Windows Server
Internet Information Services 7.0

Content Protection in Silverlight

Microsoft Corporation

April 2010

Microsoft

Contents

Introduction

With the explosive growth in online streaming video and rich Internet experiences, it is critical to ensure that your content and your business models are secure. The new peaks in online video audiences not only create a great opportunity to explore new revenue opportunities, but also expose the challenges in managing and protecting premium digital content offered across the Internet.

Microsoft® Silverlight™ not only enables you to offer a wide-range of digital content to your customers, but it also provides content protection that helps you ensure that users can only use your digital content as you intend.

What Is Content Protection?

Content protection is technology that enables you, as a digital content provider, to safeguard your online content from unauthorized use, copying, and dispersal. Content protection technologies enable you to identify users and to specify and enforce rights and restrictions for digital content, which enables you to securely distribute digital content. Such systems enforce your rules about how users can access and copy digital content files and may protect the content from being used in ways you have not authorized.

Why Should You Protect Online Content?

Regardless of the business model or distribution method that you use to offer premium media content to customers over the Internet, you want to protect those content investments. The primary reasons that you should consider protecting your online digital content are:

- You can ensure that users only access and use content in ways that you authorize.
- If you hold the copyright to digital content that you offer to users over the Internet, you can track usage for each authorized user and charge or report royalties for the content as appropriate.
- It can enable you to reliably monetize the content you provide by ensuring that users cannot skip advertisements.

Techniques for Protecting Online Content

A good content protection solution should be comprehensive; you must consider how to protect the content you provide over the Internet not only as it travels from server to client, but also after it reaches the client. Additionally, you should create a protection solution that enables you to provide content using the business models and distribution techniques that make sense for your organization.

There are many techniques that your organization can use to protect digital content that you make available to users over the Internet. You should consider using some combination of the following approaches to make sure your site and digital content are secure.

End-User Authentication and Authorization

To be able to protect your content at all, you must know who is accessing your digital content and set permissions to your content that reflects the rights you grant those individuals. Authentication is the process of obtaining a user's identity when they log on to your site, while authorization involves setting permissions on your content files, enabling you to restrict users' access to particular media resources.

For example, if your company operates a subscription-based online video service that enables users to watch movies or TV shows over the Internet, you can authentication and authorization to ensure that only users with active subscriptions can access watch the content. Authorization technologies enable you to deny access to digital resources as necessary – perhaps based on their subscription level in the example above.

Stream Encryption Using Secure Sockets Layer

Secure Sockets Layer (SSL) encryption, and its successor, Transport Layer Security (TLS), are protocols that you can use to protect your content as it travels from the server that hosts your content to the browsers that request it. When SSL or TLS is combined with HTTP, they are known as Hypertext Transfer Protocol Secure (HTTPS), which provides encryption support for the connection. Unauthorized users must decrypt the SSL connection in order to access your digital content.

It is important to note that SSL does not encrypt the digital content; it only encrypts the connection between your server and the browser that sends the request. It does not encrypt the source file, so the content on the server or on the client is not protected if SSL is the sole protection technique that you apply.

Stream Encryption Using RTMPE

A proprietary variation on SSL is Encrypted RTMP (RTMPE), which is used by Adobe Flash Media Server. RTMPE secures a media stream from the server to the requesting browser. Similar to SSL, stream encryption encrypts the connection between the server and the browser, but without requiring certificate management on the server. Like SSL, RTMPE does not encrypt the media files themselves, which means that after the content arrives at the client it is no longer protected. Only recent versions of the Flash player and Flash Media Server support the proprietary RTMPE protocol.

Full Digital Rights Management

Digital Rights Management (DRM) technologies enable you to specify and enforce rights on digital content and to enable secure distribution of that content. A DRM system enforces usage rules that you define and may protect digital content from being used in ways that you have not authorized. You can define usage rules that include expiration dates, how to license the content to the user, and more. DRM solutions attach rights and permissions to content files themselves, enabling you to enforce rules even after users have downloaded files to their computers.

Microsoft has been active in the DRM space for several years and its PlayReady® technology is widely accepted by premium content owners. Silverlight uses PlayReady technology as its native DRM system.

Output Protection

Premium content is usually encrypted to protect it from unauthorized duplication, and the content must be decrypted before it is rendered. After it is decrypted and uncompressed, the data must travel across a physical connector to the output device. Content providers may require the data to be protected at this point, as it travels across the physical connector.

Various protection mechanisms exist for this purpose, including High-Bandwidth Digital Content Protection (HDCP) and DisplayPort Content Protection (DPCP) for digital outputs, and Copy Generation Management System - Analog (CGMS-A) for analog outputs. Generally, these mechanisms involve encrypting or scrambling the signal before it travels to the display.

Microsoft Windows has technologies that enable a fine degree of control over content playback on various devices through a set of published APIs. This enables the content owner to be more or less restrictive depending on the capabilities of the display device.

How Silverlight Protects Online Content

Microsoft Silverlight supports four of the approaches described in the previous section:

- End-user authentication and authorization using ASP.NET Forms Authentication,
- SSL, which protects the files as they travel from the server to the requesting Silverlight client,
- DRM using PlayReady for both online and offline content[1],
- Output protection, which allows content to be securely transferred from the Silverlight application to display devices connected to the computer, based on policies set by the content owner.

End-User Authentication and Authorization

Silverlight applications can take advantage of ASP.NET Forms Authentication to check the identity of users who access content on your servers. In a typical Web-facing Silverlight application, when a user first visits your site, they register and create a user name and password. You store those credentials in a database. The Web server then sends a cookie that contains these credentials to the browser so that users do not have to log on each time they visit your site.

You can also use ASP.NET Membership and Role Manager to create authorization rules for users who register on your site.

SSL

You can now use SSL to secure communications between the media server and Silverlight clients. To do this you must configure SSL on your IIS server and install a certificate on the server from a Microsoft Certificate Authority (CA). You can also obtain certificates from a trusted third-party CA. If you are using a non-HTTP server as your media server, you must configure it to stream over HTTP if you want to use SSL encryption.

Additionally, you can configure a client access policy to allow your non-secured Silverlight applications to call SSL-secured services and applications.

Silverlight DRM, Powered by PlayReady

Silverlight DRM, Powered by PlayReady was introduced in Silverlight 2 and offers a means to protect content according a variety of popular scenarios and business models. The following table contains descriptions of frequently requested customer media scenarios that are supported by Silverlight DRM in Silverlight 4.

[1] Support for PlayReady in offline applications is a feature of Silverlight 4.

Live video	Live video webcasts using either conventional streaming or IIS Smooth Streaming can be protected using Silverlight DRM.
Online video on demand (VOD) services	Web-based VOD “catch-up” services that deliver content using progressive download, traditional streaming, or IIS Smooth Streaming can be protected using Silverlight DRM. In this scenario, a persistent Internet connection is assumed.
Offline VOD services	VOD “catch-up” services that can be used without a persistent connection to the Internet. In this scenario, content can be delivered through progressive download, traditional streaming, or IIS Smooth Streaming, and can be protected using Silverlight DRM. The typical use case is a consumer viewing downloaded videos while on a plane. You typically assign the downloaded content a limited playback lifespan, which means that the consumer's viewing rights expire after a specific duration or on a specific date.
Download-to-Own (DTO)	Similar to the offline VOD scenario. However, the consumer can watch the content for an indefinite period of time.
Download-to-Rent (DTR)	Similar to the offline VOD scenario. However, you set the content expiration date relative to the time the content was first played. For example, consumers can view the content as many times as they like within 24 hours of first play.
Subscription services	These are either online or offline scenarios, where content is playable as long as the consumer has a valid subscription to the service.

The table below summarizes the differences between content protection in Silverlight 3 and in Silverlight 4.

Content Type	Silverlight 3	Silverlight 4
Online VOD content	Yes	Yes
Online live content	Yes	Yes
Content downloaded for local playback	No	Yes

The Silverlight PlayReady DRM solution encrypts the digital content files, not just the stream or connection to the server. This enables you to use the Microsoft PlayReady DRM environment to define the ways in which you want the content to be used, and PlayReady associates this content protection information, known as a license, to each media file in your collection.

Microsoft designed and optimized Silverlight DRM to enable key Silverlight online and offline content distribution scenarios. These include live and on-demand streaming as offered by media servers such as Microsoft Windows Media® Services, progressive file download as offered by sites such as YouTube, and HTTP adaptive streaming as offered by servers such as Microsoft IIS 7 Smooth Streaming. Silverlight DRM encrypts the video and audio in a secure wrapper, ensuring that content, including advertising, stays protected from server to browser until the Silverlight plug-in decrypts and decompresses it for playback.

Silverlight DRM is a small, cross-platform PlayReady client used exclusively by Silverlight. Securing content using PlayReady is quite simple: the content rights holder packages the content for PlayReady using the PlayReady Server SDK, and then builds a license acquisition server for IIS using the PlayReady Server SDK to respond to license requests for that content.

Assuming a consumer is permitted to access the content, the content just plays back for them in their Silverlight application without their having to do anything else. What actually happens behind the scenes is that when a consumer wants to play that protected content, the Silverlight client requests and obtains the license from a PlayReady License Server that uses the PlayReady Server SDK.

The following diagram illustrates how the Silverlight client requests and plays PlayReady protected content for online scenarios.

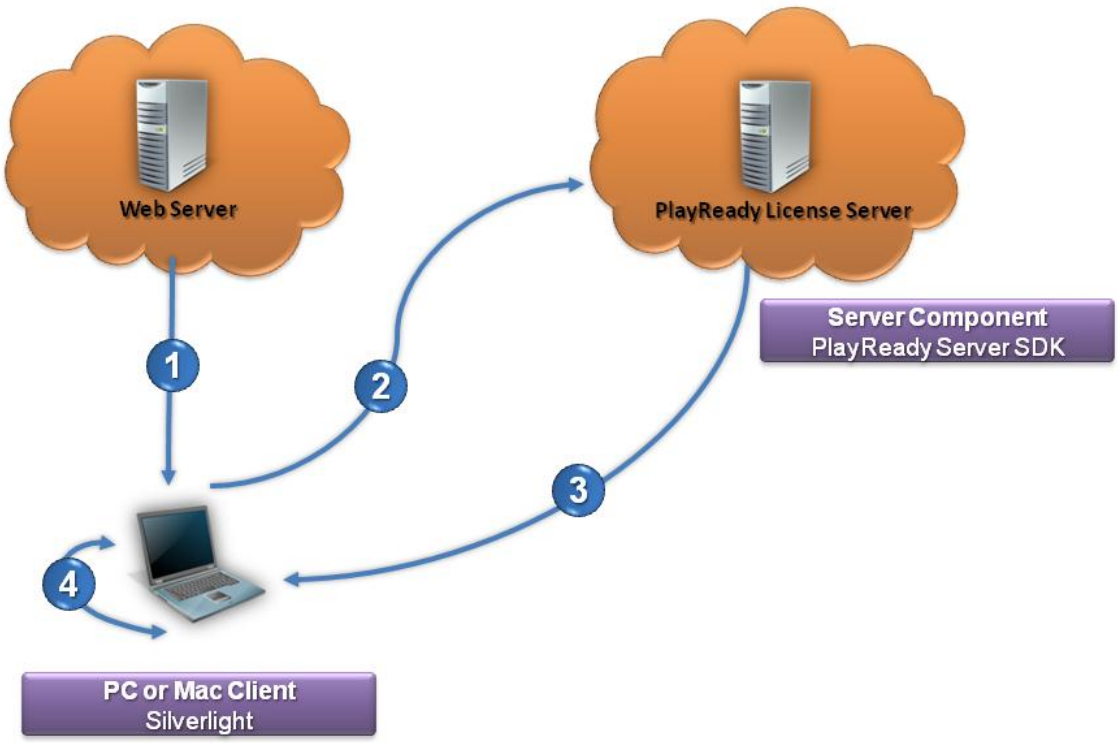

Figure 1. How Silverlight works in a PlayReady solution

1. **Silverlight client acquires the content**. The end user attempts to play some DRM-protected content in a Silverlight application that is stored on the distribution server. The distribution server is usually a Web server used to distribute your content. The Silverlight client downloads the content, or, in the case of streaming, some of the content and the content header.
2. **Silverlight requests a license**. The Silverlight application requests a license to decrypt the content. If the license is not present in the local license store, the Silverlight client contacts the PlayReady License Server to obtain a license. You or your service provider controls the License Server.
3. **PlayReady License Server delivers the license**. If the License Server approves the request, it issues a license which the client uses to decrypt the particular media file. This process is completely seamless and transparent to the consumer.
4. **The Silverlight application decrypts and plays the digital content**.

For offline scenarios, the situation is a little different. The following diagram begins with the assumption that the client computer has already downloaded the encrypted content and the content is available locally to the Silverlight application.

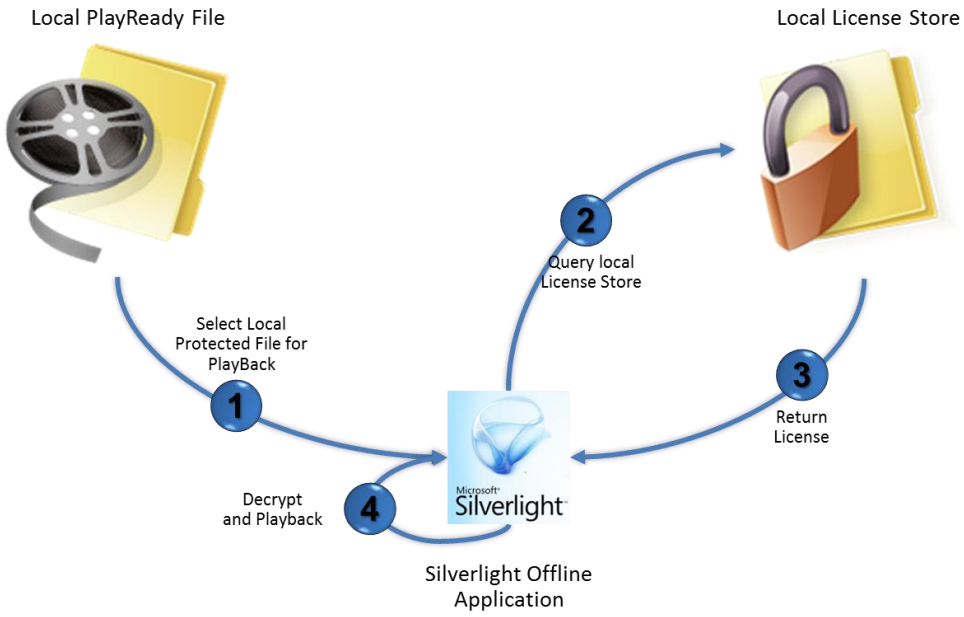

Figure 2. How Silverlight offline applications work with PlayReady licenses

1. **The user selects local protected file for playback**. The consumer uses the Silverlight offline application to attempt to play a DRM-protected content file that is stored on the local device.
2. **Silverlight requests a license**. When the Silverlight offline application attempts to play back the local PlayReady file, it queries the local license store for a PlayReady license.

3. **Local license store delivers the license**. If the required license is available on the client computer, the local license store returns the license to the Silverlight offline application. At some earlier time, a PlayReady License Server would have had to provide the license to the local store and bound that license to the client device.
4. **Silverlight plays the content**. The Silverlight offline application uses the provided license to decrypt and play the digital content.

Finally, Silverlight 4 introduces the concept of domains, which enables content or service providers to provide consumers with the ability to view restricted content on multiple computers while maintaining control over their assets. For example, an online movie rental provider wants to enable consumers to view content on up to three devices of the consumers' choice. After consumers reach that limit, they can remove one or more devices from their PlayReady domain in order to add a new one.

The following diagram illustrates this scenario.

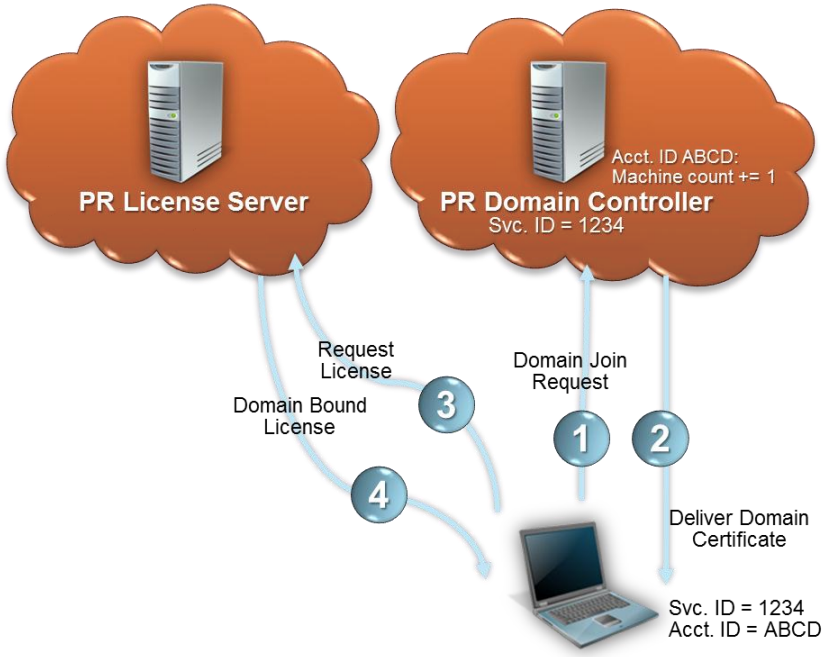

Figure 3. *How Silverlight 4 works with PlayReady domains*

1. **Silverlight requests to join a PlayReady domain**. This can happen transparently to the user, either after the consumer opts into the streaming service or when the consumer requests content for the first time.
2. **PlayReady issues a domain certificate**. The PlayReady Domain Controller issues a Domain Certificate, which is bound to the device that requested the certificate.
3. **Silverlight requests a PlayReady license**. The Silverlight application requests a PlayReady license from the PlayReady License Server.

4. **PlayReady License Server issues a license to the client's domain**. The License Servers issues a PlayReady license that it binds to the requesting device's domain rather than the device itself. This enables the PlayReady content to be decrypted by any device that has both a valid Domain Certificate and a PlayReady license. The Domain Controller tracks the number of devices.

Output Protection

Output protection works in conjunction with Silverlight DRM to protect your content as it passes from your computer to the audio and video hardware that is connected to it. You can define policies in the PlayReady license that enable you to restrict media playback over the Silverlight player, based on whether audio or video outputs on the device are secure. On Microsoft Windows®, the output protection manager components offer enough control that you can specify whether the content can only be played on secure digital devices (HDCP or DPCP), whether it can be played on standard digital devices (DVI-D) or high-definition digital devices (HDMI), and whether it can be played on analog devices (composite video).

Implementing PlayReady

You have two options when you want to use PlayReady to protect your digital content. The first is to have an application service provider (ASP) that specializes in PlayReady DRM solutions host your PlayReady server environment. Second, you can set up your own PlayReady server environment to support your DRM solutions.

Using an Application Service Provider to Host PlayReady

There are a large number of Microsoft-approved partners whom your organization can work with to host a PlayReady implementation for your digital content that is Silverlight DRM-enabled. In this way, you can minimize your development and hosting costs. Microsoft provides a list of PlayReady Service partners who specialize in content access technology solutions to develop, implement, and host your PlayReady service.

The benefits of working directly with a PlayReady Service Provider include:

- Outsourcing the development and deployment of the content access and protection part of the service to specialists who understand the complexities of content-access technology.
- Having no agreements to sign with Microsoft, eliminating the need to report and pay royalties to Microsoft.
- Having no upfront license fees for deploying your PlayReady service.

To view a list of Microsoft-approved ASPs that provide PlayReady server environments, see Engaging a PlayReady Service Provider.

Self-Hosting PlayReady

If you choose to host your own PlayReady environment for your own content distribution DRM solution, you must license and download the PlayReady Server Software Development Kit (SDK). You can then configure and customize the PlayReady server environment to include the server roles required for your solution. These can include:

- **Content Packaging Servers** that take in unprotected content and package it for distribution. When the content is packaged, you copy the protected content to a Distribution Server and transfer the license information to a License Server.
- **Distribution Servers** that store and distribute content. Distribution Servers are usually Web servers, but Microsoft PlayReady technology does not require a specialized Web server for content storage and distribution.
- **License Servers** that store the content protection information and rights for using the content. Before a client can play back protected content it must acquire a license, typically from a license server.
- **Domain Controllers** that determine what a user's domain represents, such as a single user, a family, or a group of users. Domain controllers store the list of entities that are associated with the domain and enforce the policy that defines how many devices or computers can join the domain.

If you choose to host your own PlayReady server environment, there are two licensing approaches:

- If you are an independent software vendor (ISV), network operator, or content service provider and want to develop PlayReady Server Applications, you must acquire a PlayReady Server Application Development and Distribution License. Under this license, Microsoft provides you with a PlayReady Server software development kit (SDK) and all required intellectual property rights to develop and distribute server applications to other PlayReady Server licensees.
- If you are a network operator or content service provider and want to deploy a PlayReady Service, you must acquire a PlayReady Service Deployment License. Under this license, Microsoft provides you with all required intellectual property rights for you to receive server applications from other PlayReady Server licensees and the license rights for you to deploy a PlayReady Service to end users.

For more information about these licensing options, see Licensing PlayReady Server Technology.

PlayReady and Cross-Platform Content Protection

The Silverlight PlayReady client, like the Silverlight plug-in itself, works on a variety of browsers, operating systems, and devices. Cross-browser support includes Mozilla Firefox, Apple Safari, and Internet Explorer browsers, and is available for both Windows and Mac OS.

Summary

Silverlight offers a comprehensive content protection strategy from lightweight stream encryption to full DRM. You can ensure that customers use your premium media content only as you intended by creating content protection licenses that you associate with each media file in your collection. PlayReady is the most comprehensive content protection technology available today. To learn more about PlayReady technology, see the Microsoft PlayReady Home Page. To learn more about how Silverlight DRM works, see Silverlight Digital Rights Management (DRM).

For More Information

Microsoft PlayReady	http://www.microsoft.com/PlayReady/Default.mspx
PlayReady Licensing	http://www.microsoft.com/PlayReady/Licensing/request.mspx
PlayReady Approved ASPs	http://www.microsoft.com/PlayReady/Licensing/engageprovider.mspx
Microsoft Silverlight—Media	http://www.microsoft.com/silverlight/overview/media.aspx
Silverlight Developer Center	http://msdn.microsoft.com/silverlight
Microsoft Silverlight Community	http://silverlight.net/community/

Legal Notice

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.