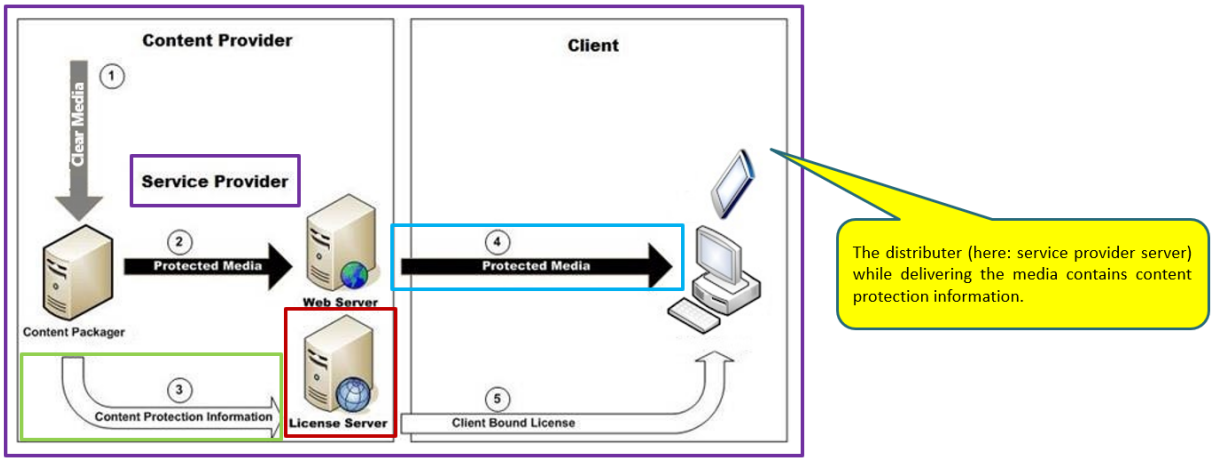
To decrypt content, a PlayReady client sends a license request to a PlayReady license server.
The PlayReady license server authenticates the client and issues a license back to the client. As the client uses the license key to unencrypt the content, it plays back the content according to the policies specified in the license. Some of the common policies utilized are time based restrictions and output protections (for example, restricting playback to a secure HDMI port to safeguard against copying).

SOURCE: http://download.microsoft.com/download/8/3/C/83C936E9-0EF5-4528-885E-DCDD3172811A/MicrosoftPlayReadyContentProtectionWhitePaper_March2015.pdf

One media file is encrypted using multiple keys. For example, the video track is encrypted using Key1, and the audio track is encrypted using Key2. When a client requests a license for KID1, the License Server issues a license response including licenses for KID1 and KID2, so the client has all the keys to decrypt the video and audio tracks of the file.

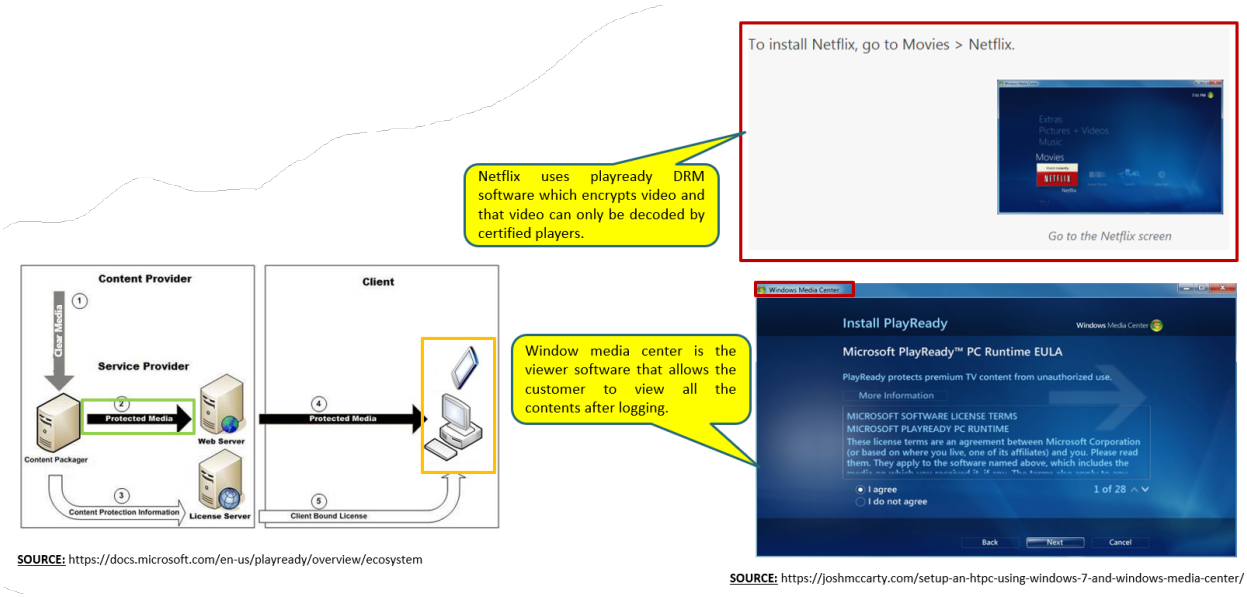
SOURCE: https://docs.microsoft.com/en-us/playready/overview/key-and-key-ids-kids

when delivering the ordered document copy to the customer, the delivery server sending to the control server the controlled information containing at least the unique identifier of the ordered document copy and the set of digital rights controlled; and



SOURCE: https://docs.microsoft.com/en-us/playready/overview/ecosystem

operating a customer computing device, supporting a viewer, to allow the customer, via the viewer, to consult the ordered document, previously downloaded from the delivery server, said viewer designed to allow the customer to consult the ordered document; and



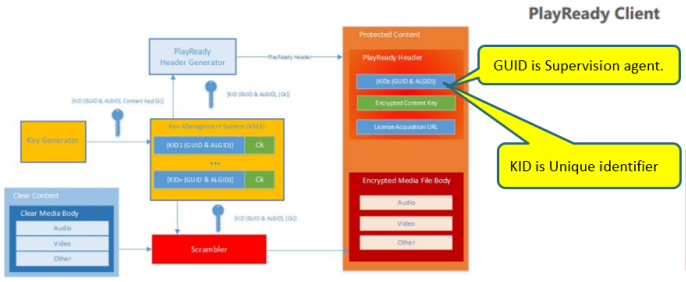
SOURCE: https://docs.microsoft.com/en-us/playready/overview/ecosystem

SOURCE: https://joshmccarty.com/setup-an-htpc-using-windows-7-and-windows-media-center/

a verification step comprising the sub-steps of when opening the specific copy on the customer computing device, the supervision agent of the specific copy causing the customer computing device to connect to the control server, and the supervision agent of the specific copy sending a query containing at least the unique identifier of the specific copy;

The part that interests us is the `<KIDS>` element, which contains one or more `<KID>` elements. A KID (Key ID) contains a globally unique identifier (GUID) that the client uses to ask the Server for a corresponding key, and an ALGID, which is then used to decrypt the file. The KID is public, since it's contained in the PRO, but the key itself is a secret to the service, and the relationship between key and KID is known only to the service.

SOURCE: https://docs.microsoft.com/en-us/playready/overview/key-and-key-ids-kids



SOURCE: https://docs.microsoft.com/en-us/playready/overview/key-and-key-ids-kids

Accesses the system and decrypts and plays content according to the policies specified in scalable root and leaf licenses. A scalable root license authorizes the client to access the overall service and specifies policies for a user's account, such as region, channel subscriptions, and time-based policies. Scalable leaf licenses are delivered in stream and allow the client to decrypt and play specific streams.

Each time a client starts, it verifies that it has a valid scalable root license. If it doesn't, it requests a new one from the scalable root license service. After it has a valid scalable root license, the client uses a key in the scalable root license to decrypt and play content in individual streams according to policies.

SOURCE: http://download.microsoft.com/download/2/D/D/2DD6B4E8-CABF-4DE9-8F61-895BE8F1ED33/ProtectingLiveTVServicesWithPlayReady_March2015.pdf

in response to receiving the query, the control server returning a response comprised of one of i) an authorization to consult the specific copy, and ii) a consultation refusal, according to the specific copy's controlled digital rights as stored by the control server, and

Refusal according to DRM

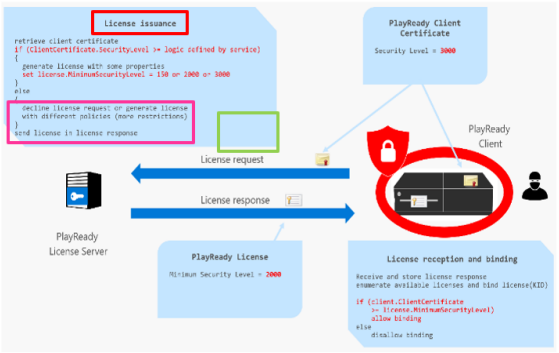
"Whoops, something went wrong... Digital Rights Management (DRM) Error. We're sorry, but there is a problem playing protected (DRM) content. The date on your computer is set to 12/17/2012, which may be incorrect. Please correct the date on your computer and try again."

SOURCE: https://www.technipages.com/fix-netflix-drm-error-n8156-6013

Today's agreement, which makes Microsoft PlayReady the primary content protection technology for Netflix partner devices and applications, underscores the benefits of PlayReady as a flexible, reliable and scalable content protection technology. Netflix already deploys PlayReady to enable all instant streaming scenarios on Windows-based PCs and Macs. The company expects the first Netflix ready devices beyond computers to incorporate Microsoft PlayReady as early as this summer. The Netflix ready device program, which launched in 2007, already has dozens of devices on the market that use Windows Media DRM.

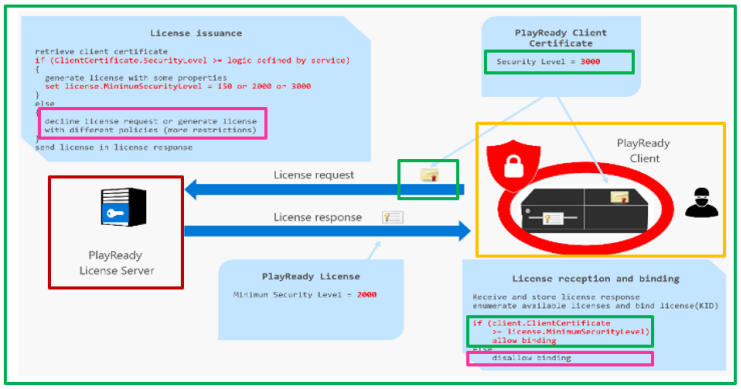
SOURCE: https://media.netflix.com/en/press-releases/netflix-taps-microsoft-playready-as-its-primary-drm-technology-for-netflix-ready-devices-and-applications-migration-1

- In addition, every license delivered includes a property called MinimumSecurityLevel, which is set to 150, 2000, or 3000 by the License Server. A License Server delivering a license to a client sets this value in the license. Clients binding a license verify if their own Client Security Level is equal or greater than the MinimumSecurityLevel value of the license. If it isn't, they refuse to bind and play.

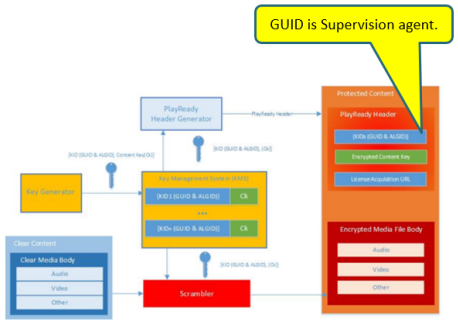


SOURCE: https://docs.microsoft.com/en-us/playready/overview/security-level

when the customer computing device receives the response from the control server, the supervision agent of the specific copy allowing the consultation of the specific copy when the response comprises the authorization to consult the specific copy and prohibiting the consultation of the specific copy when the response comprises the consultation refusal.



SOURCE: https://docs.microsoft.com/en-us/playready/overview/security-level



SOURCE: https://docs.microsoft.com/en-us/playready/overview/key-and-key-ids-kids

26. Defendant's aforesaid activities have been without authority and/or license from Plaintiff.

27. To the extent any marking was required by 35 U.S.C. § 287, Plaintiff and all predecessors in interest to the '143 patent complied with all marking requirements under 35 U.S.C. § 287.

28. Plaintiff is entitled to recover from Defendant the damages sustained by Plaintiff as a result of the Defendant's wrongful acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

Plaintiff hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

Plaintiff respectfully requests that the Court find in its favor and against the Defendant, and that the Court grant Plaintiff the following relief:

A. a judgment that Defendant directly and/or indirectly infringes one or more claims of the '143 patent;

B. award Plaintiff damages in an amount adequate to compensate Plaintiff for Defendant's infringing products' infringement of the claims of the '143 patent, but in no event less than a reasonable royalty, and supplemental damages for any continuing post-verdict infringement until entry of the final judgment with an accounting as needed, under 35 U.S.C. § 284;

C. award Plaintiff pre-judgment interest and post-judgment interest on the damages awarded, including pre-judgment interest, pursuant to 35 U.S.C. § 284, from the date of each act of infringement of the '143 patent by Defendant to the day a damages judgment is entered, and an award of post-judgment interest, pursuant to 28 U.S.C. § 1961, continuing until such judgment is paid, at the maximum rate allowed by law; and an accounting of all damages not presented at trial;

D. a judgment and order finding this to be an exceptional case and requiring defendant to pay the costs of this action (including all disbursements) and attorneys' fees, pursuant to 35 U.S.C. § 285;

E. award a compulsory future royalty for the '143 patent; and award such further relief as the Courts deems just and proper.

Dated: April 9, 2019

STAMOULIS & WEINBLATT LLC

/s/ Stamatios Stamoulis

Stamatios Stamoulis (#4606)
Richard C. Weinblatt (#5080)
800 N. West Street, Third Floor
Wilmington, DE 19801
(302) 999-1540
stamoulis@swdelaw.com
weinblatt@swdelaw.com

Austin Hansley (*pro hac vice* application forthcoming)
Texas Bar No.: 24073081
HANSLEY LAW FIRM, PLLC
13355 Noel Rd., STE. 1100
Dallas, Texas 75240
(972) 528-9321 Ext. 1000
ahansley@hansleyfirm.com

Attorneys for Plaintiff
DRM Vectors, LLC