AWS Elemental Secure Packager and Encoder Key Exchange API Specification
Developer Guide
AWS Elemental Secure Packager and Encoder Key Exchange API Specification: Developer Guide

Copyright © 2017 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.
# Table of Contents

What Is AWS Elemental Secure Packager and Encoder Key Exchange? ................................................................. 1
  How to Get Started .............................................................................................................................................. 1
Customer Onboarding ............................................................................................................................................ 3
  Step 1: Check Supported Technologies ........................................................................................................... 3
  Step 2: Get On Board with an AWS DRM Solution Provider ........................................................................ 3
SPEKE API Specification for DRM Solution Providers ....................................................................................... 5
  Architectural Overview .................................................................................................................................. 5
  Are You New to SPEKE? .................................................................................................................................. 6
  Terminology ..................................................................................................................................................... 6
  Related Services and Specifications .................................................................................................................. 7
AWS Authentication for SPEKE ......................................................................................................................... 7
SPEKE API ........................................................................................................................................................... 8
  Live Workflow Method Calls ............................................................................................................................ 8
  VOD Workflow Method Calls .......................................................................................................................... 12
Heartbeat .......................................................................................................................................................... 14
Document History .............................................................................................................................................. 16
AWS Glossary ................................................................................................................................................... 17
What Is AWS Elemental Secure Packager and Encoder Key Exchange?

AWS Elemental Secure Packager and Encoder Key Exchange (SPEKE) is part of the AWS Elemental content encryption protection strategy for media services customers. SPEKE defines the standard for communication between our media services and digital rights management (DRM) system key servers. SPEKE is used to encrypt video on demand (VOD) content through AWS Elemental MediaConvert and for live content through AWS Elemental MediaPackage.

The following illustration shows a high-level view of the AWS Elemental content encryption architecture.

These are the main services and components:

- **AWS Elemental media service**—Provides the encryption technology. The service receives encryption requests from its operator and retrieves the required keys from the DRM key server, through Amazon API Gateway. It delivers the encrypted content to Amazon S3 buckets or Amazon CloudFront.

- **AWS IAM and API Gateway**—Manages customer trusted roles and proxy communication between the media service and the key server. API Gateway provides logging capabilities and lets customers control their relationships with the AWS Elemental media service and with the DRM system. Customers enable key server access through IAM role configuration.

- **DRM system key server**—Provides encryption keys to the AWS Elemental media services through a SPEKE-compliant API. Also provides licenses to media players for decryption.

How to Get Started

Are you a customer?
Partner with an AWS Elemental DRM solution provider to get set up to use encryption. For details, see *Customer Onboarding* (p. 3).

**Are you a DRM solution provider or a customer with your own key server?**

Expose a REST API for your key server in compliance with our AWS Elemental SPEKE specification. For details, see *SPEKE API Specification for DRM Solution Providers* (p. 5).
Customer Onboarding

Protect your content from unauthorized use by combining a digital rights management (DRM) system key server with your AWS Elemental media services and with your media players. Follow the steps in this chapter to get started using encryption with your AWS Elemental media services.

Step 1: Check Supported Technologies

The following tables show supported technologies. Verify that your streaming protocol and the DRM system that you want are available for your live or VOD service.

AWS Elemental MediaPackage: Streaming Protocol / DRM System Support Matrix

<table>
<thead>
<tr>
<th></th>
<th>Microsoft PlayReady</th>
<th>Google Widevine</th>
<th>Apple Fairplay</th>
<th>AES-128</th>
</tr>
</thead>
<tbody>
<tr>
<td>DASH</td>
<td>✓ with key rotation</td>
<td>✓ with key rotation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple HLS</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓ with key rotation</td>
</tr>
<tr>
<td>Microsoft Smooth</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

AWS Elemental MediaConvert: Streaming Protocol / DRM System Support Matrix

<table>
<thead>
<tr>
<th></th>
<th>Microsoft Playready</th>
<th>Google Widevine</th>
<th>Apple Fairplay</th>
<th>AES-128</th>
</tr>
</thead>
<tbody>
<tr>
<td>DASH</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple HLS</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Microsoft Smooth</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

Step 2: Get On Board with an AWS DRM Solution Provider

The following Amazon partners provide third-party DRM system implementations for AWS Elemental products. For details about each solution provider's offerings and information about how to contact them, follow the links to their Amazon Partner Network pages. The partners will help you get set up to use their solutions with AWS Elemental media services.

- BuyDRM
- Castlabs
- Conax AS
- EZDRM
- Irdeto
- Verimatrix
We use a standard key exchange protocol, which is documented in our Secure Packager and Encoder Key Exchange (SPEKE) Digital Rights Management (DRM) specification at SPEKE API Specification for DRM Solution Providers (p. 5). Our DRM solution providers have integrated with AWS Elemental media services by exposing a SPEKE-compliant REST API.
**SPEKE API Specification for DRM Solution Providers**

This is the REST API specification for AWS Elemental Secure Packager and Encoder Key Exchange (SPEKE). Use this specification to write a REST API for your digital rights management (DRM) system key server that is compatible with AWS Elemental MediaConvert and AWS Elemental MediaPackage.

In a video streaming workflow, the encryption engine communicates with the DRM system key store to request content keys. These keys are highly sensitive, so it is critical that the key store and encryption engine establish a highly secure, trusted communication channel.

This specification addresses the following goals:

- Define a simple, trusted, highly secure interface that DRM vendors and customers can use to integrate with AWS Elemental products when content encryption is required.
- Cover VOD and live workflows, and include the error conditions and the authentication mechanisms that are required for robust, highly secure communication between AWS Elemental products and DRM key server endpoints.
- Include support for HLS, MSS, and DASH packaging and their common DRM systems (Fairplay, PlayReady, and Widevine/CENC).
- Keep the specification simple and extensible, to support future DRM systems.
- Use a simple REST API.

**Architectural Overview**

SPEKE can be implemented for any DRM key server. The following illustration shows a typical architecture using a third-party key server.
• **AWS Elemental Account**—Provides the encryption technology. The service receives encryption requests from its operator and retrieves the required keys from the DRM key server, through Amazon API Gateway. It saves the encrypted content to Amazon S3 buckets or Amazon CloudFront.

• **Customer AWS Account**—Management of customer trusted roles in the AWS system and DRM key server and proxy communication between the media service and the key server. Customers enable key server access through IAM role configuration for their account. API Gateway provides logging capabilities and lets the customer control their relationships with the AWS Elemental service and with the DRM system.

• **DRM Partner Account**—Provides secure keys to the encryptor. Provides encryption keys to the AWS Elemental services through a SPEKE-compliant API. Provides secure licenses to media players for decryption on behalf of viewers.

The following illustration shows a typical architecture for a customer-implemented key server. In this case, the customer account and partner account are combined.

---

**Are You New to SPEKE?**

This section lists common SPEKE terminology and provides links to related services and specifications.

**Terminology**

• **ARN**—Amazon Resource Name. Uniquely identifies an AWS resource.

• **Content Key**—Cryptographic key used for encrypting part of the content.

• **Content Provider**—Publisher who provides the rights and rules for delivering protected media. The content provider might also provide source media (mezzanine format, for transcoding), asset identifiers, key identifiers (KID), key values, encoding instructions, and content description metadata.

• **Encryptor**—Video processing component (packaging stage as part of compressor or packager). For example, AWS Elemental MediaConvert and AWS Elemental MediaPackage.

• **Key Server**—Component of a DRM system that is used to provide keys to the encryptor.
**Operator** – Person in charge of operating the overall system, including the encryptor and the DRM system.

**Player** – Media player operating on behalf of a viewer. Gets its information from different sources, including the media manifest files, media files, and DRM licenses. Requests licenses from the DRM server on behalf of the viewers.

### Related Services and Specifications

- **AWS AssumeRole**
- **API Gateway Permissions**
- **AWS Sigv4**
- **DASH-IF CPIX specification**
- **DASH-IF System IDs**

### AWS Authentication for SPEKE

SPEKE requires AWS authentication through IAM roles. IAM roles are created by the DRM system service or by the operator who owns the DRM endpoint in an AWS account. Each role is assigned an Amazon Resource Name (ARN), which the AWS Elemental product operator provides in the service UI when requesting encryption. The role’s policy permissions must be configured to give permission to access the key server API and no other AWS resource access. When the encryptor contacts the DRM key server, it uses the role ARN to assume the role of the key server account holder, which returns temporary credentials for the encryptor to use to access the key server.

One common implementation involves the operator or DRM vendor using Amazon API Gateway in front of the key server, and then enabling AWS_IAM authorization on the API Gateway resource. You can use the following policy definition example and attach it to a new role to give permissions to the appropriate resource. In this case the permissions are for all API Gateway resources.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "execute-api:Invoke"
      ],
      "Resource": [
        "arn:aws:execute-api:us-west-2:*:*/*/GET/*"
      ]
    }
  ]
}
```

Finally, a trust relationship is added to the role and the properly named service is selectable by the operator.

The following example shows a role ARN that is created for accessing the key server:

```
arn:aws:iam::2949266363526:role/DRMKeyServer
```

For more information about the creation of a role, see [AWS AssumeRole](#). For more information about signing a request, see [AWS Sigv4](#).
SPEKE API

To work with AWS Elemental services, your key server must expose the REST API described in this specification. The encryptor makes requests to the API to exchange the payload with your key server.

SPEKE uses the DASH Industry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) data structure definition for key exchange. DASH-IF-CPIX defines a schema to provide an extensible, multi-DRM exchange from the DRM system to the encryptor. This enables content encryption for all adaptive bitrate packaging formats at the time of content compression and packaging. Adaptive bitrate packaging formats include HLS, DASH, and MSS.


The AWS Elemental SPEKE API payload response conforms to DASH-IF-CPIX with the following constraints and customizations:

- SPEKE follows the Encryptor Consumer workflow.
- SPEKE does not use the encrypted document feature. Instead, it relies on encryption at the transport layer, plus strong authentication.
- SPEKE requires the ContentKeyUsageRule filter, KeyPeriodFilter for rotating key workflows. SPEKE ignores all other ContentKeyUsageRules.
- SPEKE omits the UpdateHistoryItemList functionality. If the list is present in the response, SPEKE ignores it.
- SPEKE supports key rotation. SPEKE uses only the ContentKeyPeriod@index to track the key period.
- To support MSS Playready, SPEKE uses a custom parameter under the DRMSystem tag, speke:ProtectionHeader.
- For HLS packaging, if the URIExtXKey is present in the response, then it contains the full data to be added in the URI parameter of the EXT-X-KEY tag of an HLS playlist, with no further signaling requirement.
- For HLS playlist, under the DRMSystem tag, SPEKE provides the optional custom parameters speke:KeyFormat and speke:KeyFormatVersions, for the values of the KEYFORMAT and KEYFORMATVERSIONS parameters of the EXT-X-KEY tag.

The HLS IV always follows segment number unless explicitly specified by the operator.

- When requesting keys, the encryptor might use the optional @explicitIV attribute on the ContentKey element. The key server may respond with an IV using @explicitIV, even if the attribute is not included in the request.
- The encryptor creates the key identifier (KID). It does not change for a given content ID and key period. The key server must include the KID in the request document response.
- The key server might include a value for the Speke-User-Agent response header to identify itself for debugging purposes.
- SPEKE does not currently support multiple tracks or keys per content.

The AWS Elemental encryptor is always a client and always sends POSTs to the key server endpoint. The encryptor might send a periodic heartbeat request to ensure that the connection between the encryptor and the key server endpoint is healthy.

Live Workflow Method Calls

Request Syntax
POST https://{speke-compatible-server}/speke/v1.0/copyProtection

*Request Body*

A CPIX element.

*Request Headers*

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Occurs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization</td>
<td>String</td>
<td>1..1</td>
<td>See <a href="https://aws.amazon.com/blog">AWS Sigv4</a></td>
</tr>
<tr>
<td>X-Amz-Security-Token</td>
<td>String</td>
<td>1..1</td>
<td>See <a href="https://aws.amazon.com/blog">AWS Sigv4</a></td>
</tr>
<tr>
<td>X-Amz-Date</td>
<td>String</td>
<td>1..1</td>
<td>See <a href="https://aws.amazon.com/blog">AWS Sigv4</a></td>
</tr>
<tr>
<td>Content-Type</td>
<td>String</td>
<td>1..1</td>
<td>application/xml</td>
</tr>
</tbody>
</table>

*Response Headers*

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Occurs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speke-User-Agent</td>
<td>String</td>
<td>1..1</td>
<td>String that identifies the key server</td>
</tr>
<tr>
<td>Content-Type</td>
<td>String</td>
<td>1..1</td>
<td>application/xml</td>
</tr>
</tbody>
</table>

*Request Response*

<table>
<thead>
<tr>
<th>HTTP CODE</th>
<th>Payload Name</th>
<th>Occurs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 (Success)</td>
<td>CPIX</td>
<td>1..1</td>
<td>DASH-CPIX payload response</td>
</tr>
<tr>
<td>4XX (Client error)</td>
<td>Client error message</td>
<td>1..1</td>
<td>Description of the client error</td>
</tr>
<tr>
<td>5XX (Server error)</td>
<td>Server error message</td>
<td>1..1</td>
<td>Description of the server error</td>
</tr>
</tbody>
</table>

*Live Example Request*
Live Example Response
AWS Elemental Secure Packager and Encoder
Key Exchange API Specification Developer Guide
Live Workflow Method Calls
VOD Workflow Method Calls

Request Syntax

POST https://{speke-compatible-server}/speke/v1.0/copyProtection

Request Body

A CPIX element.

Response Headers

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Occurs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speke-User-Agent</td>
<td>String</td>
<td>1..1</td>
<td>String that identifies the key server</td>
</tr>
<tr>
<td>Content-Type</td>
<td>String</td>
<td>1..1</td>
<td>application/xml</td>
</tr>
</tbody>
</table>

Request Response

<table>
<thead>
<tr>
<th>HTTP CODE</th>
<th>Payload Name</th>
<th>Occurs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 (Success)</td>
<td>CPIX</td>
<td>1..1</td>
<td>DASH-CPIX payload response</td>
</tr>
<tr>
<td>4XX (Client error)</td>
<td>Client error message</td>
<td>1..1</td>
<td>Description of the client error</td>
</tr>
<tr>
<td>5XX (Server error)</td>
<td>Server error message</td>
<td>1..1</td>
<td>Description of the server error</td>
</tr>
</tbody>
</table>

VOD Example Request
VOD Example Response
Heartbeat

Request Syntax

GET https://{speke-compatible-server}/speke/v1.0/heartbeat
### Request Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Occurs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>speke-compatible-server</td>
<td>String</td>
<td>1..1</td>
<td>URL for a TLS-protected endpoint that supports the API defined in this document</td>
</tr>
</tbody>
</table>

### Request Response

<table>
<thead>
<tr>
<th>HTTP CODE</th>
<th>Payload Name</th>
<th>Occurs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 (Success)</td>
<td>statusMessage</td>
<td>1..1</td>
<td>Message that describes the status</td>
</tr>
</tbody>
</table>
Document History

The following table describes the documentation for this release of AWS Elemental SPEKE.

- **Latest documentation update:** November 27, 2017

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
</table>
AWS Glossary

For the latest AWS terminology, see the AWS Glossary in the AWS General Reference.