



WHITE PAPER

Digital Media Protection with Flash[®] Media Server

Macromedia Flash Media Server provides a secure solution for displaying video and streaming MP3s online because no media is cached on the client's hard drive, as is the case with progressive downloads. To deliver Macromedia Flash content safely, while maintaining the utmost control and protection over it, stream your content with Flash Media Server.

November 2005

Copyright © 2005 Macromedia, Inc. All rights reserved.

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

This white paper is for information purposes only. **MACROMEDIA MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.**

Macromedia may have patents, patent applications, trademark, copyright or other intellectual property rights covering the subject matter of this document. Except as expressly provided in any written license agreement from Macromedia, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.

Macromedia and Macromedia Flash are either trademarks or registered trademarks of Macromedia, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Macromedia, Inc.
601 Townsend Street
San Francisco, CA 94103
415-252-2000

Contents

Inherent Capabilities Built into Flash.....	1
Extra Protection Using Flash Media Server	2
Stream Authentication with Flash Media Server	2
Where to Go from Here.....	3

If it's true that content is king, then how do you protect the kingdom? How can you safely deliver content using Macromedia® Flash® while maintaining the utmost control and protection over it? Flash has very strong, built-in digital media protection capabilities when you stream your content with Flash Media Server. This white paper describes how you can take advantage of those capabilities.

Inherent Capabilities Built into Flash

Flash offers a number of digital media protection capabilities that are included from the get-go. Delivering content with Flash Media Server provides even more advanced protection (covered next).

Here are a couple of protection features built into all content delivered with Flash Player:

- **No exposed URLs and media file locations.** The location of media on the Internet can often be compromised by URLs that point back to the content source. Most media players on the market enable users to see the location of the media clip that is playing rather easily. With Flash, external media file locations are compressed into binary format in the SWF file and are unavailable for website visitors—all but eliminating the ability for visitors to obtain the file and server location for media delivered using Flash Player.
- **Control over information that is exposed.** Traditional media players often provide more information about the media than you may be willing to share—for example, filenames, file types, encoding options, delivery methods, and more (see Figure 1).

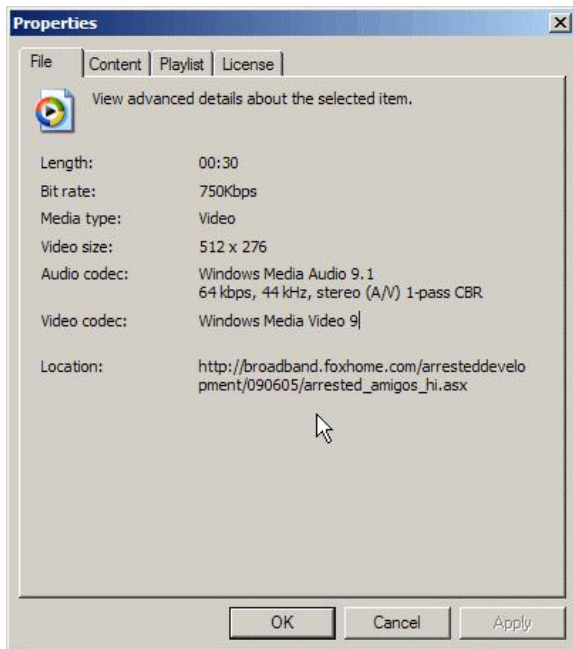


Figure 1: Traditional media players expose locations of files and servers to end users

With Flash Player you can completely customize your media player to display only the information you want your customers to see (see Figure 2). File information is not readily available unless the publisher chooses to make it so.



Figure 2: Flash Player does not expose files and server locations to end users

Extra Protection Using Flash Media Server

Delivering your content with Flash Media Server provides even more protection than what Flash Player provides alone:

- **No client cache.** Flash video content and MP3s delivered to Flash Player using a normal web server are delivered through progressive download. This content is cached on the end user's hard drive and can be easily accessed—and possibly stolen by the user. By contrast, audio, video, and data streamed to Flash clients using Flash Media Server are not cached on local client machines. You can deliver MP3 files and other media safely and securely knowing that your website visitors will not be able to go to their Temporary Internet Files folder and obtain your media file assets.
- **Unique transfer protocol limits stream ripping.** By default, content delivered by Flash Media Server is wrapped inside a Macromedia protocol called RTMP. Because this is an unpublished, proprietary format, stream ripping programs do not have the capability to rip media delivered over Flash Media Server. This minimizes the ability of unauthorized programs to capture a digital media stream from Flash Media Server to Flash Player.
- **Support for SSL and encrypted streams.** Flash Media Server 2 now provides the ability to deliver encrypted streams to provide the tightest layer of security for delivering digital media. When you use this option, the server encrypts all audio, video, and data streams prior to transport. Once they are safely delivered to the client, Flash Player decrypts the content in real time and provides it to user. This encryption is invoked when the client sends information to the server as well, providing the best way to protect content as it travels between the client and server.

Stream Authentication with Flash Media Server

Using Flash Media Server, there are a number of different ways that publishers can verify and authenticate users before a stream is delivered. Authentication methods available in Flash Media Server 2 include the following:

- **Authentication at the SWF level.** In this rather simple method of authentication, the publisher authenticates viewers using existing systems prior to serving the SWF file. Once a user passes authentication and the SWF file is served, audio and video content can be streamed. The benefit of this method is that it fits within your existing workflow, requires no additional changes, and yet authenticates users before serving up content.

- **Authentication at the stream level.** With this method, a SWF file is served up without protection but users are authenticated when they connect to the server and request a stream. This authentication can be done two ways with Flash Media Server:
 - **Scripting:** Using a combination of client-side and server-side ActionScript, client information such as username, password, or even connection information can be passed to the Flash Media Server server. Once that happens, that information can be used to authenticate users against back-end systems. Support for XML objects and Flash Remoting calls in the server facilitate this process.
 - **Executing authentication applications:** For the maximum level of control, a plug-in module with Flash Media Server enables publishers to run external applications that are responsible for providing access to the server and content. This is useful for providing access in pay-per-view scenarios or even to prevent rogue sites from deep-linking into your content or server.

The options listed above can be used to support a number of different authentication uses, including:

- Support streaming in a single sign-on system
- Authenticate users against an LDAP directory
- Prevent unauthorized sites from deep-linking to your content
- Prevent others from stealing bandwidth
- Support pay-per-view content or events

Where to Go from Here

Flash Media Server is the only solution for securely streaming audio and video through the Flash Player. For more information about Flash Media Server, visit www.macromedia.com/go/fms.