Overview

Adobe® Flash® Media Rights Management Server

May 2008

Version 1.0

Adobe® Flash® Media Rights Management Server 1.0 Overview for Microsoft® Windows®, Linux®, and UNIX®
Edition 1.1, May 2008

Adobe Systems Incorporated, 345 Park Avenue, San Jose, California 95110, USA.

Contents

About this document

Adobe® Flash® Media Rights Management Server provides content distributors with the ability to protect FLV and F4V files that are delivered to Adobe Media Player and Adobe AIR™ applications. This document provides an overview of Flash Media Rights Management Server.

Who should read this document?

This document provides information for two primary audiences:

IT administrators: Gets the system up and running, and maintains scalability, availability, reliability, and so on.

Content publishers: Uses the system to protect their content and manage the rules.

Additional information

The resources in this table provide additional information about Rights Management Server.

For information about	See
The Rights Management Server solution, development environment, run-time environment, and each Rights Management Server component	*Overview*
Installing, configuring, and deploying Rights Management Server	*Installing and Deploying Rights Management Server for JBoss Using Turnkey* *Installing and Deploying Rights Management Server for JBoss* *Installing and Deploying Rights Management Server for WebLogic*
Managing administrative users and user roles	*User Management Help*
Installing Flash Media Server	*Adobe Flash Media Server Installation Guide*
Customizing and configuring Flash Media Server	*Adobe Flash Media Server Administration and Configuration Guide*
Creating custom service providers for Adobe User Management and Adobe LiveCycle Rights Management ES	*Developing Service Providers*
The Java™ interfaces and classes used to create custom service providers	*Adobe Flash Media Rights Management Server API Reference (Javadoc)*
Securing video content and playlists by using the Rights Management Server command line tools	*Securing Video Content and Playlists*

For information about	See
Delivering content in Adobe Media Player	*Adobe Media Player Content Developer Kit*
Using Adobe Media Player to find and view content	*Adobe Media Player Help*

1 About Flash Media Rights Management Server

With Adobe Flash Media Rights Management Server, you can protect media content delivered to Adobe Media Player and Adobe AIR applications. This cross-platform solution easily integrates into your existing network and allows you to maintain more control of audio and video content, no matter how widely it is distributed. Flash Media Rights Management Server helps protect and monetize content with confidence and provides the flexibility to manage how and where your media is experienced.

Flash Media Rights Management Server gives content distributors the ability to rapidly distribute content and recuperate production costs through direct (user-paid) or indirect (advertising-paid) compensation by their consumers.

Flash Media Rights Management Server also gives consumers the flexibility to view this content as they have with traditional media, but also with access to more online media and a viewing experience that is intuitive, non-intrusive, convenient, and engaging. Using Adobe AIR, developers can develop their own custom media players.

Using the service provider interface (SPI) on the server, developers can automate Flash Media Rights Management Server capabilities, including authorization and authentication, and integrate the authorization engine into the customer environment.

Key features

Flash Media Rights Management Server has these key features:

Content integrity: Ensure that content remains intact. Consumers cannot watch or extract content without watching all the content in a particular playlist. For example, when consumers watch playlists, they have to watch the advertisements that are part of them.

Identity-based licensing: Tie permissions to specific user identities, preventing consumers without proper permissions to view the content.

Multiple authorization levels per content package: Designate different authorizations for various pieces of a content package. For example, retailers may want to make a single FLV file in a playlist freely available but charge for the remaining content.

Offline viewing: Let consumers view content offline, as well as online. Offline viewing is still subject to Automated Audit and Analytics.

User authentication: Authenticate against existing retailer systems. This is part of identity-based Flash Media Rights Management Server.

Horizontal server scaling: Scale servers horizontally for performance, reliability, and redundancy.

Server-Side SPI: Automate Flash Media Rights Management Server capabilities (including authorization and authentication) and integrate the authorization engine into your environment.

Reach as many people as possible: Protect content almost anywhere, due to the platform independence of Adobe Media Player and Adobe AIR applications.

Cross-platform content delivery: To help simplify your publishing efforts, you can deliver content across Microsoft® Windows® and Macintosh® platforms to users who use Adobe Media Player, which provides feature-rich playback or Adobe AIR applications to deploy rich internet applications (RIAs).

Content protection with Adobe Media Player: Help ensure that ads cannot be replaced or removed, and that content cannot be reused or remixed without your consent.

Persistent content protection: Help protect access to your media whether the user is online or offline, even after the content is shared.

Precise usage control: Specify a range of parameters that let you assign initial access and expiration dates to a file, limit access to an individual or group, or any combination.

Dynamic rights management: Stay in control with the flexibility to change usage rights even after a file is distributed and the ability to leverage access rights from an existing content management system.

Offline access auditing: Track usage of your content when viewed through Adobe Media Player or Adobe AIR applications, even when consumers are offline.

Monetize content: License assets according to the identity of the consumer and explore revenue-building distribution models, including rental arrangements for limited usage or download-to-own licensing with fewer restrictions.

Security solution integration: Take advantage of tight integration with Adobe Media Player and Adobe AIR applications for a complete media deployment solution and the flexibility to work smoothly with existing access protocols, including LDAP and Active Directory, as well as custom portal management environments.

Workflows

Two typical workflows are available:

- Content protection
- Identity-based licensing

Content protection

With content protection in Adobe Media Player, content publishers can protect playlist integrity, including bundled advertisements. For example, a consumer wants to download a television program to his laptop. The content publisher has included the program segments and advertisements in the playlist. The advertisements in the playlist are applicable to the demographic information that the customer provided to initiate the download. The content publisher has also set an expiration date, after which the program can no longer be played.

After the playlist is fully downloaded, the consumer can watch the program offline. The content publisher uses the Automated Audit and Analytics feature to track the number of times the content is viewed, both online and offline, so that they can collect advertisement revenues. User credentials are not required.

To enable this workflow, the content distributor runs Media Packager to encrypt the content and Adobe Media Orchestration Document (AMOD) Signer to sign the playlist. After the encrypted file is created, it can be moved to the proper server for distribution.

Identity-based licensing

With identity-based licensing, the content publisher can protect content with user credentials. For example, a consumer wants to download a television program, but does not want to watch the accompanying advertisements. To avoid watching the advertisements, consumers pay the content publisher a premium. They download the program from the content publisher's website to their Adobe Media Player, which caches their user credentials. After the program is downloaded, they only have to open it to view it anytime, even when offline. The content, however, is protected by user credentials and cannot be shared with other users. Adobe AIR application developers can also incorporate encrypted content in their custom applications.

To enable this workflow, the content publisher runs Media Packager on the unprotected content and specifies protections. The protected content can then be distributed. When a user tries to play the content, Flash Media Rights Management Server contacts the content publisher's system through their service provider interface (SPI) to query whether the user is allowed access to the content and, if so, for how long. As such, user credentials are mandatory.

However, identify-based licensing also supports anonymous access. The policy determines whether anonymous access is allowed and how it is applied. A *policy* is a collection of information that can include confidentiality settings and a list of authorized users. The confidentiality settings specified in a policy determine how a recipient can use the media file to which the content publisher applies the policy. A policy also enables the permissions on a media file to be changed dynamically. It enables content publishers to change the security setting, revoke access to the media file, or switch the policy.

Using policies, content publishers can assign the following properties to media files:

- Optional start and end dates
- Number of days to cache the license in Adobe Media Player or the AIR application
- List of approved playback application IDs (optional)
- Authentication domain (required for credentials)

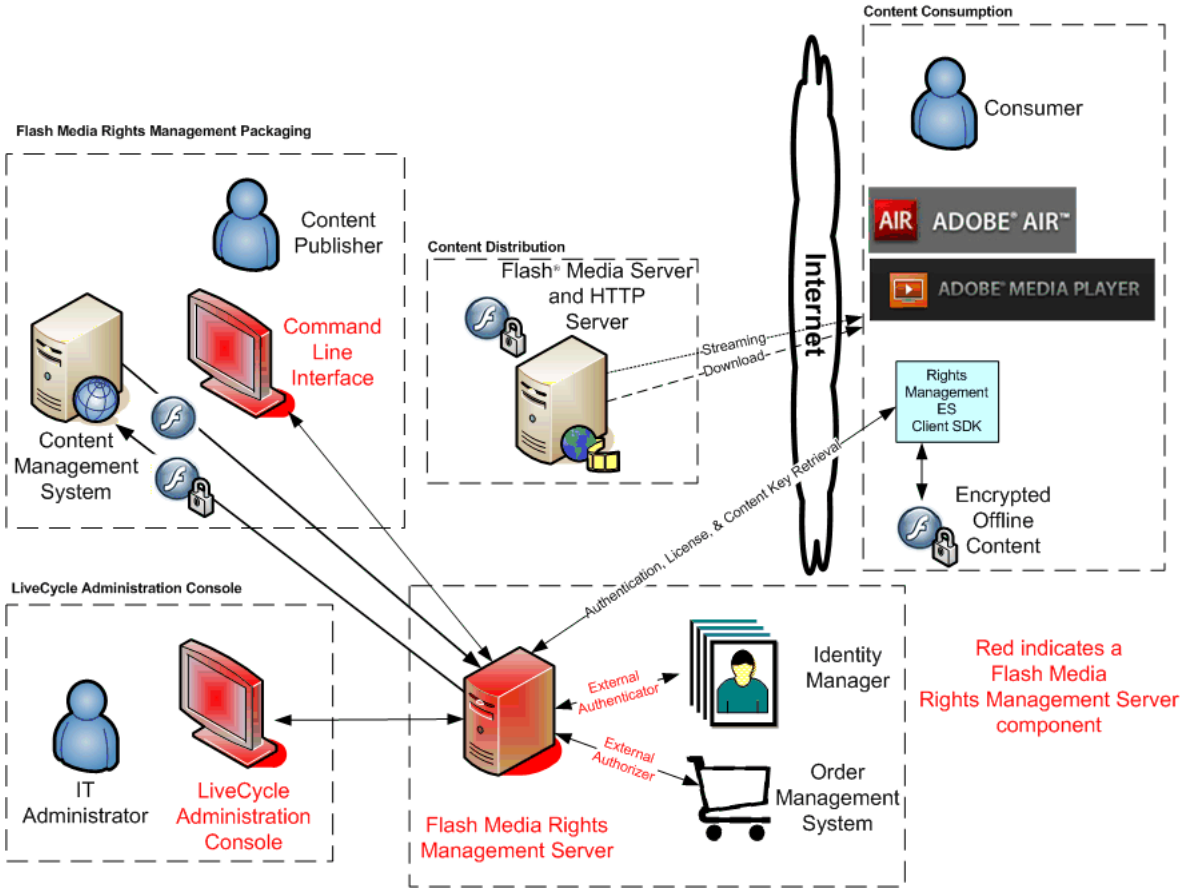
Policies are stored in the Policy database on the Flash Media Rights Management Server server. Policies use the SPI for authorization.

How Flash Media Rights Management Server works

Flash Media Rights Management Server comprises four main components:

- LiveCycle Administration Console
- Flash Media Rights Management Server packaging
- Content distribution
- Content consumption

The following illustration shows how major components interact with Flash Media Rights Management Server. Red indicates a Flash Media Rights Management Server component.



LiveCycle Administration Console

Adobe LiveCycle® Administration Console gives administrators access to tools so that they can configure and manage users, groups, and roles. For content publishers who require their customers to have credentials to access content, Flash Media Rights Management Server must be configured to authenticate the customers. IT administrators use the Domain Management user interface in LiveCycle Administration Console to configure user authentication. After the customer credentials are created, they are stored in the content publisher's database. To authenticate a customer's credentials, an interface between Flash Media Rights Management Server and the content publisher's database must be developed using the Flash Media Rights Management Server SPI. For more information, see *Developing Service Providers*.

To use Rights Manager and Media Packager for Flash Media Rights Management Server packaging, users require a special role, specifically, the Services User role. IT administrators use the Adobe User Management user interface in LiveCycle Administration Console to assign this role.

Flash Media Rights Management Server packaging

In Flash Media Rights Management Server packaging, a policy—dynamically generated or preexisting—is applied to content (FLV and F4V files). Media Packager invokes LiveCycle Rights Management ES to encrypt the content, which includes these tasks:

- Fetching the policy for the content
- Creating a license for the content and a unique content encryption key
- Storing the binding between the content and the encryption key in its database

After LiveCycle Rights Management ES returns the policy, license, and content encryption key, Media Packager embeds the policy and license into the FLV file or F4V file and encrypts the file body by using the content encryption key. (The encryption key is unique and Media Packager discards it after encryption.) Media Packager then stores the encrypted FLV file or F4V file to the path specified on the command line. The retailer's order management system uses the content identifier in the license to determine in real time whether a user should have access to the FLV or F4V file.

Note: Because Flash Media Rights Management Server encrypts the file format itself—rather than the entire file—metadata remains unencrypted and therefore search engines can still search the file.

Flash Media Rights Management Server packaging tools

Flash Media Rights Management Server packaging comprises command-line interface tools that allow content distributors to create and apply Flash Media Rights Management Server policies to encrypt and sign their content. Three tools are available:

- Rights Manager
- Media Packager
- AMOD Signer

Rights Manager

Using *Rights Manager*, administrators can create, list, view details of, and update policies.

Using the Services User role, users can specify options on the command line and in the policy.properties configuration file.

Media Packager

Using *Media Packager*, administrators can encrypt FLV files and F4V files and associate a policy with the file. Encrypting files prevents unauthorized users from viewing them. Using the Services User role, users can specify options on the command line and in the packager.properties configuration file.

AMOD Signer

Using *AMOD Signer*, administrators can sign playlists. Signatures protect playlists from being tampered with. Users can specify options on the command line and in the signer.properties configuration file. For more information about playlists, see the *Adobe Media Player Content Developer's Kit*.

AMOD Signer and Media Packager require credentials, which are distributed by Adobe.

Content distribution

The content publisher makes the content available for download. The content is distributed by using either Flash Media Server or the HTTP server. Content distribution is initiated when either a Flash Media Server or HTTP server fetches the encrypted content. The Flash Media Server streams or the HTTP server transfers the content to Adobe Media Player or a custom Adobe AIR application. Neither Flash Media Server nor the HTTP server needs to decrypt the content. All aspects of the FLV file that need to be inspected by Flash Media Server to intelligently stream the content are accessible to Flash Media Rights Management Server. HTTP servers do not inspect the FLV file.

Content consumption

Content publishers can allow consumers to access encrypted FLV files anonymously or they may require credentials. If the publisher requires credentials, the consumer has likely purchased access to the content. The content publisher can choose to have the content expire a set number of days after it is downloaded. Each consumer who downloads the content then has the set number of days to view it. This period is specified as a property in the policy. It is enforced by setting the expiration date on the voucher. The client tracks playback and determines the appropriate expiration date.

The consumer opens secured content in Adobe Media Player or in a custom Adobe AIR application. If the consumer is online, the Flash Media Rights Management Server client checks to see whether it has a cached voucher for the content. If it does, the client gets the key from the voucher. If the client does not have a cached voucher for the content, it contacts the Flash Media Rights Management Server. If the consumer is offline and has previously accessed the content, Adobe Media Player or the Adobe AIR application will have a cached voucher that allows access.

Regardless of whether the client is online or offline, the client always look for a cached voucher first. If the client does not find a cached voucher, it will try to contact Flash Media Rights Management Server to download a voucher. Content publishers can decide whether they want to allow vouchers to be cached on the client and, if so, for how long. These parameters can be set when the policy is created. It is also possible to provide different voucher caching characteristics for different users by setting the expiration in the custom external authorizer.

Typical deployment scenario

A typical deployment scenario is to have Flash Media Rights Management Server installed on a different computer than Flash Media Server or HTTP server. The other components of Flash Media Rights Management Server, such as Media Packager and administration tools, can be installed elsewhere.

For maximum scalability, Flash Media Rights Management Server and the customer's ID management and order management systems should be as close as possible.