M. ELIZABETH DAY (SBN 177125)
eday@feinday.com
DAVID ALBERTI (SBN 220265)
dalberti@feinday.com
SAL LIM (SBN 211836)
slim@feinday.com
MARC BELLOLI (SBN 244290)
mbelloli@feinday.com
FEINBERG DAY ALBERTI LIM & BELLOLI LLP
1600 El Camino Real, Suite 280
Menlo Park, CA 94025
Tel: 650.618.4360
Fax: 650.618.4368

Attorneys for Uniloc 2017 LLC

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

UNILOC 2017 LLC Plaintiff, v. MICROSOFT CORPORATION, Defendant.	CASE NO. 8:19-cv-00158 **COMPLAINT FOR PATENT INFRINGEMENT** **DEMAND FOR JURY TRIAL**

Plaintiff Uniloc 2017 LLC ("Uniloc"), by and through the undersigned counsel, hereby files this Complaint and makes the following allegations of patent infringement relating to U.S. Patent No. 9,311,485 against Defendant Microsoft Corporation ("Microsoft"), and alleges as follows upon actual knowledge with respect to itself and its own acts and upon information and belief as to all other matters:

NATURE OF THE ACTION

1. This is an action for patent infringement. Uniloc alleges that Microsoft infringes U.S. Patent No. 9,311,485 (the "'485 patent"), a copy of which is attached hereto as Exhibit A.

2. Uniloc alleges that Microsoft directly and indirectly infringes the '485 patent by making, using, offering for sale and selling devices that practice a method for determining the trustworthiness of remotely located devices, such as Microsoft PlayReady. Uniloc alleges that Microsoft also induces and contributes to the infringement of others. Uniloc seeks damages and other relief for Microsoft's infringement of the '485 patent.

THE PARTIES

3. Uniloc 2017 LLC is a Delaware corporation having places of business at 1209 Orange Street, Wilmington, Delaware 19801 and 620 Newport Center Drive, Newport Beach, California 92660.

4. Uniloc holds all substantial rights, title and interest in and to the '485 patent.

5. Upon information and belief, Defendant Microsoft is a corporation organized and existing under the laws of the State of Washington, with the following places of business in this District: 3 Park Plaza, Suite 1600, Irvine, CA 92614; 3333 Bristol Street, Suite 1249, Costa Mesa, CA 92626; 578 The Shops at Mission Viejo, Mission Viejo, CA 92691; 331 Los Cerritos Center, Cerritos, CA 90703; 13031 West Jefferson Blvd., Suite 200, Los Angeles, CA 90094; 2140

Glendale Galleria, JCPenney Court, Glendale, CA 91210; 10250 Santa Monica Blvd., Space #1045, Los Angeles, CA 90067; 6600 Topanga Canyon Blvd, Canoga Park, CA 91303. Microsoft can be served with process by serving its registered agent for service of process in California: Corporation Service Company which Will Do Business in California as CSC - Lawyers Incorporating Service, 2710 Gateway Oaks Dr., Ste. 150, Sacramento, CA 95833.

JURISDICTION AND VENUE

6. This action for patent infringement arises under the Patent Laws of the United States, 35 U.S.C. § 1 et. seq. This Court has original jurisdiction under 28 U.S.C. §§ 1331 and 1338.

7. This Court has both general and specific jurisdiction over Microsoft because Microsoft has committed acts within the Central District of California giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Microsoft would not offend traditional notions of fair play and substantial justice. Defendant Microsoft, directly and through subsidiaries, intermediaries (including distributors, retailers, franchisees and others), has committed and continues to commit acts of patent infringement in this District, by, among other things, making, using, testing, selling, licensing, importing and/or offering for sale/license products and services that infringe the '485 patent.

8. Venue is proper in this district and division under 28 U.S.C. §§ 1391(b)-(d) and 1400(b) because Microsoft has committed acts of infringement in the Central District of California and has a regular and established place of business in the Central District of California.

COUNT I– INFRINGEMENT OF U.S. PATENT NO. 9,311,485

9. The allegations of paragraphs 1-8 of this Complaint are incorporated by reference as though fully set forth herein.

10. The '485 patent titled, "Device Reputation Management," issued on

April 12, 2016. A copy of the '485 patent is attached as Exhibit A.

11. Pursuant to 35 U.S.C. § 282, the '485 patent is presumed valid.

12. Microsoft makes, uses, offers for sale, and sells in the United States and imports into the United States electronic devices that practice a method for determining the trustworthiness of a remotely located device, including but not limited to Microsoft PlayReady (collectively the "Accused Infringing Devices").

13. Upon information and belief, the Accused Infringing Devices infringe claim 1 of the '485 patent by practicing a method in the exemplary manner described below.

14. The Accused Infringing Devices provide a method for determining the trustworthiness of a remotely located device.

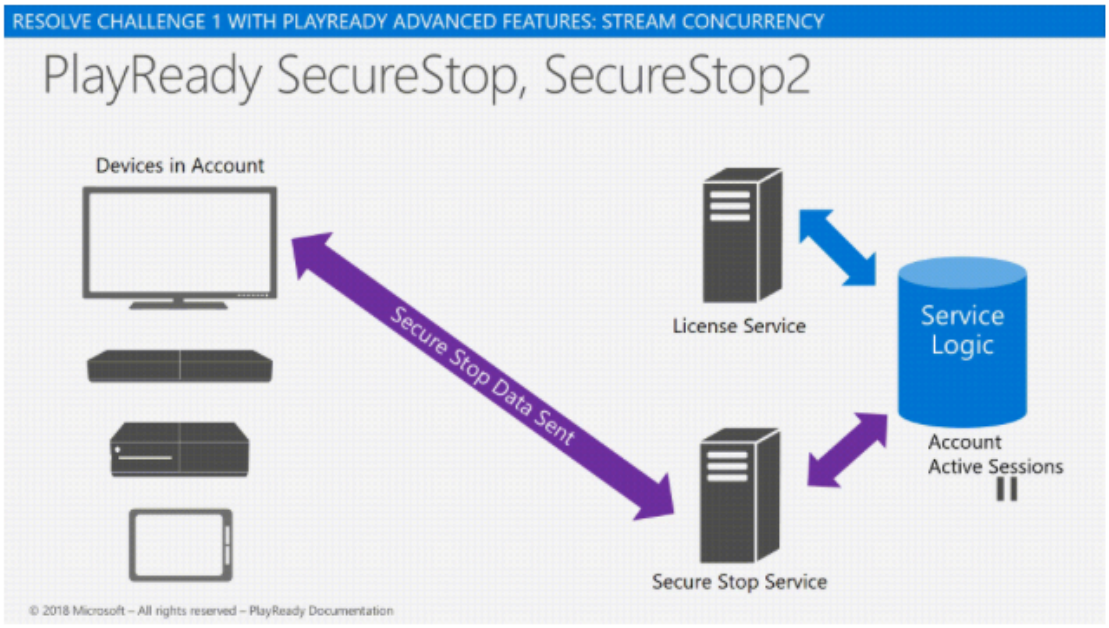
Microsoft PlayReady

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/, last accessed on Dec. 12, 2018

15. The Accused Infringing Devices' servers, such as the Secure Stop Server, receive data representing one or more attacks by one or more perpetrating devices, for example, in the form of malicious Secure Stop messages (e.g., SecureStop2 messages) from the PlayReady clients.



There are two primary scenarios for sending a Secure Stop challenge:

- When the media playback stops either at the end, or because the user stopped the media presentation somewhere in the middle.
- When the previous session ends unexpectedly (for example, due to a system or app crash). The app will need to query, either at startup or shutdown, for any outstanding Secure Stop sessions and send challenge(s) separate from any other media playback.

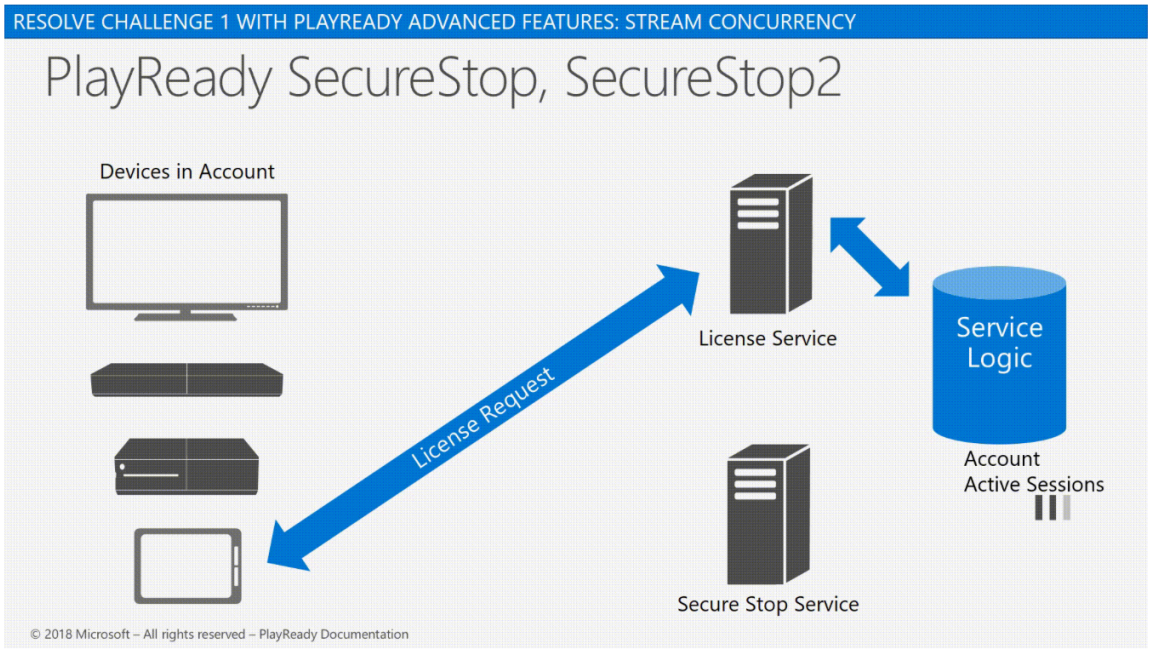
Source: https://docs.microsoft.com/en-us/playready/features/secure-stop-pk, last accessed on Dec. 10, 2018.

The following table shows the Server App logic on different Client Security Level and Secure Stop versions.

Client Version	SecureStop Server Logic	Robustness
PlayReady version 2.0+ SL2000	Server does not receive any SecureStop message from the client. Use app logic to do this.	Low
PlayReady version 3.0+ SL3000 (Example: Windows 10 App)	Server receives a SecureStop1 message from the client. The robustness of this message against attacks is higher than simple app logic.	Medium
PlayReady version 4.2+ SL3000	Server receives a SecureStop2 message from the client. A malicious SecureStop2 message from this client would require an attack in the client's Trusted Execution Environment (TEE). The robustness of this message against attacks is higher than SecureStop1.	High

Source: https://docs.microsoft.com/en-us/playready/features/secure-stop-pk, last accessed on Dec. 10, 2018.

16. The Accused Infringing Devices' server receives a License Request from the subject device through a computer network. The license request can be issued, declined or a license with different policies (more restrictions) can be issued, reflecting on the reputation of the subject device.

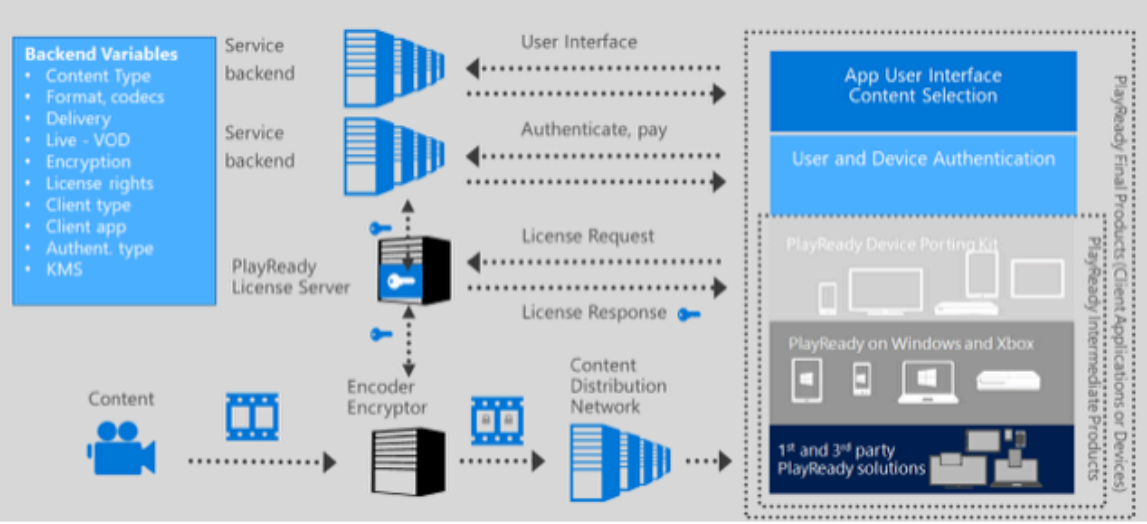


Source: https://docs.microsoft.com/en-us/playready/features/secure-stop-pk, last accessed on Jan. 7, 2019.

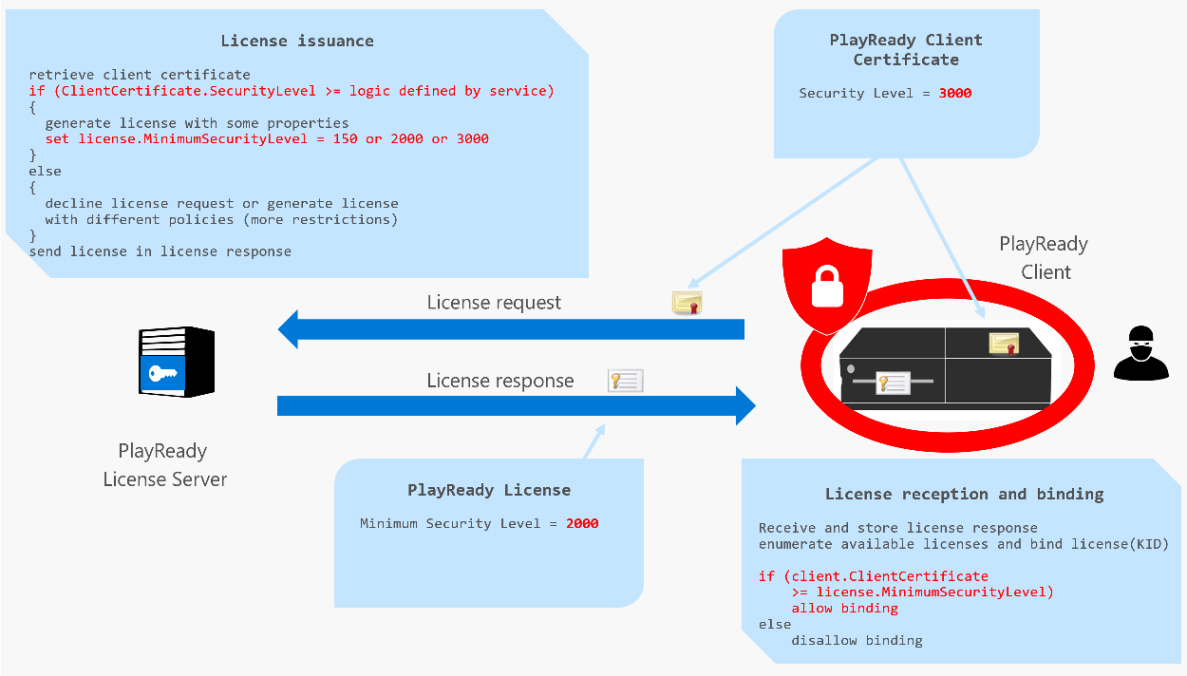
Each license contains rights and restrictions, defining exactly how the content may be used and under what conditions. For example, a music file license may enable a "right to play" but restrict the security level of the application on which the content can be played. The license might be valid for the period between October 1, 2017 and November 1, 2017. There may be multiple licenses for a single file. A user will be able to access and use his or her content so long as one of the licenses grants the appropriate rights and the restrictions do not prevent access.

Overview of an End-to-End Video Service

The following illustration contains a high-level look at an end-to-end video service, including the back end of the service on the left and clients on the right.

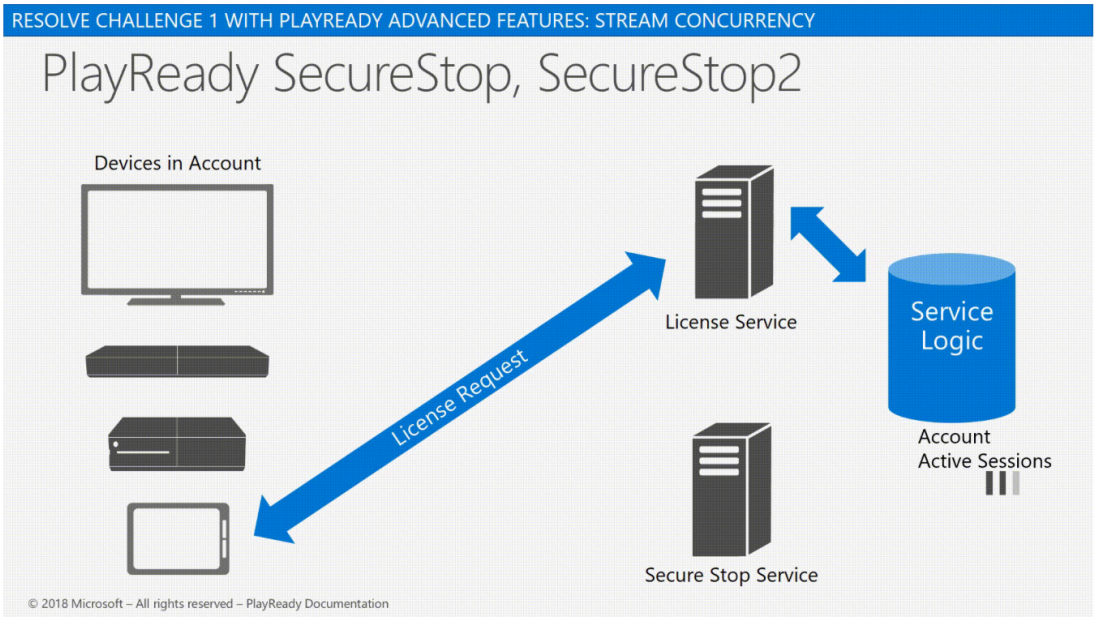


Source: https://docs.microsoft.com/en-us/playready/overview/simple-end-to-end-system, last accessed on Dec. 10, 2018.



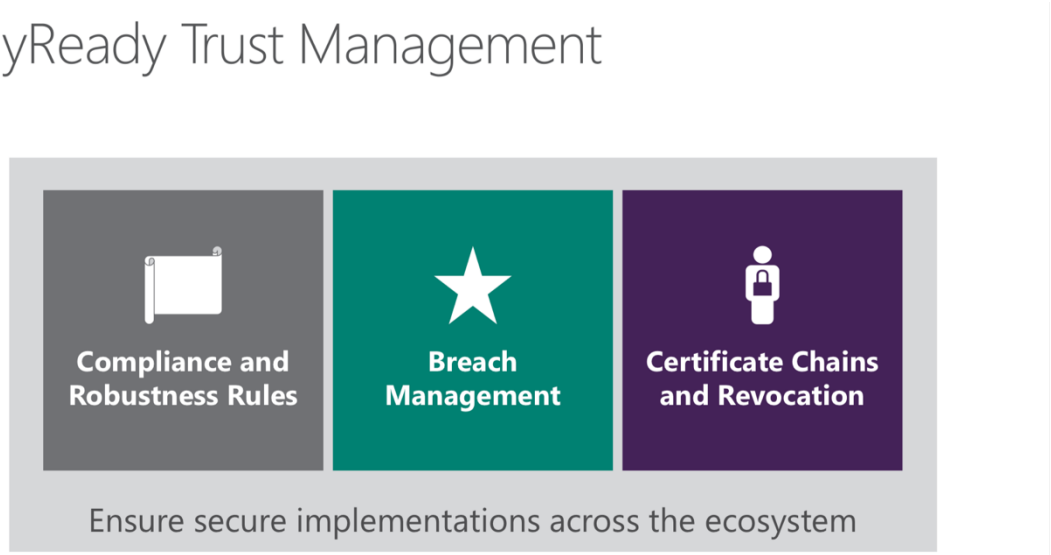
Source: https://docs.microsoft.com/en-us/playready/overview/security-level, last accessed on Dec. 12, 2018.

17. The Service Logic receives a request from a reputation of the subject device from the Accused Infringing Devices' server through a computer network.



Source: https://docs.microsoft.com/en-us/playready/features/secure-stop-pk, last accessed on Jan. 7, 2019.

18. The Accused Infringing Devices conduct a trust management at the Service Logic to "ensure implementations across the ecosystem."



Source: https://ecfsapi.fcc.gov/file/60001078239.pdf, last accessed on Dec. 12, 2018.

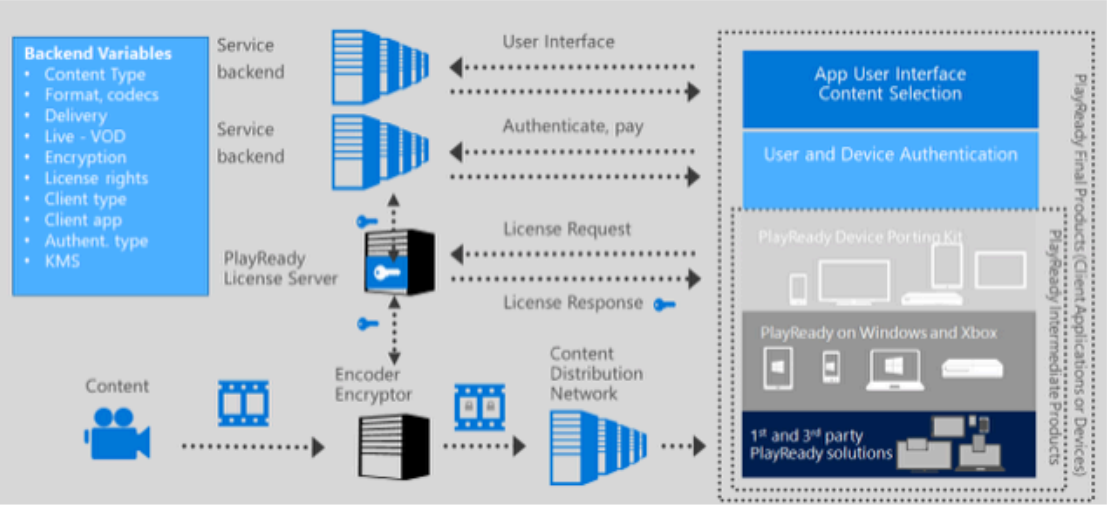
Source: https://ecfsapi.fcc.gov/file/60001078239.pdf, last accessed on Dec. 12, 2018.

19. After the Accused Infringing Devices' server and the Service Logic receive a license request through a computer network, the Accused Infringing Devices' server and the Service Logic determine whether the subject device is one of the perpetrating devices, which can result in the license request being issued, declined or a license with different policies (more restrictions) being issued.

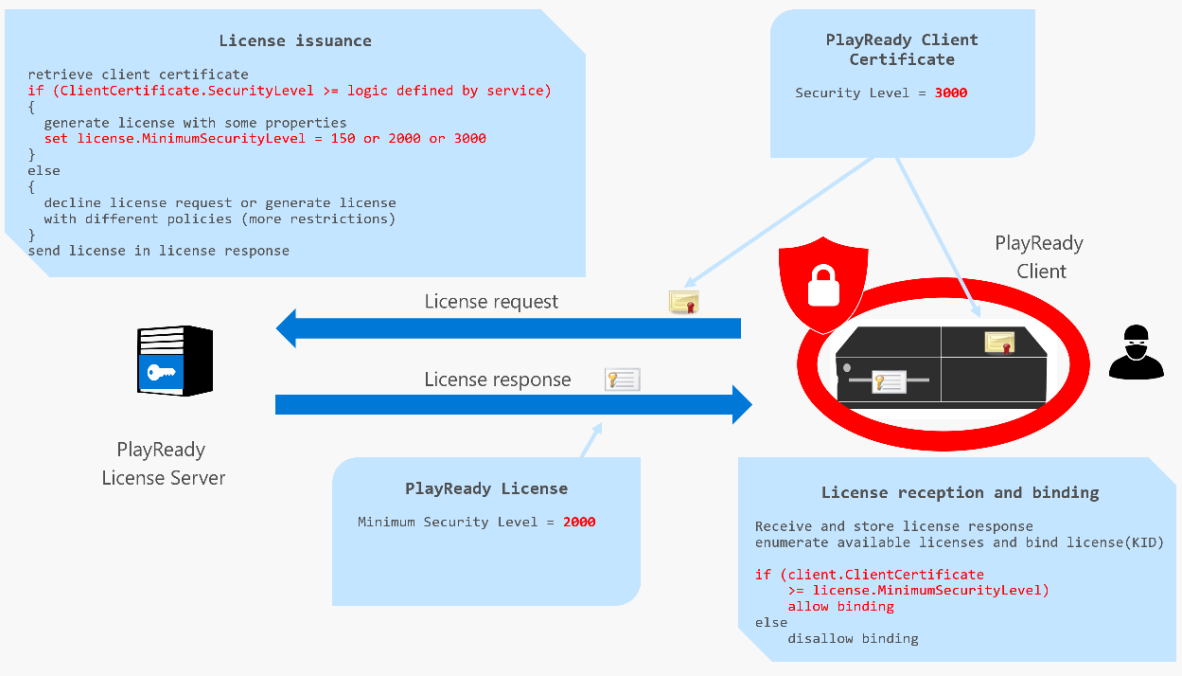
Each license contains rights and restrictions, defining exactly how the content may be used and under what conditions. For example, a music file license may enable a "right to play" but restrict the security level of the application on which the content can be played. The license might be valid for the period between October 1, 2017 and November 1, 2017. There may be multiple licenses for a single file. A user will be able to access and use his or her content so long as one of the licenses grants the appropriate rights and the restrictions do not prevent access.

Overview of an End-to-End Video Service

The following illustration contains a high-level look at an end-to-end video service, including the back end of the service on the left and clients on the right.



Source: https://docs.microsoft.com/en-us/playready/overview/simple-end-to-end-system, last accessed on Dec. 10, 2018.

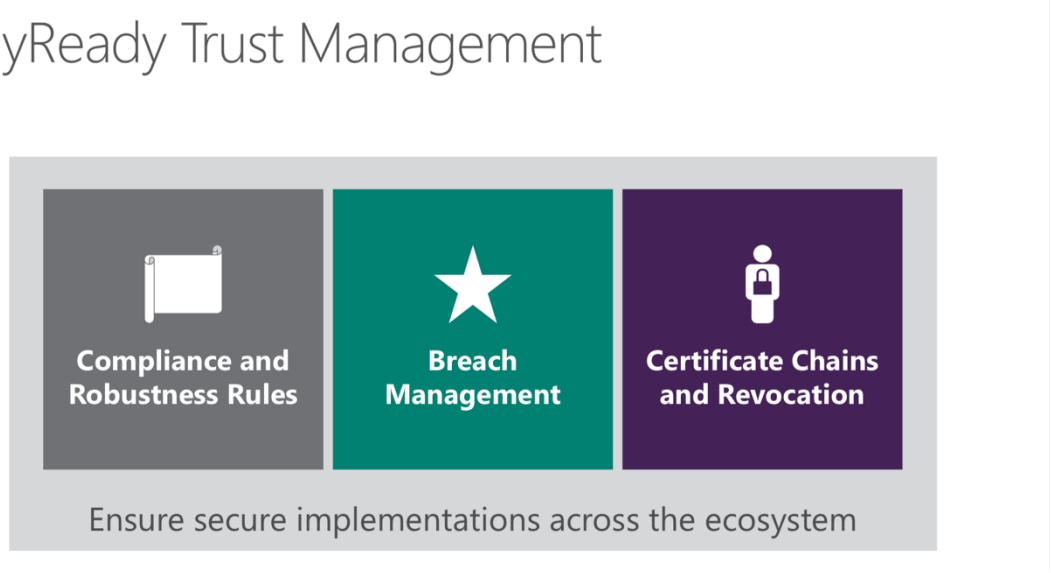


Source: https://docs.microsoft.com/en-us/playready/overview/security-level, last accessed on Dec. 12, 2018.

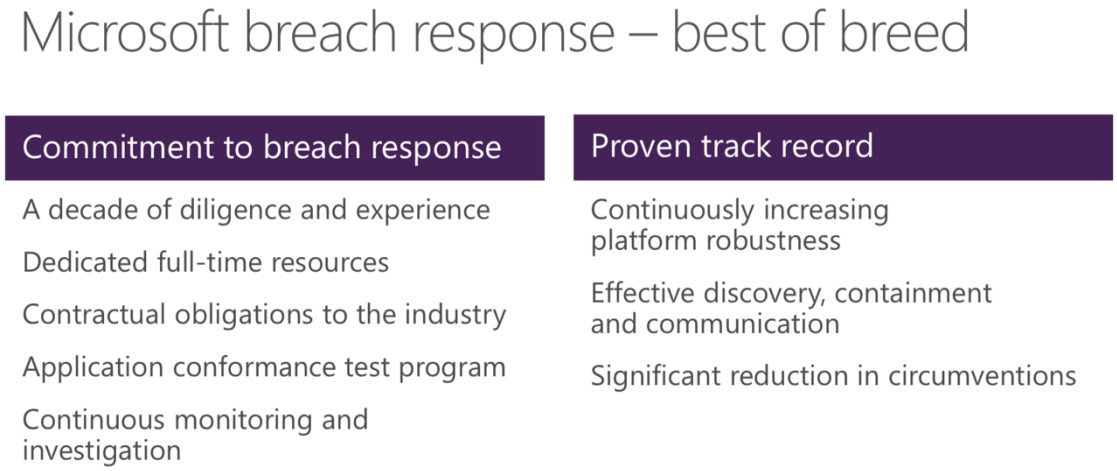
20. The perpetrating devices are also determined through the Accused Infringing Devices' trust management. As a result of this determination, as stated in Microsoft software license terms, "Microsoft may decide to revoke the software's ability to consume PlayReady-protected content for reasons including but not limited to (i) if a breach or potential breach of PlayReady technology occurs. . .."

9. **PlayReady Support.** The software may include the Windows Emulator, which contains Microsoft's PlayReady content access technology. Content owners use Microsoft PlayReady content access technology to protect their intellectual property, including copyrighted content. This software uses PlayReady technology to access PlayReady-protected content and/or WMDRM-protected content. Microsoft may decide to revoke the software's ability to consume PlayReady-protected content for reasons including but not limited to (i) if a breach or potential breach of PlayReady technology occurs, (ii) proactive robustness enhancement, and (iii) if Content owners require the revocation because the software fails to properly enforce restrictions on content usage. Revocation should not affect unprotected content or content protected by other content access technologies. Content owners may require you to upgrade PlayReady to access their content. If you decline an upgrade, you will not be able to access content that requires the upgrade and may not be able to install other operating system updates or upgrades.

Source: https://developer.microsoft.com/en-us/windows/hardware/license-terms-enterprise-wdk, last accessed on Dec. 11, 2018.



Source: https://ecfsapi.fcc.gov/file/60001078239.pdf, last accessed on Dec. 12, 2018.



Source: https://ecfsapi.fcc.gov/file/60001078239.pdf, last accessed on Dec. 12, 2018.

21. After a perpetrating device is identified, the Accused Infringing Devices may revoke the perpetrating device's license and add the perpetrating device to a license revocation list.

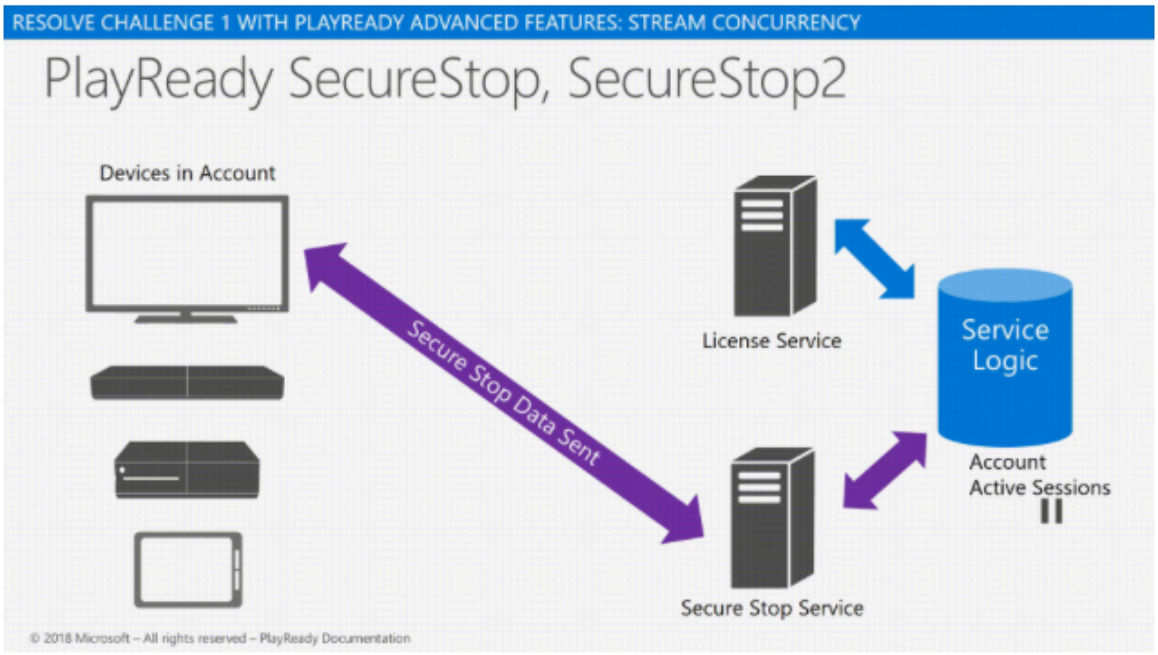
What is PlayReady Revocation

Revocation is a process to identify clients that have compromised security, and prevent those clients from getting access to additional licenses for decrypting content that has been protected.

When Microsoft identifies a client with compromised security, the device may be revoked and added to a revocation list. The revocation list is periodically downloaded by the License Servers that issue licenses for protected content. License Servers use this revocation list to deny licenses to devices that have been revoked, thereby preventing the device from playing newly protected content.

Source: https://docs.microsoft.com/en-us/playready/overview/revocation, last accessed on Dec. 12th, 2018.

22. The Accused Infringing Devices' server that runs the Service Logic retrieves data representing one or more attacks by one or more perpetrating devices in the form of malicious Secure Stop (e.g., SecureStop2) messages, from the Secure Stop Service server.



There are two primary scenarios for sending a Secure Stop challenge:

- When the media playback stops either at the end, or because the user stopped the media presentation somewhere in the middle.
- When the previous session ends unexpectedly (for example, due to a system or app crash). The app will need to query, either at startup or shutdown, for any outstanding Secure Stop sessions and send challenge(s) separate from any other media playback.

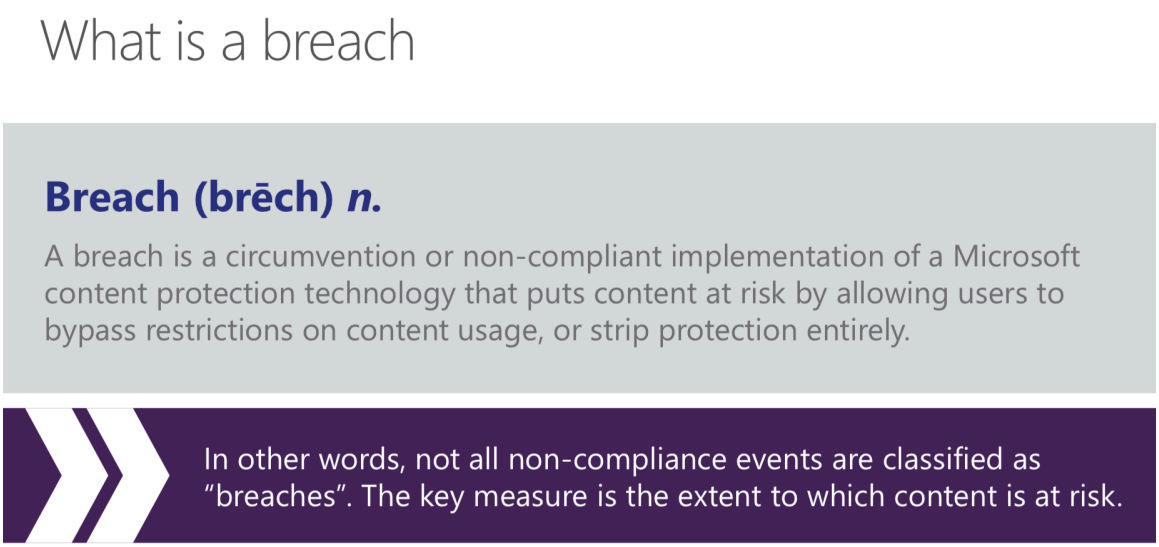
Source: https://docs.microsoft.com/en-us/playready/features/secure-stop-pk, last accessed on Dec. 10, 2018.

The following table shows the Server App logic on different Client Security Level and Secure Stop versions.

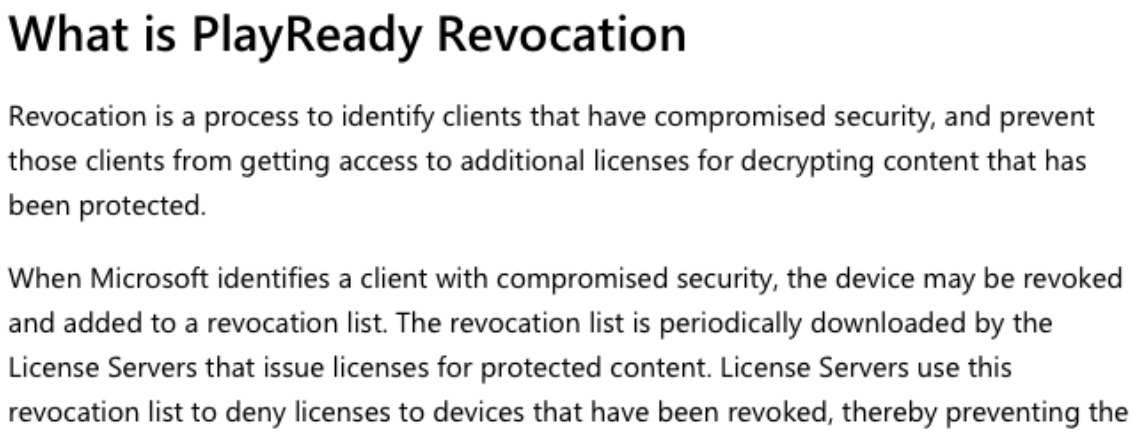
Client Version	SecureStop Server Logic	Robustness
PlayReady version 2.0+ SL2000	Server does not receive any SecureStop message from the client. Use app logic to do this.	Low
PlayReady version 3.0+ SL3000 (Example: Windows 10 App)	Server receives a SecureStop1 message from the client. The robustness of this message against attacks is higher than simple app logic.	Medium
PlayReady version 4.2+ SL3000	Server receives a SecureStop2 message from the client. A malicious SecureStop2 message from this client would require an attack in the client's Trusted Execution Environment (TEE). The robustness of this message against attacks is higher than SecureStop1.	High

Source: https://docs.microsoft.com/en-us/playready/features/secure-stop-pk, last accessed on Dec. 10, 2018.

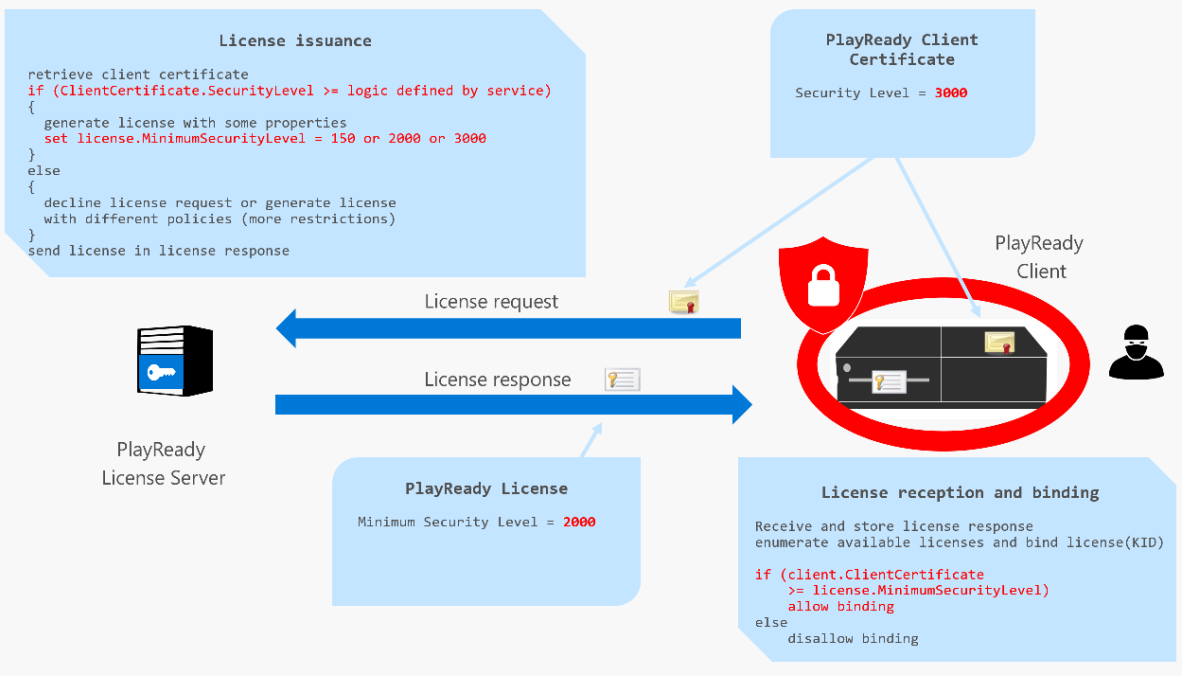
23. The Accused Infringing Devices conduct trust management to continuously monitor the frequency and severity of the attacks from the subject devices and decide if breaches occur. The Accused Infringing Devices measure quantifiably the trustworthiness of the subject devices to decide if a breach has occurred, if the license from the device should or should not be revoked, and/or if a one-time license should be issued, declined or a one-time license with different policies (with more restrictions) can be issued. An exemplary quantifiable measure is "the extent to which content is at risk."



Source: https://ecfsapi.fcc.gov/file/60001078239.pdf, last accessed on Dec. 12, 2018.



Source: https://docs.microsoft.com/en-us/playready/overview/revocation, last accessed on Dec. 12th, 2018.



Source: https://docs.microsoft.com/en-us/playready/overview/security-level, last accessed on Dec. 12, 2018.

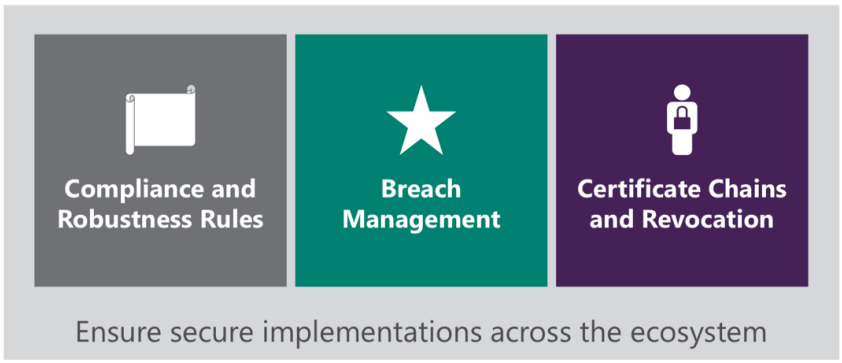
24. Another exemplary quantifiable measure of trustworthiness of the subject device is the robustness of the SecureStop messages. The Accused Infringing Devices also determine the type of malicious SecureStop message, e.g., SecureStop, SecureStop 1 or SecureStop 2, which are quantifiably different. When the malicious SecureStop2 messages or the malicious SecureStop1 messages are received at the Accused Infringing Devices' servers, the "high" and "medium" robustness level represents the severity of the penetration at the subject device.

The following table shows the Server App logic on different Client Security Level and Secure Stop versions.

Client Version	SecureStop Server Logic	Robustness
PlayReady version 2.0+ SL2000	Server does not receive any SecureStop message from the client. Use app logic to do this.	Low
PlayReady version 3.0+ SL3000 (Example: Windows 10 App)	Server receives a SecureStop1 message from the client. The robustness of this message against attacks is higher than simple app logic.	Medium
PlayReady version 4.2+ SL3000	Server receives a SecureStop2 message from the client. A malicious SecureStop2 message from this client would require an attack in the client's Trusted Execution Environment (TEE). The robustness of this message against attacks is higher than SecureStop1.	High

Source: https://docs.microsoft.com/en-us/playready/features/secure-stop-pk, last accessed on Dec. 10, 2018.

25. Data representing the measure of trustworthiness of the subject device is sent between the Accused Infringing Devices' servers across the ecosystem and from the the Accused Infringing Devices' License Server back to the subject device. The full license is granted, partially granted, or declined based on the measure of trustworthiness.

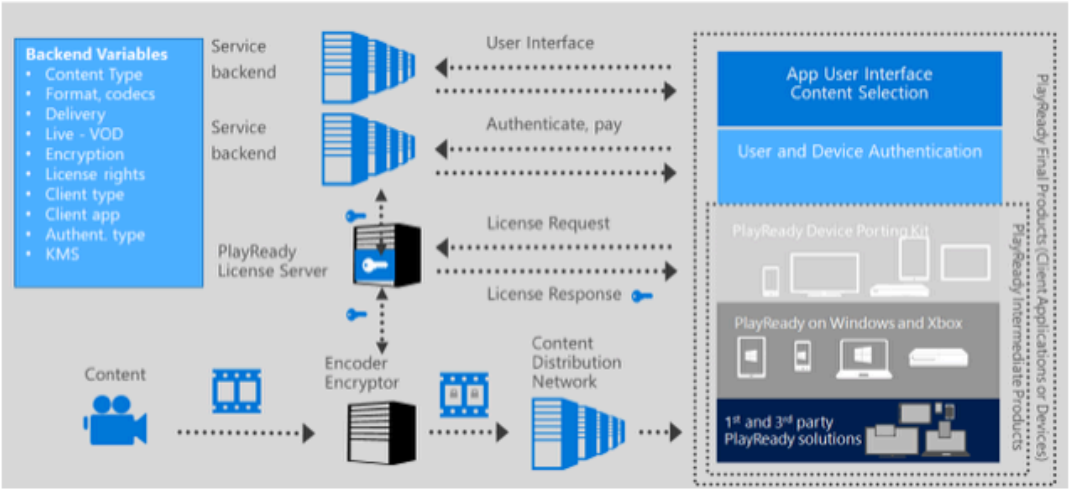


Source: https://ecfsapi.fcc.gov/file/60001078239.pdf, last accessed on Dec. 12, 2018.

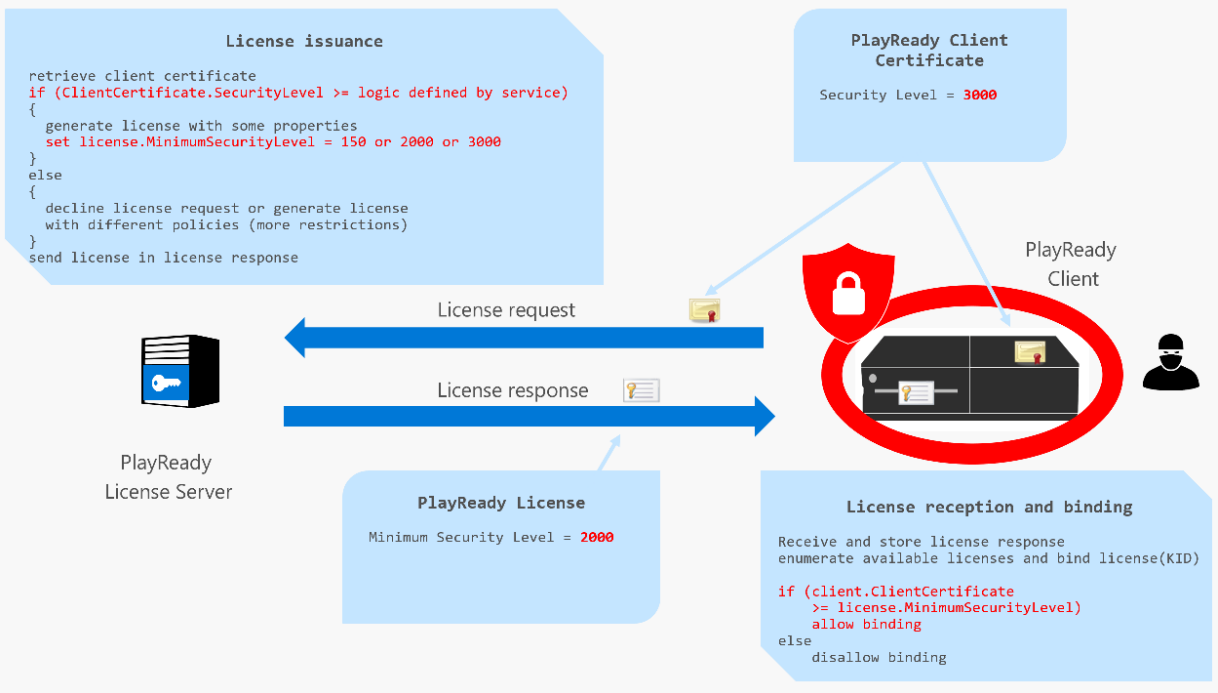
Each license contains rights and restrictions, defining exactly how the content may be used and under what conditions. For example, a music file license may enable a "right to play" but restrict the security level of the application on which the content can be played. The license might be valid for the period between October 1, 2017 and November 1, 2017. There may be multiple licenses for a single file. A user will be able to access and use his or her content so long as one of the licenses grants the appropriate rights and the restrictions do not prevent access.

Overview of an End-to-End Video Service

The following illustration contains a high-level look at an end-to-end video service, including the back end of the service on the left and clients on the right.



Source: https://docs.microsoft.com/en-us/playready/overview/simple-end-to-end-system, last accessed on Dec. 10, 2018.



Source: https://docs.microsoft.com/en-us/playready/overview/security-level, last accessed on Dec. 12, 2018.

26. Microsoft has infringed, and continues to infringe, at least claim 1 of the '485 patent in the United States, by making, using, offering for sale, selling and/or importing the Accused Infringing Devices in violation of 35 U.S.C. § 271(a).

27. Microsoft has also infringed, and continues to infringe, at least claim 1 of the '485 patent by actively inducing others to use, offer for sale, and sell the Accused Infringing Devices. Microsoft's users, customers, agents or other third parties who use those devices in accordance with Microsoft's instructions infringe claim 1 of the '485 patent, in violation of 35 U.S.C. § 271(a). Microsoft intentionally instructs its customers to infringe through training videos, demonstrations, brochures, installation and user guides, such as those located at: www.microsoft.com, support.microsoft.com, https://www.microsoft.com/playready/, https://docs.microsoft.com/en-us/playready/ and related domains and subdomains. Microsoft is thereby liable for infringement of the '485 patent under 35 U.S.C. § 271(b).

28. Microsoft has also infringed, and continues to infringe, at least claim 1 of the '485 patent by offering to commercially distribute, commercially distributing, or importing the Accused Infringing Devices which devices are used in practicing the processes, or using the systems, of the '485 patent, and constitute a material part of the invention. Microsoft knows portions of the Accused Infringing Devices to be especially made or especially adapted for use in infringement of the '485 patent, not a staple article, and not a commodity of commerce suitable for substantial noninfringing use. Microsoft is thereby liable for infringement of the '485 patent under 35 U.S.C. § 271(c).

29. Microsoft is on notice of its infringement of the '485 patent by virtue of a letter from Uniloc to Microsoft dated January ___, 2019. By the time of trial, Microsoft will have known and intended (since receiving such notice) that its continued actions would actively induce and contribute to the infringement of at least claim 1 of the '485 patent.

30. Upon information and belief, Microsoft may have infringed and continues to infringe the '485 patent through other software and devices utilizing the same or reasonably similar functionality, including other versions of the Accused Infringing Devices.

31. Microsoft's acts of direct and indirect infringement have caused and continue to cause damage to Uniloc and Uniloc is entitled to recover damages sustained as a result of Microsoft's wrongful acts in an amount subject to proof at trial.

PRAYER FOR RELIEF

WHEREFORE, plaintiff Uniloc 2017 LLC respectfully prays that the Court enter judgment in its favor and against Microsoft as follows:

a. A judgment that Microsoft has infringed one or more claims of the '485 patent literally and/or under the doctrine of equivalents directly and/or indirectly by inducing infringement and/or by contributory infringement;

b. That for each Asserted Patent this Court judges infringed by Microsoft this Court award Uniloc its damages pursuant to 35 U.S.C. § 284 and any royalties determined to be appropriate;

c. That this be determined to be an exceptional case under 35 U.S.C. § 285;

d. That this Court award Uniloc prejudgment and post-judgment interest on its damages;

e. That Uniloc be granted its reasonable attorneys' fees in this action;

f. That this Court award Uniloc its costs; and

g. That this Court award Uniloc such other and further relief as the Court deems proper.

DEMAND FOR JURY TRIAL

Uniloc hereby demands trial by jury on all issues so triable pursuant to Fed. R. Civ. P. 38.

Dated: January 28, 2019

FEINBERG DAY ALBERTI LIM & BELLOLI LLP

By: */s/ M. Elizabeth Day*
M. Elizabeth Day

Attorneys for Plaintiff
Uniloc 2017 LLC