White Paper

Akamai® HD Network
SecureHD

Table of Contents

Overview

With the skyrocketing popularity of online video, content publishers have an extraordinary opportunity to leverage the compelling, interactive Internet medium to reach greater audiences and explore new business models. Key to enabling success, however, is meeting the contractual obligations of the rights holders. This is the ability to protect online content from unauthorized use and redistribution, as content piracy fundamentally threatens the content publisher's ability to monetize its valuable assets.

Securing media assets is a complex issue – one that requires a defense-in-depth approach employing different techniques to defend against different threats. In addition, content protection solutions need to strike the right balance between business and legal requirements, end user experience, and cost.

This whitepaper looks at the most common types of attacks video content providers face today and explains how the security mechanisms built into the Akamai HD Network combat these threats. We will examine Akamai's security features in detail, to illustrate how publishers can protect their media assets while delivering the best possible user experience to global, broadcast scale audiences.

While the Akamai HD Network offers these secure capabilities across popular platforms, including Adobe® Flash®, Microsoft Silverlight, and the Apple iPhone & iPad, this document provides technical details specific to Akamai HD for the Adobe Flash platform.

How Video Content Gets Stolen

The points that follow list some of the most common forms of premium content attack:

- **Link Sharing** – Unauthorized users obtaining access to premium/paid content and bypassing a retailer's business model.
- **Deep Linking** – A hacker decompiles the player and posts the hidden links to his own site to monetize on the content.
- **Player Hijacking** – Theft of the player, followed by copying it to a different website, thereby bypassing attributions to the origin site.
- **Stream Ripping** – Theft of the actual content from the stream while it is being delivered to client systems.
- **Stealing from Cache** – Theft of the content from a browser, player cache or disk.
- **Content Tampering** – Modification of the actual content (e.g., replacing/injecting unwanted advertisements into the stream).

Protecting Content on the Akamai HD Network

Akamai offers "SecureHD", a set of security modules that can be used, independently or together, to provide content protection while allowing legitimate users to enjoy a smooth and stunning viewing experience. These mechanisms are designed to discourage and disable content and link piracy, while allowing the content owner to successfully monetize its assets — whether through pay-per-view, rentals and subscriptions, ad-supported, or other innovative business models.

SecureHD includes four key protective mechanisms:

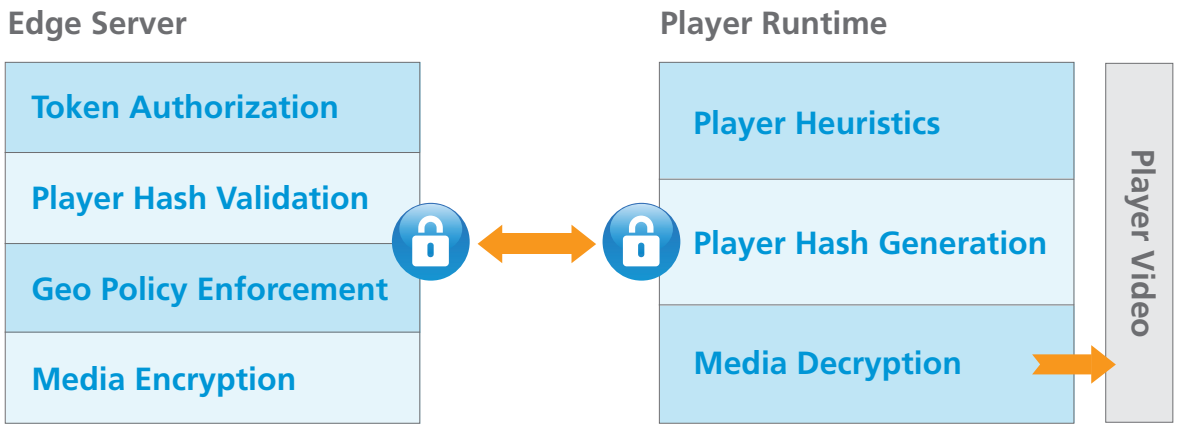
- **HD Token Authorization** – Authorizes the end user and prevents Link Sharing and Player Hijacking
- **HD Player Verification** – Validates that the player playing the content is one of the approved players; helps detect player tampering and prevents deep linking
- **HD Media Encryption** – Delivers the encrypted content to player runtime
- **Content Targeting** – Enforces access in specific geographic regions (GEOs) and prevents GEO access violations

SecureHD Building Blocks

HD Token Authorization	Subscriber/User Entitlement to Enforce Authentication
HD Player Verification	Player Tamper Detection and Validation
HD Media Encryption	Secure Content Encryption
Content Targeting	Enforcement of Geographic Access Restrictions

HD Network Streaming and Security

Streaming Security Use Case



Security operations between the Edge Server and the Player Runtime

The steps that follow document a standard streaming use case example that incorporates SecureHD.

1. A media customer uploads video on-demand (VOD) content to the Akamai Storage service (NetStorage). Optionally, this content can be retrieved directly from a customer location or can be a live stream.
2. The media customer creates security policies using the Akamai EdgeControl portal to help protect its online content from the most common threats discussed in previous section.
3. An end user attempting to access this content authenticates to the customer portal and clicks a link to the video they wish to view.
4. The customer portal generates a time-bound Akamai Token, appends it to the URL and redirects the end user to an Akamai Edge Server.
5. The Akamai Edge Server authorizes the end user by validating the token to help prevent link sharing and player hijacking attacks.
6. The Akamai Edge Server also applies any geo-based policies streaming the content.
7. The Akamai Edge Server then validates that the player used by the end user is one of the players approved for use by the media customer. This is to help prevent deep linking attacks and detect player tampering
8. Once the Akamai Edge Server validates that the end user is authorized and the player in use is authentic, the Akamai Edge Server performs "In Network" encryption of the streams and delivers them to player run time.
9. The player retrieves a unique session key, which is secured by Akamai tokenization. Using this session key, the player derives the content encryption key and uses it to decrypt the stream.
10. Content encryption from the Edge Server to player run time helps prevents against stream ripping and content tempering attacks. It is designed such that content stays encrypted in transit and when at rest in the browser cache.
11. The player plays the decrypted stream back to the end user.

Technical Overview

This section provides additional details on the various security layers available as part of SecureHD that can be used to secure live or on-demand content.

HD Token Authorization

Token-based authorization mechanisms are commonly used across the internet as a security mechanism to validate user rights. To help confirm that only authorized users get access to your video stream, Akamai's HD Token Authorization security mechanism can be used to provide a hybrid token scheme in which a combination of a short TTL URL token and a long TTL cookie-based token is used.

Some of the key highlights of HD Token Authorization are as follows:

- Support for multiple cryptographic hash functions. Offers HMAC-SHA256 (strongest) and HMAC-SHA1.
- Allows for passage of data for advanced usage and encryption of the entire token payload.
- Allows for configuration of start and expiration times for better control of token validity.

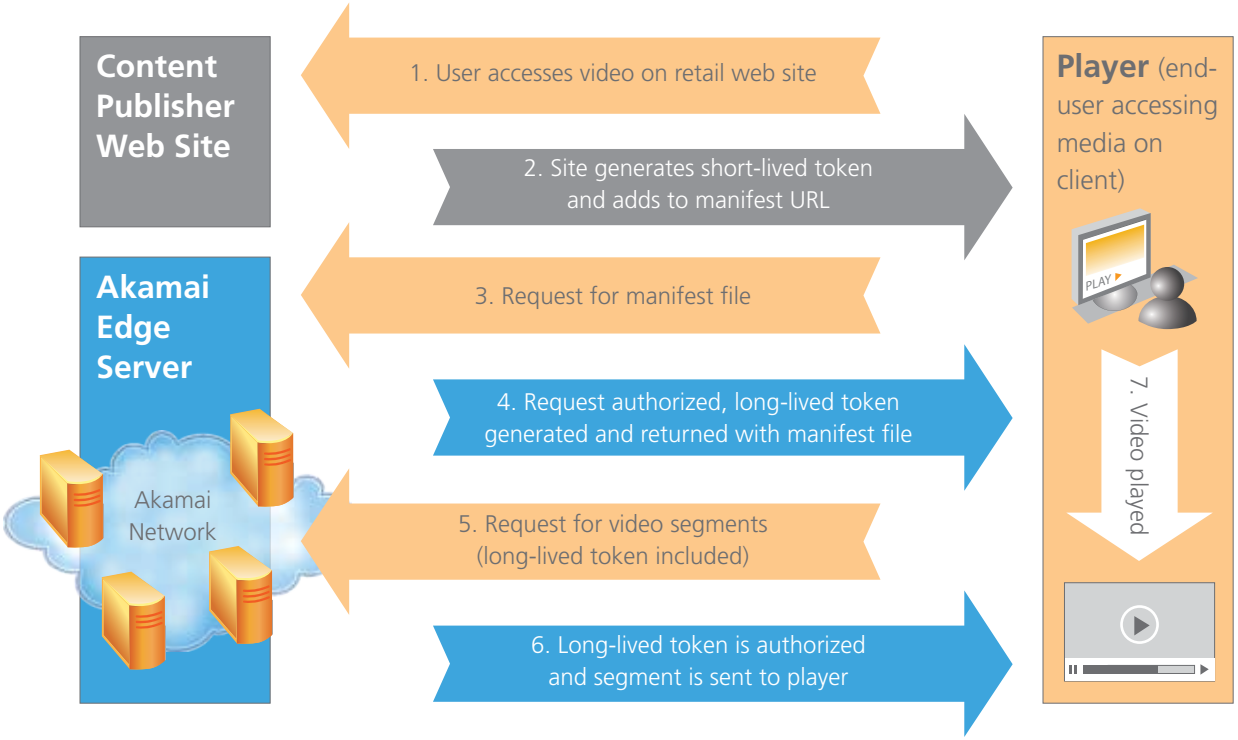
HD Token Authorization is seamless to the end user and typically requires no changes to the video player.

Edge Server Configuration

The retailer/customer configures a "secret" password using the Akamai EdgeControl portal. This shared secret is used to verify a Token received by Edge Server from the player requesting the content.

Content Publisher Site Integration

The Token Generation SDK is provided by Akamai, which is used by a content publisher site to generate a Token. HMAC of the various inputs (like IP Address, start time, expiration, URL, ACL time, duration) is calculated using a shared secret (Hex-encoded key) and appended to the URL.



HD Token Authorization 2.0 Workflow

HD Player Verification

HD Player Verification is designed to prevent unauthorized players from playing protected content. Because the video player application can control much of the user experience (e.g., look and feel, playback functionality, ad watching, and security features) ensuring that the player is a valid and unaltered one offers a high level of security against deep linking attacks aimed at circumventing the content provider's business model.

This security mechanism is designed to ensure that a player and resident AUTH module are authentic. This is normally achieved by hashing the player and the AUTH module to produce a message digest for verification by Edge Server. In addition, Player Verification will also include a means by which to test the running image for certain security code, and obfuscation of the AUTH module.

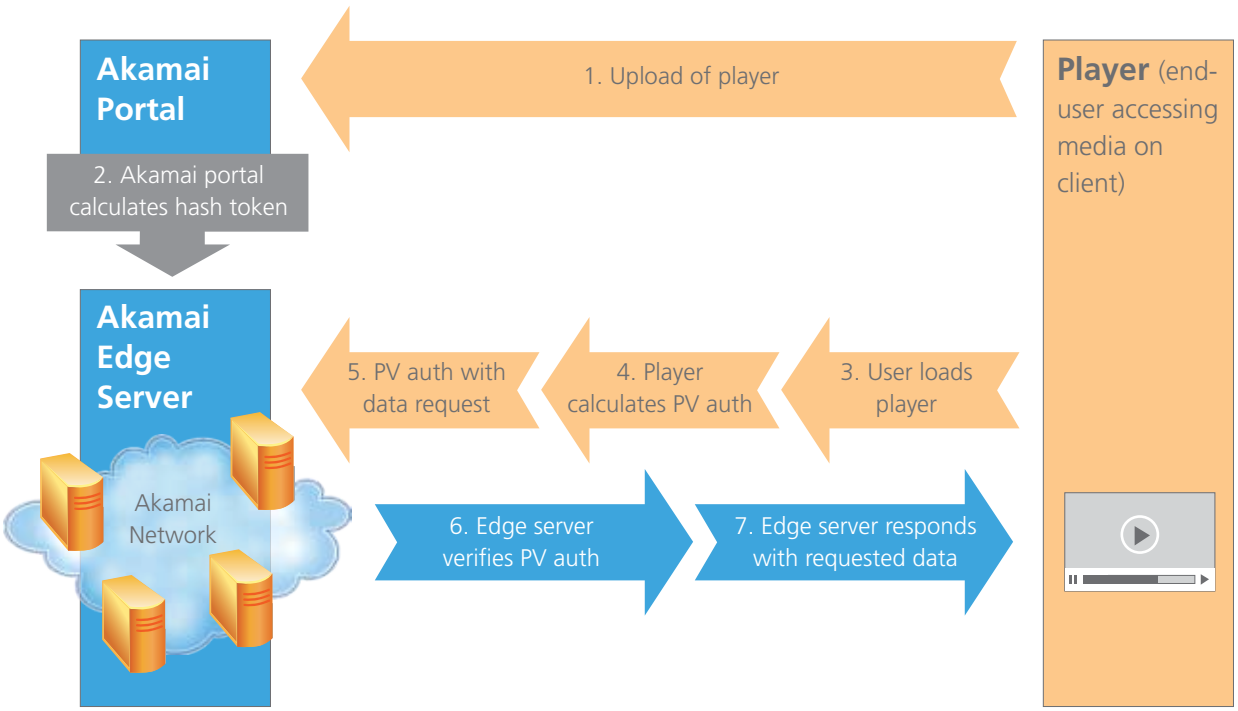
The points that follow illustrate some of the key highlights of HD Player Verification:

- Each customer can enforce delivery to only their approved player(s).
- An approved list of players is maintained on the Edge Server. It can be easily updated and becomes effective in the matter of minutes.
- Allows the customer to respond faster to player breaches by renewing the AUTH module.

Player Integration

Akamai provides an HD Player component that contains a security AUTH module. This module includes cryptographic hashing and encryption methods for the purpose of identifying the running player, and securely communicating the results to an Akamai Edge Server. Customers are required to build their players using this HD Player component to leverage HD Player Verification.

The diagram below offers an example of Adobe HTTP dynamic streaming (HD) workflow using HDS Player Verification security mechanism.



HD Player Verification 2.0 Workflow

Faster Breach Response Mechanism

The Renewable Player side AUTH plugin (part of the HD Player component) allows for a change in the hash-computing algorithm (KDF) in real time, without requiring any player patches to the run time. These changes can be pushed to the player from Akamai Edge Server.

HD Media Encryption

HD Media Encryption is a unique way of providing content protection, which enables for faster breach response. By using a combination of configurable security elements, the player security module accepts messages in the content stream that provide the instructions needed to decrypt the payload. These messages are used to produce the keys that protect the clear text content. The message format supports group, per session, and shared keying, along with file-level persistent encryption for a variety of file formats. Unlike DRM, the messages do not carry policy information. Instead, the messages confer entitlement through conditional access to a session-specific key referenced through a URL in the message. In this way, access to the session key requires a valid token for each segment of content. Using unique a multi-factor security mechanism in protected portions of the message, HD Media Encryption allows the system to switch keys continually, reducing the risk of prolonged breach due to key sharing. This is provided through the use of secure control messages, a set of renewable key derivation functions and metadata configuration parameters.

The key highlights of HD Media Encryption are listed below:

- Content is encrypted in transit and at rest
- Limits the content breach by using unique encryption key per session
- Multi-factor decryption mechanism for stronger security
- Supports message integrity to detect content tempering
- Provides breach response

Player Integration

Akamai provides an HD Player component that contains a security AUTH module, that is used to perform the above-mentioned security operations. Customers are required to build their players using this HD Player component to leverage HD Media Encryption.

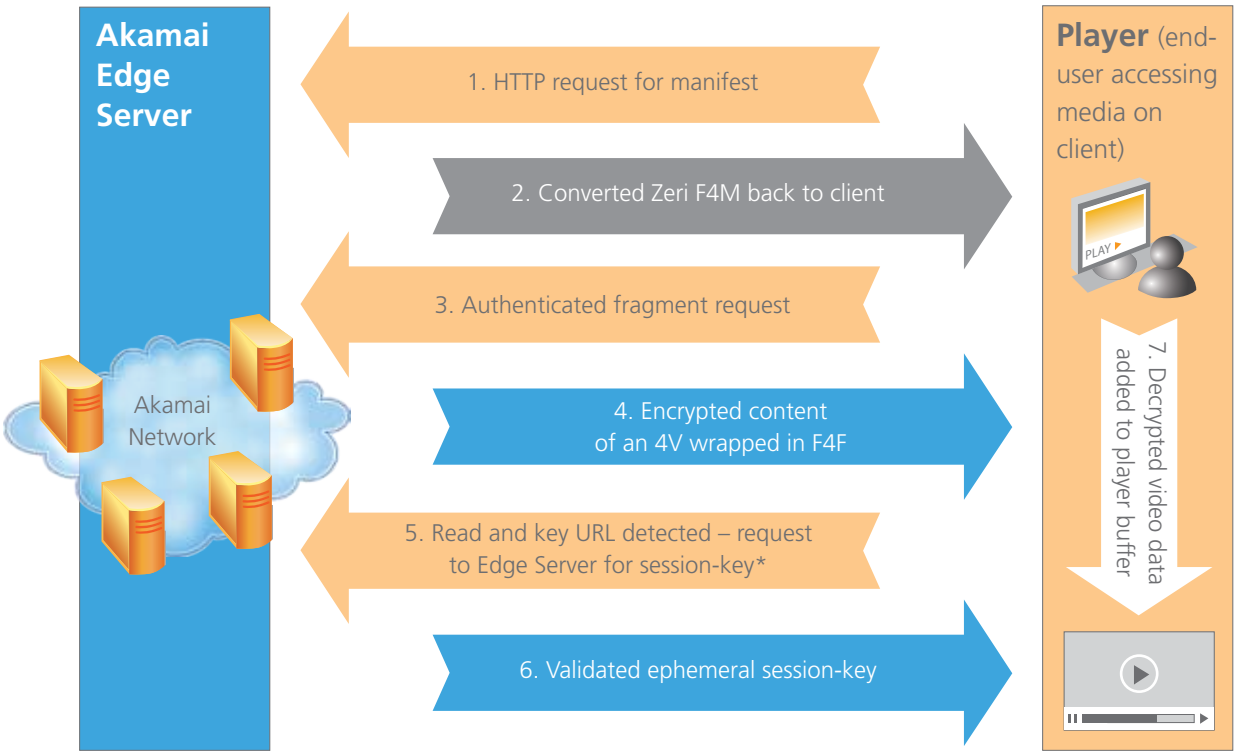
Edge Server Configuration

The Akamai Edge Server encrypts the video content dynamically and, through Akamai EdgeControl, can be configured to specify which cryptographic algorithm to use (default is AES 128-CBC).

Breach Response Mechanism

The Renewable Player Side AUTH plugin (part of the HD Player component) allows for a change in the key derivation algorithms in real time, without requiring any player patches to the run time. These changes can be pushed to the player from Akamai Edge Server.

The diagram on the next page offers an example of Adobe HTTP dynamic streaming (i.e. for Adobe HTTP Dynamic Streaming) workflow using the HD Media Encryption security mechanism.



**This request is protected by token authorization, player verification, or some other custom scheme.*

HD Media Encryption Workflow

Content Targeting

Based on the Akamai EdgeScape service, Content Targeting protects against content access in specific geographic areas. At a standard level of service, EdgeScape provides geo-based protection based on continent, country, or region within an individual country. The EdgeScape Pro level of service offers additional granularity. The system can be enabled to support access control based on city, marketing area, metropolitan statistical area (MSA), primary metropolitan statistical area (PMSA), and zip code (US and Canada only) through professional services.

Content Targeting works by looking up the end user's IP address in Akamai's EdgeScape Database. Using a sophisticated collection of data gathering and verification techniques, Akamai has leveraged the unmatched breadth of its global network and network service provider partnerships to build and continually refine a comprehensive and accurate IP database.

Content Targeting can be implemented in two different ways, as outlined in the sections that follow.

Akamai Edge Server Side Implementation (Using the Akamai EdgeControl Portal)

In this type of implementation, customers simply define the access control rules for their video content via the Akamai EdgeControl portal. Customers can update the configuration as needed. There is no additional infrastructure running on the customer origin server, and this requires no changes to the player or customer web site code.

When an end user video request is received by an Akamai Edge Server, the server evaluates the end user's IP address against the EdgeScape data, applies the customer's business rules, and delivers the content only if access is allowed.

Summary

The security mechanisms enabled by the Akamai HD Network are designed to provide customers with proven, industry-leading tools for defending against the theft and unauthorized use of their online video content across major player run times. SecureHD offers a multi-layer security approach, which can be implemented in an easy and scalable way that avoids end-user software installation and maintenance hassle. The solutions integrate seamlessly with customers' existing authentication and access control architectures.

Moreover, by leveraging Akamai's global network of tens of thousands of edge servers, content providers can deliver stunning HD experiences to audiences of any scale – securing their content and revenue streams without sacrificing performance or end user experience.

The streaming media security landscape is one that will continue to evolve. As more and more compelling content is made available online, efforts to misappropriate and misuse the content will increase as well, and content providers need to arm themselves with best-of-breed solutions to protect against those threats.

Akamai has spent the last decade innovating to make the Internet a better, faster, and more secure place to interact, entertain, and transact business. With thousands of companies depending on its EdgePlatform to securely and reliably deliver an aggregate of 500 billion Web interactions each day, security is never a secondary priority at Akamai. Instead, it is comprehensively integrated into every aspect of Akamai's network and operations, from hardened servers and a self-healing architecture to the rigorous physical and operational security policies in place. And because it understands the critical importance of video content protections—to its customers businesses and ultimately to its own, Akamai intends to continue to innovate and produce market-leading streaming media security solutions.

SecureHD – Key Features	Description	Business Value
Support for major formats	Supports FLV, HDS and HLS	Reach and scale by delivering securely over HTTP
Encryption	AES-128-CBC bit encryption	Content is encrypted in transit and at rest, mitigating attacks from stream rippers
Unique Encryption Key per session	Does not require any key rotation	Designed to defeat key sharing attacks and minimize scope of breaches
Performance (Client/Server side)	Simple workflow providing content protection	No additional complexity or over head
Client Hardening	Full obfuscation, custom key smearing, per player versioned secrets	Designed to mitigate the scale of attacks against the player to a narrow/low-value target.
Breach Response (if compromised)	Optional: late-binding of security module supports transparent renewability	Breach can be stopped within minutes and requires no player run time changes.

The Akamai Difference

Akamai® is the leading cloud platform for helping enterprises provide secure, high-performing user experiences on any device, anywhere. At the core of the company's solutions is the Akamai Intelligent Platform™ providing extensive reach, coupled with unmatched reliability, security, visibility and expertise. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling enterprises to securely leverage the cloud. To learn more about how Akamai is accelerating the pace of innovation in a hyperconnected world, please visit www.akamai.com and follow @Akamai on Twitter.

Akamai Technologies, Inc.

U.S. Headquarters

8 Cambridge Center
Cambridge, MA 02142
Tel 617.444.3000
Fax 617.444.3001
U.S. toll-free 877.4AKAMAI
(877.425.2624)

www.akamai.com

International Offices

Unterfoehring, Germany
Paris, France
Milan, Italy
London, England
Madrid, Spain
Stockholm, Sweden
Bangalore, India
Sydney, Australia
Beijing, China
Tokyo, Japan
Seoul, Korea
Singapore