

Panduan mitra dan pelanggan

Spesifikasi API Pertukaran Kunci Pengemas dan Encoder Aman



Spesifikasi API Pertukaran Kunci Pengemas dan Encoder Aman: Panduan mitra dan pelanggan

Copyright © 2021 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara para pelanggan, atau dengan cara apa pun yang menghina atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan properti dari masing-masing pemilik, yang mungkin berafiliasi, terkait dengan, atau disponsori oleh Amazon, atau tidak.

Table of Contents

Apa itu Secure Packager dan Encoder Key Exchange?	1
Arsitektur umum	1
Arsitektur berbasis cloud AWS	2
Cara memulai	3
Apakah Anda baru mengenal SPEKE?	4
Layanan dan spesifikasi terkait	4
Terminologi	4
Orientasi pelanggan	6
Bergabunglah dengan penyedia platform DRM	6
Dukungan SPEKE dalam layanan dan produk AWS	7
Dukungan SPEKE dalam layanan dan produk AWS Partner	8
Spesifikasi SPEKE API	9
Autentikasi	10
Otentikasi untuk implementasi AWS cloud	10
Otentikasi untuk produk lokal	11
SPEKE API v1	12
SPEKE API v1 - Kustomisasi dan kendala untuk spesifikasi DASH-IF	13
SPEKE API v1 - Komponen muatan standar	14
SPEKE API v1 - Contoh panggilan metode alur kerja langsung	16
SPEKE API v1 - contoh panggilan metode alur kerja VOD	21
SPEKE API v1 - Enkripsi kunci konten	24
SPEKE API v1 - Detak Jantung	28
SPEKE API v1 - Mengganti pengenalan kunci	28
SPEKE API v2	30
SPEKE API v2 - Kustomisasi dan kendala untuk spesifikasi DASH-IF	31
SPEKE API v2 - Komponen muatan standar	35
SPEKE API v2 - Kontrak enkripsi	40
SPEKE API v2 - Contoh panggilan metode alur kerja langsung	50
SPEKE API v2 - contoh panggilan metode alur kerja VOD	56
SPEKE API v2 - Enkripsi kunci konten	62
SPEKE API v2 - Mengganti pengenalan kunci	65
Lisensi	67
Atribusi Creative Commons- ShareAlike 4.0 Lisensi Publik Internasional	67
Riwayat dokumen	74

Glosarium AWS	77
.....	lxxviii

Apa itu Secure Packager dan Encoder Key Exchange?

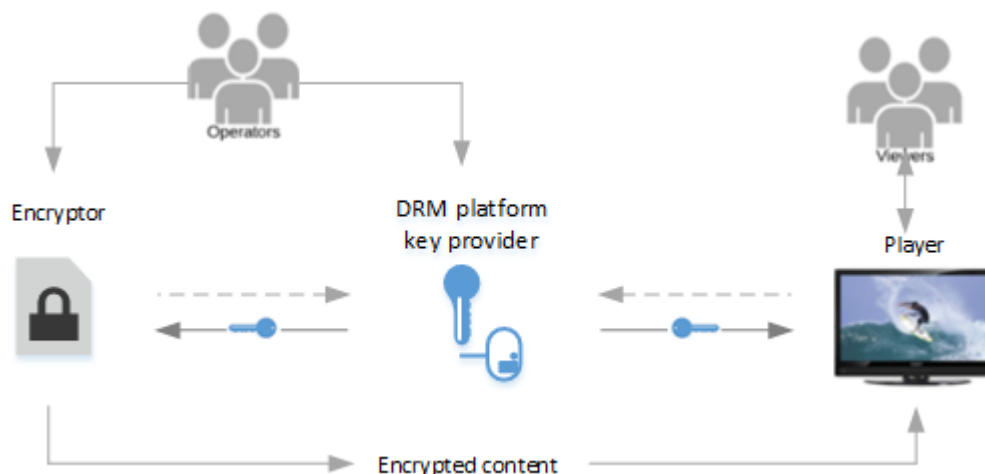
Secure Packager dan Encoder Key Exchange (SPEKE) mendefinisikan standar komunikasi antara enkripsi dan pembuat paket konten media dan penyedia kunci manajemen hak digital (DRM). Spesifikasi ini mengakomodasi enkripsi yang berjalan di lokasi dan di AWS Cloud.

Topik

- [Arsitektur umum](#)
- [Arsitektur berbasis cloud AWS](#)
- [Cara memulai](#)

Arsitektur umum

Ilustrasi berikut menunjukkan tampilan tingkat tinggi arsitektur enkripsi konten SPEKE untuk produk lokal.

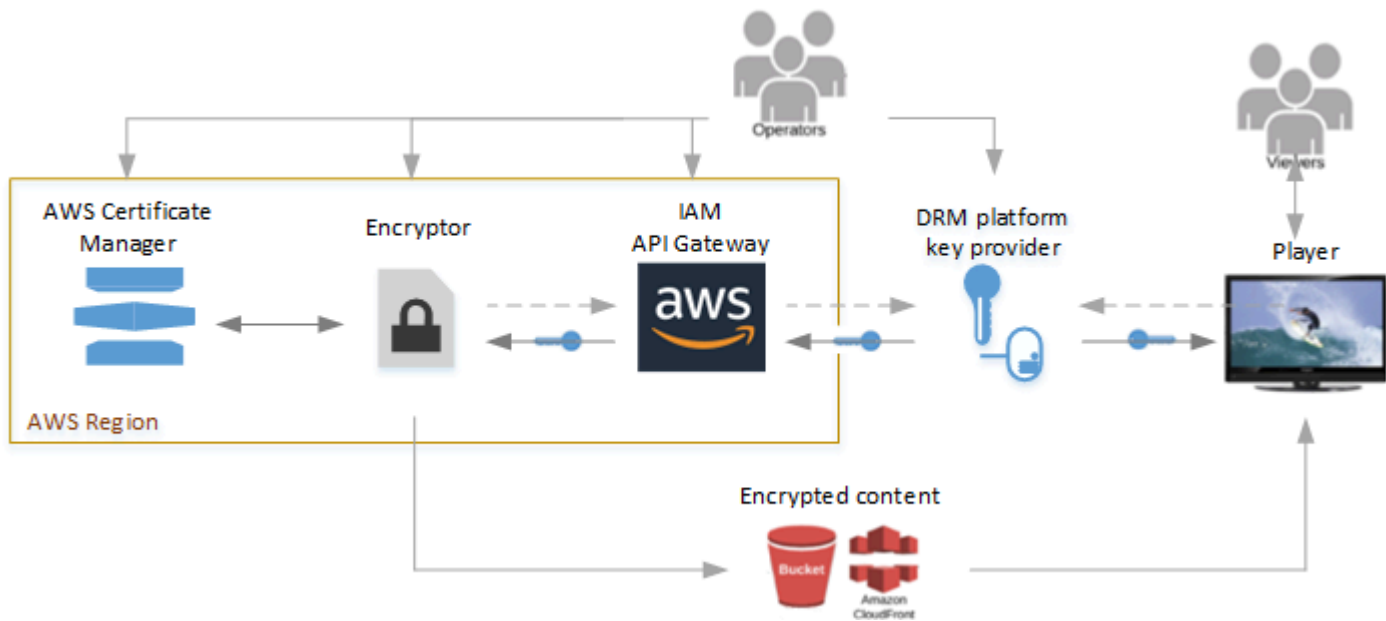


Ini adalah komponen utama dari arsitektur sebelumnya:

- Encryptor — Menyediakan teknologi enkripsi. Menerima permintaan enkripsi dari operatornya, dan mengambil kunci yang diperlukan dari penyedia kunci DRM untuk mengamankan konten terenkripsi.
- Penyedia kunci platform DRM — Menyediakan kunci enkripsi ke enkripsi melalui API yang sesuai dengan Speke. Penyedia juga memberikan lisensi kepada pemutar media untuk dekripsi.
- Pemain — Meminta kunci dari penyedia kunci platform DRM yang sama, yang digunakan pemain untuk membuka kunci konten dan menyajikannya kepada pemirsa.

Arsitektur berbasis cloud AWS

Ilustrasi berikut menunjukkan arsitektur tingkat tinggi ketika SPEKE digunakan dengan layanan dan fitur yang berjalan di AWS Cloud.



Ini adalah layanan dan komponen utama:

- **Encryptor** — Menyediakan teknologi enkripsi di AWS Cloud. Enkripsi menerima permintaan dari operatornya dan mengambil kunci enkripsi yang diperlukan dari penyedia kunci DRM, melalui Amazon API Gateway, untuk mengamankan konten terenkripsi. Ini mengirimkan konten terenkripsi ke ember Amazon S3 atau melalui distribusi Amazon. CloudFront
- **AWS IAM dan Amazon API Gateway** — Mengelola peran tepercaya pelanggan dan komunikasi proxy antara enkripsi dan penyedia kunci. API Gateway menyediakan kemampuan logging dan memungkinkan pelanggan mengontrol hubungan mereka dengan enkripsi dan dengan platform DRM. Pelanggan mengaktifkan akses penyedia kunci melalui konfigurasi peran IAM. API Gateway harus berada di Wilayah AWS yang sama dengan enkripsi.
- **AWS Certificate Manager** — (Opsional) Menyediakan manajemen sertifikat untuk enkripsi kunci konten. Mengenkripsi kunci konten adalah praktik yang disarankan untuk komunikasi yang aman. Manajer sertifikat harus berada di Wilayah AWS yang sama dengan enkripsi.
- **Penyedia kunci platform DRM** — Menyediakan kunci enkripsi ke enkripsi melalui API yang sesuai dengan Speke. Penyedia juga memberikan lisensi kepada pemutar media untuk dekripsi.
- **Pemain** — Meminta kunci dari penyedia kunci platform DRM yang sama, yang digunakan pemain untuk membuka kunci konten dan menyajikannya kepada pemirsa.

Cara memulai

Untuk materi pengantar tambahan tentang SPEKE, lihat [Apakah Anda baru mengenal SPEKE?](#) .

Apakah Anda seorang pelanggan?

Bermitra dengan penyedia platform AWS Elemental DRM untuk mengatur penggunaan enkripsi. Untuk detailnya, lihat [Orientasi pelanggan](#).

Apakah Anda penyedia platform DRM atau pelanggan dengan penyedia kunci Anda sendiri?

Paparkan REST API untuk penyedia kunci Anda sesuai dengan spesifikasi SPEKE. Untuk detailnya, lihat [spesifikasi SPEKE API](#).

Apakah Anda baru mengenal SPEKE?

Bagian ini menyediakan materi pengantar, untuk pembaca yang baru mengenal Secure Packager dan Encoder Key Exchange (SPEKE).

Untuk pengenalan SPEKE, tonton webcast berikut:

Layanan dan spesifikasi terkait

- Izin [gateway API — Cara mengontrol akses ke API dengan izin](#) AWS Identity and Access Management (AWS IAM).
- [AWS AssumeRole](#) — Cara menggunakan AWS Security Token Service (AWS STS) untuk menjalankan fungsionalitas peran.
- [AWS Sigv4](#) — Cara menandatangani permintaan HTTP menggunakan Signature Versi 4.
- Spesifikasi [DASH-IF CPIX v2.0 - Versi spesifikasi](#) DASH-IF Content Protection Information Exchange Format (CPIX), yang menjadi dasar spesifikasi SPEKE v1.0 ini.
- Spesifikasi [DASH-IF CPIX v2.3 - Versi spesifikasi](#) DASH-IF Content Protection Information Exchange Format (CPIX), yang menjadi dasar spesifikasi SPEKE v2.0 ini.
- [ID sistem DASH-IF](#) — Daftar pengidentifikasi terdaftar untuk sistem DRM.
- <https://github.com/awslabs/speke-reference-server> — Contoh penyedia kunci referensi untuk digunakan dengan akun AWS Anda, untuk membantu Anda memulai implementasi SPEKE di AWS.

Terminologi

Daftar berikut mendefinisikan terminologi yang digunakan dalam spesifikasi ini. Jika memungkinkan, spesifikasi ini mengikuti terminologi yang digunakan dalam spesifikasi [DASH-IF CPIX](#).

- ARN - Nama Sumber Daya Amazon. Mengidentifikasi sumber daya AWS secara unik.
- Content key — Kunci kriptografi yang digunakan untuk mengenkripsi bagian konten.
- Penyedia konten — Penerbit yang memberikan hak dan aturan untuk memberikan media yang dilindungi. Penyedia konten mungkin juga menyediakan media sumber (format mezzanine, untuk transcoding), pengidentifikasi aset, pengidentifikasi kunci (KID), nilai kunci, instruksi pengkodean, dan metadata deskripsi konten.

- DRM — Manajemen hak digital. Digunakan untuk melindungi konten digital berhak cipta dari akses yang tidak disetujui.
- Platform DRM — Sistem yang menyediakan fungsionalitas DRM dan dukungan untuk enkripsi konten dan pemirsa, termasuk menyediakan kunci DRM dan lisensi untuk enkripsi dan dekripsi konten.
- Penyedia DRM - Lihat platform DRM.
- Sistem DRM — Standar untuk implementasi DRM. Sistem DRM umum termasuk Apple FairPlay, Google Widevine, dan Microsoft. PlayReady Sistem DRM digunakan oleh penyedia konten untuk mengamankan konten digital untuk pengiriman ke pemirsa dan untuk akses oleh pemirsa. [Untuk daftar sistem DRM yang terdaftar dengan DASH-IF, lihat ID sistem DASH-IF. Spesifikasi DASH-IF CPIX](#) menggunakan istilah “sistem DRM” seperti yang didefinisikan di sini dan, di beberapa tempat, menggunakan “sistem DRM” untuk berarti apa yang disebut spesifikasi ini sebagai platform DRM.
- Solusi DRM - Lihat platform DRM.
- Teknologi DRM - Lihat sistem DRM.
- Encryptor — Komponen pemrosesan media yang mengenkripsi konten media menggunakan kunci yang diperoleh dari penyedia kunci. Enkripsi biasanya juga menambahkan sinyal enkripsi DRM dan metadata ke media. Enkripsi biasanya encoder, packagers, dan transcoder.
- Penyedia kunci — Komponen platform DRM yang mengekspos SPEKE REST API untuk menangani permintaan utama. Penyedia kunci mungkin server kunci itu sendiri, atau mungkin komponen lain dari platform.
- Server kunci — Komponen platform DRM yang memelihara kunci untuk enkripsi dan dekripsi konten.
- Operator — Seseorang yang bertanggung jawab untuk mengoperasikan sistem secara keseluruhan, termasuk enkripsi dan penyedia kunci.
- Player — Pemutar media yang beroperasi atas nama pemirsa. Mendapatkan informasinya dari berbagai sumber, termasuk file manifes media, file media, dan lisensi DRM. Meminta lisensi dari platform DRM atas nama pemirsa.

Orientasi pelanggan

Lindungi konten Anda dari penggunaan yang tidak sah dengan menggabungkan penyedia kunci manajemen hak digital (DRM) Secure Packager dan Encoder Key Exchange (SPEKE) dengan enkripsi Anda dan pemutar media Anda. SPEKE mendefinisikan standar untuk komunikasi antara enkripsi dan pengemas konten media dan penyedia kunci manajemen hak digital (DRM). Untuk onboard, Anda memilih penyedia kunci platform DRM dan mengonfigurasi komunikasi antara penyedia kunci dan enkripsi dan pemain Anda.

Topik

- [Bergabunglah dengan penyedia platform DRM](#)
- [Dukungan SPEKE dalam layanan dan produk AWS](#)
- [Dukungan SPEKE dalam layanan dan produk AWS Partner](#)

Bergabunglah dengan penyedia platform DRM

Mitra Amazon berikut menyediakan implementasi platform DRM pihak ketiga untuk SPEKE. Untuk detail tentang penawaran mereka dan informasi tentang cara menghubungi mereka, ikuti tautan ke halaman Jaringan Mitra Amazon mereka. Mitra yang tidak memiliki tautan saat ini tidak memiliki halaman Jaringan Mitra Amazon, tetapi Anda dapat menghubungi mereka secara langsung. Mitra dapat membantu Anda mengatur untuk menggunakan platform mereka.

Penyedia Platform DRM	Dukungan SPEKE v1	Dukungan SPEKE v2 (MediaPackageAWS Elemental)
Axinom	√	√
BuyDRM	√	√
CastLabs	√	√
EZDRM	√	√
Inisoft	√	√
INKA Entworks	√	√

Penyedia Platform DRM	Dukungan SPEKE v1	Dukungan SPEKE v2 (MediaPackageAWS Elemental)
DRM Awan Insys	√	√
Teknologi Intertrust	√	√
Irdeto	√	√
Pemain JW	√	√
Kaltura	√	
NAGRA	√	√
NEXTSCAPE, Inc.	√	√
SeaChange	√	
Verimatrix	√	√
Viaccess-Orca	√	
WebStream	√	

Dukungan SPEKE dalam layanan dan produk AWS

Bagian ini mencantumkan dukungan SPEKE yang disediakan oleh AWS Media Services yang berjalan di AWS Cloud dan produk media lokal AWS. Layanan dan produk ini adalah enkripsi dalam arsitektur enkripsi konten SPEKE. Verifikasi bahwa protokol streaming Anda dan sistem DRM yang Anda inginkan tersedia untuk layanan atau produk Anda.

Layanan atau Produk AWS	Dukungan SPEKE v1	Dukungan SPEKE v2	Teknologi DRM yang Didukung
AWS Elemental MediaConvert - Layanan yang	√		Dokumentasi

Layanan atau Produk AWS	Dukungan SPEKE v1	Dukungan SPEKE v2	Teknologi DRM yang Didukung
Berjalan di AWS Cloud			
AWS Elemental MediaPackage - Layanan yang Berjalan di AWS Cloud	√	√	Dokumentasi
AWS Elemental Live - Produk Lokal	√		Dokumentasi: MPEG-DASH/HLS
AWS Elemental Server - Produk Lokal	√		Dokumentasi

Dukungan SPEKE dalam layanan dan produk AWS Partner

Bagian ini mencantumkan dukungan SPEKE yang disediakan oleh layanan AWS Partner dan produk yang berjalan di AWS Cloud. Layanan dan produk ini adalah enkripsi dalam arsitektur enkripsi konten SPEKE. Verifikasi bahwa protokol streaming Anda dan sistem DRM yang Anda inginkan tersedia untuk layanan atau produk Anda.

Layanan atau Produk AWS	Dukungan SPEKE v1	Dukungan SPEKE v2	Teknologi DRM yang Didukung
Pengkodean Video Langsung Bitmovin	√		Dokumentasi
Pengkodean Video sesuai permintaan (VOD) Bitmovin	√		Dokumentasi

Spesifikasi SPEKE API

Ini adalah spesifikasi REST API untuk Secure Packager dan Encoder Key Exchange (SPEKE). Gunakan spesifikasi ini untuk memberikan perlindungan hak cipta DRM bagi pelanggan yang menggunakan enkripsi.

Dalam alur kerja streaming video, mesin enkripsi berkomunikasi dengan penyedia kunci platform DRM untuk meminta kunci konten. Kunci ini sangat sensitif, jadi sangat penting bahwa penyedia kunci dan mesin enkripsi membangun saluran komunikasi yang sangat aman dan tepercaya. Anda juga dapat mengenkripsi kunci konten dalam dokumen untuk end-to-end enkripsi yang lebih aman.

Spesifikasi ini membahas tujuan berikut:

- Tentukan antarmuka yang sederhana, tepercaya, dan sangat aman yang dapat digunakan vendor dan pelanggan DRM untuk berintegrasi dengan enkripsi saat enkripsi konten diperlukan.
- Cakup VOD dan alur kerja langsung, dan sertakan kondisi kesalahan dan mekanisme otentikasi yang diperlukan untuk komunikasi yang kuat dan sangat aman antara enkripsi dan titik akhir penyedia kunci DRM.
- Sertakan dukungan untuk kemasan HLS, MSS, dan DASH dan sistem DRM umum mereka: FairPlay PlayReady, dan WideVine/CENC.
- Jaga agar spesifikasi tetap sederhana dan dapat diperluas, untuk mendukung sistem DRM masa depan.
- Gunakan REST API sederhana.

Note

Hak Cipta 2021, Amazon Web Services, Inc. atau afiliasinya. Semua hak dilindungi undang-undang.

Dokumentasi tersedia di bawah Lisensi Internasional Creative Commons Attribution-ShareAlike 4.0.

MATERI YANG TERKANDUNG DI SINI DISEDIAKAN “SEBAGAIMANA ADANYA”, TANPA JAMINAN DALAM BENTUK APA PUN, TERSURAT MAUPUN TERSIRAT, TERMASUK TETAPI TIDAK TERBATAS PADA JAMINAN KELAYAKAN UNTUK DIPERJUALBELIKAN, KESESUAIAN UNTUK TUJUAN TERTENTU DAN NON-PELANGGARAN. DALAM HAL APA PUN PENULIS ATAU PEMEGANG HAK CIPTA MATERI INI TIDAK AKAN BERTANGGUNG JAWAB ATAS KLAIM, KERUSAKAN, ATAU TANGGUNG JAWAB LAINNYA, BAIK DALAM

TINDAKAN KONTRAK, KESALAHAN ATAU LAINNYA, YANG TIMBUL DARI, DI LUAR ATAU SEHUBUNGAN DENGAN MATERI INI ATAU PENGGUNAAN ATAU TRANSAKSI LAIN DARI MATERI INI.

Topik

- [Autentikasi](#)
- [SPEKE API v1](#)
- [SPEKE API v2](#)
- [Lisensi](#)

Autentikasi

SPEKE memerlukan otentikasi untuk produk lokal dan untuk layanan dan fitur yang berjalan di AWS Cloud.

Topik

- [Otentikasi untuk implementasi AWS cloud](#)
- [Otentikasi untuk produk lokal](#)

Otentikasi untuk implementasi AWS cloud

SPEKE memerlukan otentikasi AWS melalui peran IAM untuk digunakan dengan enkripsi. Peran IAM dibuat oleh penyedia DRM atau oleh operator yang memiliki titik akhir DRM di akun AWS. Setiap peran diberi Nama Sumber Daya Amazon (ARN), yang disediakan oleh operator layanan AWS Elemental di konsol layanan saat meminta enkripsi. Izin kebijakan peran harus dikonfigurasi untuk memberikan izin untuk mengakses API penyedia kunci dan tidak ada akses sumber daya AWS lainnya. Ketika enkripsi menghubungi penyedia kunci DRM, ia menggunakan peran ARN untuk mengambil peran pemegang akun penyedia kunci, yang mengembalikan kredensial sementara untuk enkripsi untuk digunakan untuk mengakses penyedia kunci.

Salah satu implementasi umum adalah operator atau vendor platform DRM menggunakan Amazon API Gateway di depan penyedia kunci, dan kemudian mengaktifkan otorisasi AWS Identity and Access Management (AWS IAM) pada sumber daya API Gateway. Anda dapat menggunakan contoh definisi kebijakan berikut dan melampirkannya ke peran baru untuk memberikan izin ke sumber daya yang sesuai. Dalam hal ini, izin tersebut untuk semua resource API Gateway:

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

Akhirnya, peran tersebut membutuhkan penambahan hubungan kepercayaan, dan operator harus dapat memilih layanan.

Contoh berikut menunjukkan peran ARN yang dibuat untuk mengakses penyedia kunci DRM:

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

Untuk informasi selengkapnya tentang pembuatan peran, lihat [AWS AssumeRole](#). Untuk informasi selengkapnya tentang menandatangani permintaan, lihat [AWS Sigv4](#).

Otentikasi untuk produk lokal

Untuk produk lokal, kami menyarankan Anda menggunakan SSL/TLS dan mencerna otentikasi untuk keamanan terbaik, tetapi setidaknya Anda harus menggunakan otentikasi dasar melalui HTTPS.

Kedua jenis otentikasi menggunakan `Authorization` header dalam permintaan HTTP:

- Autentikasi intisari - Header otorisasi terdiri dari pengenalan `Digest` diikuti oleh serangkaian nilai yang mengotentikasi permintaan. Secara khusus, nilai respons dihasilkan melalui serangkaian fungsi hash MD5 yang mencakup unik, one-time-use nonce dari server yang digunakan untuk memastikan bahwa kata sandi berjalan dengan aman.
- Otentikasi dasar - Header otorisasi terdiri dari pengenalan `Basic` diikuti oleh string yang dikodekan basis-64 yang mewakili nama pengguna dan kata sandi, dipisahkan oleh titik dua.

Untuk informasi tentang otentikasi dasar dan intisari, termasuk informasi rinci tentang header, lihat spesifikasi Internet Engineering Task Force (IETF) [RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication](#).

SPEKE API v1

Agar sesuai dengan Speke, penyedia kunci DRM Anda harus mengekspos REST API yang dijelaskan dalam spesifikasi ini. Enkripsi membuat panggilan API ke penyedia kunci Anda.

Note

Contoh kode dalam spesifikasi ini hanya untuk tujuan ilustrasi. Anda tidak dapat menjalankan contoh karena mereka bukan bagian dari implementasi SPEKE yang lengkap.

Secure Packager dan Encoder Key Exchange menggunakan definisi struktur data DASH Industry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) untuk pertukaran kunci, dengan beberapa batasan. DASH-IF-CPIX mendefinisikan skema untuk menyediakan pertukaran multi-DRM yang dapat diperluas dari platform DRM ke enkripsi. Ini memungkinkan enkripsi konten untuk semua format kemasan bitrate adaptif pada saat kompresi dan pengemasan konten. Format kemasan bitrate adaptif termasuk HLS, DASH, dan MSS.

[Untuk informasi rinci tentang format pertukaran, lihat spesifikasi DASH Industry Forum CPIX di https://dashif.org/docs/DASH-IF-CPIX-v2-0.pdf.](https://dashif.org/docs/DASH-IF-CPIX-v2-0.pdf)

Topik

- [SPEKE API v1 - Kustomisasi dan kendala untuk spesifikasi DASH-IF](#)
- [SPEKE API v1 - Komponen muatan standar](#)
- [SPEKE API v1 - Contoh panggilan metode alur kerja langsung](#)
- [SPEKE API v1 - contoh panggilan metode alur kerja VOD](#)
- [SPEKE API v1 - Enkripsi kunci konten](#)
- [SPEKE API v1 - Detak Jantung](#)
- [SPEKE API v1 - Mengganti pengenalan kunci](#)

SPEKE API v1 - Kustomisasi dan kendala untuk spesifikasi DASH-IF

Spesifikasi DASH-IF CPIX, <https://dashif.org/docs/DASH-IF-CPIX-v2-0.pdf>, mendukung sejumlah kasus penggunaan dan topologi. Spesifikasi SPEKE API mematuhi spesifikasi CPIX dengan penyesuaian dan kendala berikut:

- SPEKE mengikuti alur kerja Encryptor Consumer.
- Untuk kunci konten terenkripsi, SPEKE menerapkan batasan berikut:
 - SPEKE tidak mendukung verifikasi tanda tangan digital (XMLDSIG) untuk muatan permintaan atau respons.
 - SPEKE membutuhkan 2048 sertifikat berbasis RSA.
- Untuk memutar alur kerja kunci, SPEKE membutuhkan filter, `ContentKeyUsageRule` `KeyPeriodFilter` SPEKE mengabaikan semua pengaturan lainnya `ContentKeyUsageRule`.
- SPEKE menghilangkan fungsionalitas `UpdateHistoryItemList` Jika daftar hadir dalam tanggapan, SPEKE mengabaikannya.
- SPEKE mendukung rotasi kunci. SPEKE hanya menggunakan `ContentKeyPeriod@index` untuk melacak periode kunci.
- Untuk mendukung MSS PlayReady, SPEKE menggunakan parameter kustom di bawah `DRMSystem` tag, `SPEKE:ProtectionHeader`
- Untuk kemasan HLS, jika `URIExtXKey` ada dalam respons, maka harus berisi data lengkap untuk menambahkan parameter `URI EXT-X-KEY` tag daftar putar HLS, tanpa persyaratan pensinyalan lebih lanjut.
- Untuk daftar putar HLS, di bawah `DRMSystem` tag, SPEKE menyediakan parameter kustom opsional `speke:KeyFormat` dan `speke:KeyFormatVersions`, untuk nilai `KEYFORMAT` dan `KEYFORMATVERSIONS` parameter tag. `EXT-X-KEY`

Vektor inisialisasi HLS (IV) selalu mengikuti nomor segmen kecuali ditentukan secara eksplisit oleh operator.

- Saat meminta kunci, enkripsi mungkin menggunakan `@explicitIV` atribut opsional pada elemen `ContentKey` Penyedia kunci dapat merespons dengan menggunakan `IV@explicitIV`, bahkan jika atribut tidak termasuk dalam permintaan.
- Enkripsi membuat pengenal kunci (KID), yang tetap sama untuk setiap ID konten dan periode kunci tertentu. Penyedia kunci memasukkan KID dalam tanggapannya terhadap dokumen permintaan.

- Penyedia kunci mungkin menyertakan nilai untuk header `Speke-User-Agent` respons, untuk mengidentifikasi dirinya sendiri untuk tujuan debugging.
- SPEKE saat ini tidak mendukung beberapa trek atau kunci per konten.

Enkripsi yang sesuai dengan Speke bertindak sebagai klien dan mengirimkan POST operasi ke titik akhir penyedia kunci. Enkripsi mungkin mengirim heartbeat permintaan berkala untuk memastikan bahwa koneksi antara enkripsi dan titik akhir penyedia kunci sehat.

SPEKE API v1 - Komponen muatan standar

Dalam setiap permintaan SPEKE, enkripsi dapat meminta tanggapan untuk satu atau lebih sistem DRM. Enkripsi menentukan sistem DRM di payload permintaan `<cpix:DRMSystemList>`. Setiap spesifikasi sistem menyertakan kunci dan menunjukkan jenis respons untuk kembali.

Contoh berikut menunjukkan daftar sistem DRM dengan spesifikasi sistem DRM tunggal:

```
<cpix:DRMSystemList>
  <!-- HLS AES-128 (systemId is implementation specific)-->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
    systemId="81376844-f976-481e-a84e-cc25d39b0b33">
    <cpix:URIEExtXKey></cpix:URIEExtXKey>
    <speke:KeyFormat></speke:KeyFormat>
    <speke:KeyFormatVersions></speke:KeyFormatVersions>
  </cpix:DRMSystem>
</cpix:DRMSystemList>
```

Tabel berikut mencantumkan komponen utama masing-masing `<cpix:DRMSystem>`.

Pengidentifikasi	Deskripsi
systemId atau schemeId	Pengidentifikasi unik untuk tipe sistem DRM, seperti yang terdaftar di organisasi DASH IF. Untuk daftar, lihat ID Sistem DASH-IF .
kid	ID kunci. Ini bukan kunci yang sebenarnya, tetapi pengidentifikasi yang menunjuk ke kunci dalam tabel hash.

Pengidentifikasi	Deskripsi
<cpix:UriExtXKey>	Meminta kunci standar yang tidak terenkripsi. Jenis respons kunci harus berupa ini atau PSSH responsnya.
<cpix:PSSH>	Meminta Header Khusus Sistem Perlindungan (PSSH). Jenis header ini berisi referensi kekid,systemID, plus data kustom untuk vendor DRM, sebagai bagian dari Common Encryption (CENC). Jenis respons kunci harus berupa ini atau UriExtXKey responsnya.

_Contoh Permintaan untuk Kunci Standar dan untuk PSSH _

Contoh berikut menunjukkan bagian dari permintaan sampel dari enkripsi ke penyedia kunci DRM, dengan komponen utama disorot. Permintaan pertama adalah untuk kunci standar, sedangkan permintaan kedua adalah untuk respons PSSH:

```

<cpix:CPIX id="abc123" xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc" xmlns:speke="urn:aws:amazon:com:speke">
  <cpix:ContentKeyList>
    <cpix:ContentKey kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
      explicitIV="OFj2IjCsPJFfMAxmQxLGPw=="></cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- HLS AES-128 (systemId is implementation specific)-->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" ← KID
      systemId="81376844-f976-481e-a84e-cc25d39b0b33" ← System Id
      <cpix:UriExtXKey></cpix:UriExtXKey> ← request Key
      <speke:KeyFormat></speke:KeyFormat>
      <speke:KeyFormatVersions></speke:KeyFormatVersions>
    </cpix:DRMSystem>

    <!-- Common encryption (Widevine)-->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" ← KID
      systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed" ← System Id
      <cpix:PSSH></cpix:PSSH> ← request PSSH
    </cpix:DRMSystem>

  </cpix:DRMSystemList>
  ...
</cpix:CPIX>

```

_Contoh Respons untuk Kunci Standar dan untuk PSSH _

Contoh berikut menunjukkan respons yang sesuai dari penyedia kunci DRM ke enkripsi:

```

<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix" xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:speke="urn:aws:amazon:com:speke" id="abc123">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="OFj2IjCsPJFFmAxmQxLGPw=="
    kid="98ee5596-cd3e-a20d-163a-e382420c6eff">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- HLS AES-128 (systemId is implementation specific) -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" ← KID
    systemId="81376844-f976-481e-a84e-cc25d39b0b33" ← System Id
      <cpix:URIExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWNldGUtYXBpLnVzLXd1c3QtMi5hbWF6b25hd3M
uY29tL0VrZVN0YVdlL2NsaWVudC9hYmMxMjMvOThlZTU1OTYtY2QzZS1hMjBkLTE2M2EtZTM4MjQyMGM2ZWZ
m</cpix:URIExtXKey> ← Key
      <speke:KeyFormat>aWRlbnRpdHk=</speke:KeyFormat>
      <speke:KeyFormatVersions>MQ==</speke:KeyFormatVersions>
    </cpix:DRMSystem>

    <!-- Common encryption (Widevine) -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" ← KID
    systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed" ← System Id
      <cpix:PSSH>AAAAanBzc2gAAAAA7e+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd
2lkZXX2pbmVfdGVzdCIfa2V5LWlkOmVTSWNibGF0YmI3RGppNnNBdEtaelE9PSoCU0QyAA==</cpix:PSSH> ← PSSH
    </cpix:DRMSystem>
  </cpix:DRMSystemList>
  ...
</cpix:CPIX>

```

SPEKE API v1 - Contoh panggilan metode alur kerja langsung

Minta Contoh Sintaks

URL berikut adalah contoh dan tidak menunjukkan format tetap:

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

Permintaan Badan

Sebuah elemen CPIX.

Permintaan Header

Nama	Tipe	Terjadi	Deskripsi
AWS Authoriza tion	String	1.. 1	Lihat AWS Sigv4

Nama	Tipe	Terjadi	Deskripsi
X-Amz-Security-Token	String	1.. 1	Lihat AWS Sigv4
X-Amz-Date	String	1.. 1	Lihat AWS Sigv4
Content-Type	String	1.. 1	aplikasi/xml.

Header Respons

Nama	Tipe	Terjadi	Deskripsi
Speke-User-Agent	String	1.. 1	String yang mengidentifikasi penyedia kunci
Content-Type	String	1.. 1	aplikasi/xml.

Permintaan Respon

KODE HTTP	Nama Muatan	Terjadi	Deskripsi
200 (Success)	CPIX	1.. 1	Respons muatan DASH-CPIX
4XX (Client error)	Pesan kesalahan klien	1.. 1	Deskripsi kesalahan klien
5XX (Server error)	Pesan kesalahan server	1.. 1	Deskripsi kesalahan server

Note

Contoh di bagian ini tidak termasuk enkripsi kunci konten. Untuk informasi tentang cara menambahkan enkripsi kunci konten, lihat [Enkripsi kunci konten](#).

Contoh Langsung Minta Payload dengan Kunci di Clear

Contoh berikut menunjukkan payload permintaan langsung tipikal dari enkripsi ke penyedia kunci DRM:

```
<cpix:CPIX id="abc123" xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
  xmlns:speke="urn:aws:amazon:com:speke">
  <cpix:ContentKeyList>
    <cpix:ContentKey kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  explicitIV="0Fj2IjCsPJFFMAxmQxLGPw=="></cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- HLS AES-128 (systemId is implementation specific)-->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="81376844-
  f976-481e-a84e-cc25d39b0b33">
      <cpix:URIEExtXKey></cpix:URIEExtXKey>
      <speke:KeyFormat></speke:KeyFormat>
      <speke:KeyFormatVersions></speke:KeyFormatVersions>
    </cpix:DRMSystem>

    <!-- HLS SAMPLE-AES -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
      <cpix:URIEExtXKey></cpix:URIEExtXKey>
      <speke:KeyFormat></speke:KeyFormat>
      <speke:KeyFormatVersions></speke:KeyFormatVersions>
    </cpix:DRMSystem>

    <!-- Common encryption (Widevine)-->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
      <cpix:PSSH></cpix:PSSH>
    </cpix:DRMSystem>

    <!-- Common encryption / MSS (Playready) -->
```

```

<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
  <speke:ProtectionHeader></speke:ProtectionHeader>
  <cpix:PSSH></cpix:PSSH>
</cpix:DRMSystem>
</cpix:DRMSystemList>
<cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
</cpix:ContentKeyPeriodList>
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>

```

Muatan Respons Contoh Langsung dengan Kunci di Clear

Contoh berikut menunjukkan payload respons tipikal dari penyedia kunci DRM:

```

<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:speke="urn:aws:amazon:com:speke" id="abc123">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- HLS AES-128 (systemId is implementation specific) -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="81376844-
f976-481e-a84e-cc25d39b0b33">

    <cpix:URIExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVzLXd1c3Q0tMi5hbWF6b25hd3MuY29tL0V1Z
cpix:URIExtXKey>
    <speke:KeyFormat>aWR1bnRpdHk=</speke:KeyFormat>
    <speke:KeyFormatVersions>MQ==</speke:KeyFormatVersions>
  </cpix:DRMSystem>

```

```

<!-- HLS SAMPLE-AES -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">

<cpix:URIEExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZWN1dGUtYXBpLnVzLXd1c3QtMi5hbWF6b25hd3MuY29tL0VrZ
cpix:URIEExtXKey>
  <speke:KeyFormat>Y29tLmFwcGx1LnN0cmVhbWluZ2tleWRlbG12ZXJ5</speke:KeyFormat>
  <speke:KeyFormatVersions>MQ==</speke:KeyFormatVersions>
</cpix:DRMSystem>

<!-- Common encryption (Widevine) -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
  <cpix:PSSH>AAAAanBzc2gAAAAA7e
+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd2lkZXZpbmVfdGVzdCIfa2V5LWlk0mVTSWNibGF0Y
cpix:PSSH>
</cpix:DRMSystem>

<!-- Common encryption / MSS (Playready) -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">

<speke:ProtectionHeader>CgMAAAEAAQAAAzwAVwBSAE0ASABFAEEARABFAFIAIAB4AG0AbABuAHMAPQAIAGgAdAB0AH
+ADwAQQBMAEcASQBEAD4AQQBFAFMAQwBUAFIAPAAvAEEATABHAEKARAA
+ADwALwBQAFIATwBUAEUAQwBUAEkATgBGAE8APgA8AEsASQBEAD4ATwBXAGoAaAB0AHIAMwB1ADkAawArAHIAZABvADEASQ
+AGgAdAB0AHAA0gAvAC8ACABsAGEAeQByAGUAYQBkAHkALgBkAGkAcgB1AGMAdAB0AGEAcABzAC4AbgB1AHQALwBwAHIALw
+ADwALwBXAFIATQBIAEUAQQBEAEUAUgA+AA==</speke:ProtectionHeader>

<cpix:PSSH>AAADMHBzc2gAAAAAmgTweZhAQoarkuZb4Ihf1QAAAxAQAwAAAQABAAAYDPABXAFIATQBIAEUAQQBEAEUAUgA
+ADwASwBFAFkATABFAE4APgAxADYAPAAvAEsARQBZAEwARQBOAD4APABBAEwARwBJAEQAPgBBAEUAUwBDAFQAUgA8AC8AQ
+ADwASwBJAEQAPgBiAGgAdwBpAGUAWQAxAFcAdgBtADMARABqAGkANgBzAEEAdABLAFoAegBRAD0APQA8AC8ASwBJAEQAPg
+AGEAVABtAFAASgBWAEMAvgBaADYAcwA9ADwALwBDAEgARQBDAEsAUwBVAE0APgA8AEwAQQBFAFUUgBMAD4AaAB0AHQAca
+ADwALwBEAEEAVABBAD4APAAvAFcAUgBNAEgARQBBAEQARQBSAD4A</cpix:PSSH>
  </cpix:DRMSystem>
</cpix:DRMSystemList>
<cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
</cpix:ContentKeyPeriodList>
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
  </cpix:ContentKeyUsageRule>

```



```
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

SPEKE API v1 - contoh panggilan metode alur kerja VOD

Minta Contoh Sintaks

URL berikut adalah contoh dan tidak menunjukkan format tetap.

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

Permintaan Badan

Sebuah elemen CPIX.

Header Respons

Nama	Tipe	Terjadi	Deskripsi
Speke-User-Agent	String	1.. 1	String yang mengidentifikasi penyedia kunci
Content-Type	String	1.. 1	aplikasi/xml.

Permintaan Respon

KODE HTTP	Nama Muatan	Terjadi	Deskripsi
200 (Success)	CPIX	1.. 1	Respons muatan DASH-CPIX
4XX (Client error)	Pesan kesalahan klien	1.. 1	Deskripsi kesalahan klien
5XX (Server error)	Pesan kesalahan server	1.. 1	Deskripsi kesalahan server

Note

Contoh di bagian ini tidak termasuk enkripsi kunci konten. Untuk informasi tentang cara menambahkan enkripsi kunci konten, lihat [Enkripsi kunci konten](#).

Contoh VOD Minta Payload dengan Kunci di Clear

Contoh berikut menunjukkan payload permintaan VOD dasar dari enkripsi ke penyedia kunci DRM:

```
<cpix:CPIX id="abc123" xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:speke="urn:aws:amazon:com:speke">
<cpix:ContentKeyList>
  <cpix:ContentKey kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
explicitIV="0Fj2IjCsPJFfMAxmQxLGPw=="></cpix:ContentKey>
</cpix:ContentKeyList>
<cpix:DRMSystemList>
  <!-- HLS AES-128 (systemId is implementation specific)-->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="81376844-
f976-481e-a84e-cc25d39b0b33">
    <cpix:URIEExtXKey></cpix:URIEExtXKey>
    <speke:KeyFormat></speke:KeyFormat>
    <speke:KeyFormatVersions></speke:KeyFormatVersions>
  </cpix:DRMSystem>

  <!-- HLS SAMPLE-AES -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
    <cpix:URIEExtXKey></cpix:URIEExtXKey>
    <speke:KeyFormat></speke:KeyFormat>
    <speke:KeyFormatVersions></speke:KeyFormatVersions>
  </cpix:DRMSystem>

  <!-- Common encryption (Widevine)-->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
    <cpix:PSSH></cpix:PSSH>
  </cpix:DRMSystem>

  <!-- Common encryption / MSS (Playready) -->
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
```

```

<speke:ProtectionHeader></speke:ProtectionHeader>
<cpix:PSSH></cpix:PSSH>
</cpix:DRMSystem>
</cpix:DRMSystemList>
</cpix:CPIX>

```

VOD Contoh Respons Payload dengan Keys di Clear

Contoh berikut menunjukkan payload respons VOD dasar dari penyedia kunci DRM:

```

<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
  xmlns:speke="urn:aws:amazon:com:speke" id="abc123">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- HLS AES-128 (systemId is implementation specific) -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff" systemId="81376844-
f976-481e-a84e-cc25d39b0b33">

      <cpix:URIEExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZW1dGUtYXBpLnVzLXd1c3Q0tMi5hbWF6b25hd3MuY29tL0VrZ
cpix:URIEExtXKey>
      <speke:KeyFormat>aWR1bnRpdHk=</speke:KeyFormat>
      <speke:KeyFormatVersions>MQ==</speke:KeyFormatVersions>
    </cpix:DRMSystem>

    <!-- HLS SAMPLE-AES -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">

      <cpix:URIEExtXKey>aHR0cHM6Ly83azR5dHV4cTVkLmV4ZW1dGUtYXBpLnVzLXd1c3Q0tMi5hbWF6b25hd3MuY29tL0VrZ
cpix:URIEExtXKey>
      <speke:KeyFormat>Y29tLmFwcGx1LnN0cmVhbWluZ2tleWR1bG12ZXJ5</speke:KeyFormat>
      <speke:KeyFormatVersions>MQ==</speke:KeyFormatVersions>
    </cpix:DRMSystem>

```

```

<!-- Common encryption (Widevine) -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
  <cpix:PSSH>AAAAAnBzc2gAAAAA7e
+LqXnWSS6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd2lkZXZpbmVfdGVzdCIfa2V5LWlk0mVTSWNibGF0Y
cpix:PSSH>
</cpix:DRMSystem>

<!-- Common encryption / MSS (Playready) -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">

<speke:ProtectionHeader>CgMAAAEAAQAAAzwAVwBSAE0ASABFAEEARABFAFIAIAB4AG0AbABuAHMAPQAIAGgAdAB0AH
+ADwAQQBMAEcASQBEAD4AQQBFAFMAQwBUAFIAPAAvAEEATABHAEkARAA
+ADwALwBQAFIATwBUAEUAQwBUAEkATgBGAE8APgA8AEsASQBEAD4ATwBXAGoAaAB0AHIAMwB1ADkAawArAHIAZABvADEASQ
+AGgAdAB0AHAA0gAvAC8ACABsAGEAeQByAGUAYQBkAHkALgBkAGkAcgBlAGMAdAB0AGEACABzAC4AbgBlAHQALwBwAHIALw
+ADwALwBXAFIATQBIAEUAQQBEAEUAUGA+AA==</speke:ProtectionHeader>

  <cpix:PSSH>AAADMHBzc2gAAAAAmgTweZhAQoarkuZb4Ihf1QAAAxAQAwAAAQABAAYDPABXAFIATQBIAEUAQQBEAEUAUGA
+ADwASwBFAFKATABFAE4APgAxADYAPAAvAEsARQBZAeWArQB0AD4APABBAEwArwBJAEQAPgBBAEUAUwBDAFQAUGA8AC8AQ
+ADwASwBJAEQAPgBiAGgAdwBpAGUAWQAxAFcAdgBtADMARABqAGkAngBzAEEAdABLAFoAegBRAD0APQA8AC8ASwBJAEQAPg
+AGEAVABtAFAASgBWAEMAvgBaADYAcwA9ADwALwBDAEgARQBDAEsAUwBVAE0APgA8AEwAQQBFAFUUGBMAD4AaAB0AHQAC
+ADwALwBEAEEAVABBAD4APAAvAFcAUgBNAEgARQBBAEQARQBSAD4A</cpix:PSSH>
  </cpix:DRMSystem>
</cpix:DRMSystemList>
</cpix:CPIX>

```

SPEKE API v1 - Enkripsi kunci konten

Anda dapat menambahkan enkripsi kunci konten secara opsional ke implementasi SPEKE Anda. Enkripsi kunci konten menjamin end-to-end perlindungan penuh dengan mengenkripsi kunci konten untuk transit, selain mengenkripsi konten itu sendiri. Jika Anda tidak menerapkan ini untuk penyedia kunci Anda, Anda mengandalkan enkripsi lapisan transport ditambah otentikasi yang kuat untuk keamanan.

Untuk menggunakan enkripsi kunci konten untuk enkripsi yang berjalan di AWS Cloud, pelanggan mengimpor sertifikat ke AWS Certificate Manager dan kemudian menggunakan ARN sertifikat yang dihasilkan untuk aktivitas enkripsi mereka. Enkripsi menggunakan ARN sertifikat dan layanan ACM untuk menyediakan kunci konten terenkripsi ke penyedia kunci DRM.

Pembatasan

SPEKE mendukung enkripsi kunci konten sebagaimana ditentukan dalam spesifikasi DASH-IF CPIX dengan batasan berikut:

- SPEKE tidak mendukung verifikasi tanda tangan digital (XMLDSIG) untuk muatan permintaan atau respons.
- SPEKE membutuhkan 2048 sertifikat berbasis RSA.

Pembatasan ini juga tercantum dalam [Kustomisasi dan kendala](#) untuk spesifikasi DASH-IF.

Menerapkan enkripsi kunci konten

Untuk menyediakan enkripsi kunci konten, sertakan yang berikut ini dalam implementasi penyedia kunci DRM Anda:

- Tangani elemen `<cpix:DeliveryDataList>` dalam permintaan dan muatan respons.
- Berikan nilai terenkripsi dalam `<cpix:ContentKeyList>` muatan respons.

Untuk informasi selengkapnya tentang elemen-elemen ini, lihat spesifikasi [DASH-IF CPIX 2.0](#).

Contoh Elemen Enkripsi Kunci Konten `<cpix:DeliveryDataList>` di Muatan Permintaan

Contoh berikut menyoroti `<cpix:DeliveryDataList>` elemen yang ditambahkan dalam huruf tebal:

```
<?xml version="1.0" encoding="UTF-8"?>
<cpix:CPIX id="example-test-doc-encryption"
  xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
  xmlns:speke="urn:aws:amazon:com:speke">
  <cpix:DeliveryDataList>
    <cpix:DeliveryData id="<ORIGIN SERVER ID>">
      <cpix:DeliveryKey>
        <ds:X509Data>
          <ds:X509Certificate><X.509 CERTIFICATE, BASE-64 ENCODED></
ds:X509Certificate>
        </ds:X509Data>
      </cpix:DeliveryKey>
    </cpix:DeliveryData>
  </cpix:DeliveryDataList>
  <cpix:ContentKeyList>
```

```

...
</cpix:ContentKeyList>
</cpix:CPIX>

```

Contoh Elemen Enkripsi Kunci Konten <cpix:DeliveryDataList> di Payload Respons

Contoh berikut menyoroti <cpix:DeliveryDataList> elemen yang ditambahkan dalam huruf tebal:

```

<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix"
  xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
  xmlns:speke="urn:aws:amazon:com:speke" id="hls_test_001">
  <cpix:DeliveryDataList>
    <cpix:DeliveryData id="<ORIGIN SERVER ID>">
      <cpix:DeliveryKey>
        <ds:X509Data>
          <ds:X509Certificate><X.509 CERTIFICATE, BASE-64 ENCODED></
ds:X509Certificate>
        </ds:X509Data>
      </cpix:DeliveryKey>
      <cpix:DocumentKey Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc">
        <cpix>Data>
          <pskc:Secret>
            <pskc:EncryptedValue>
              <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#rsa-oaep-mgf1p" />
              <enc:CipherData>
                <enc:CipherValue><RSA CIPHER VALUE></enc:CipherValue>
              </enc:CipherData>
            </pskc:EncryptedValue>
            <pskc:ValueMAC>qnei/5TsfUwDu+8bhsZrLjDRDngvmnUZD2eva7SfXWw=</
pskc:ValueMAC>
          </pskc:Secret>
        </cpix>Data>
      </cpix:DocumentKey>
      <cpix:MACMethod Algorithm="http://www.w3.org/2001/04/xmlldsig-more#hmac-
sha512">
        <cpix:Key>
          <pskc:EncryptedValue>
            <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#rsa-oaep-mgf1p" />
          <enc:CipherData>

```

```

                <enc:CipherValue><RSA CIPHER VALUE></enc:CipherValue>
            </enc:CipherData>
        </pskc:EncryptedValue>
        <pskc:ValueMAC>DGqdpHUfFKxds09+EWrPjtdTCVfjPLwwtzEcFC/j0xY=</
pskc:ValueMAC>
            </cpix:Key>
        </cpix:MACMethod>
    </cpix:DeliveryData>
</cpix:DeliveryDataList>
<cpix:ContentKeyList>
    ...
</cpix:ContentKeyList>
</cpix:CPIX>

```

Contoh Elemen Enkripsi Kunci Konten <cpix:ContentKeyList> di Payload Respons

Contoh berikut menunjukkan penanganan kunci konten terenkripsi dalam <cpix:ContentKeyList> elemen payload respons. Ini menggunakan <pskc:EncryptedValue> elemen:

```

<cpix:ContentKeyList>
  <cpix:ContentKey kid="682681c8-69fa-4434-9f9f-1a7f5389ec02">
    <cpix:Data>
      <pskc:Secret>
        <pskc:EncryptedValue>
          <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#aes256-cbc" />
          <enc:CipherData>
            <enc:CipherValue>NJYebfvJ2TdMm3k6v
+rLNVYb0NoTJoTLBdbpe8nmilEfp82SKa7MkqTn2lmQBPB</enc:CipherValue>
          </enc:CipherData>
        </pskc:EncryptedValue>
        <pskc:ValueMAC>t9lW4WCebfS1GP+dh0IicMs+2+jnrAmfDa4WU6VGHc4=</
pskc:ValueMAC>
      </pskc:Secret>
    </cpix:Data>
  </cpix:ContentKey>
</cpix:ContentKeyList>

```

Sebagai perbandingan, contoh berikut menunjukkan muatan respons serupa dengan kunci konten yang dikirimkan tanpa enkripsi, sebagai kunci yang jelas. Ini menggunakan <pskc:PlainValue> elemen:

```

<cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw=="
kid="682681c8-69fa-4434-9f9f-1a7f5389ec02">
    <cpix:Data>
      <pskc:Secret>
        <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
      </pskc:Secret>
    </cpix:Data>
  </cpix:ContentKey>
</cpix:ContentKeyList>

```

SPEKE API v1 - Detak Jantung

Minta Contoh Sintaks

URL berikut adalah contoh dan tidak menunjukkan format tetap:

```
GET https://speke-compatible-server/speke/v1.0/heartbeat
```

Permintaan Respon

KODE HTTP	Nama Muatan	Terjadi	Deskripsi
200 (Success)	StatusPesan	1.. 1	Pesan yang menggambarkan status

SPEKE API v1 - Mengganti pengenalan kunci

Enkripsi membuat pengenalan kunci baru (KID) setiap kali memutar kunci. Ini meneruskan KID ke penyedia kunci DRM dalam permintaannya. Hampir selalu, penyedia kunci merespons menggunakan KID yang sama, tetapi dapat memberikan nilai yang berbeda untuk KID dalam tanggapannya.

Berikut ini adalah contoh permintaan dengan KID11111111-1111-1111-1111-111111111111:

```

<cpix:CPIX id="abc123" xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:speke="urn:aws:amazon:com:speke">
  <cpix:ContentKeyList>

```



```

    <cpix:ContentKey kid="11111111-1111-1111-1111-111111111111"></cpix:ContentKey>
</cpix:ContentKeyList>
<cpix:DRMSystemList>
  <!-- Common encryption (Widevine)-->
  <cpix:DRMSystem kid="11111111-1111-1111-1111-111111111111"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
    <cpix:PSSH />
  </cpix:DRMSystem>
</cpix:DRMSystemList>
<cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
</cpix:ContentKeyPeriodList>
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="11111111-1111-1111-1111-111111111111">
    <cpix:KeyPeriodFilter
periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>

```

Tanggapan berikut mengesampingkan KID ke: 22222222-2222-2222-2222-222222222222

```

<cpix:CPIX xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc"
xmlns:speke="urn:aws:amazon:com:speke" id="abc123">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="ASgwx9pQ2/2lnDzJsUxWcQ=="
kid="22222222-2222-2222-2222-222222222222">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>p3dWaHARtL97MpT7TE916w==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <cpix:DRMSystem kid="22222222-2222-2222-2222-222222222222"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
      <cpix:PSSH>AAAAanBzc2gAAAAA7e
+LqXnWSs6jyCfc1R0h7QAAAEoIARIQeSIcblaNbb7Dji6sAtKZzRoNd2lkZXZpbmVfdGVzdCIfa2V5LWlkOmVTSWNibGFOY
cpix:PSSH>
    </cpix:DRMSystem>

```

```
</cpix:DRMSystemList>
<cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
</cpix:ContentKeyPeriodList>
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="22222222-2222-2222-2222-222222222222">
    <cpix:KeyPeriodFilter
periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

SPEKE API v2

Agar sesuai dengan Speke, penyedia kunci DRM Anda harus mengekspos REST API yang dijelaskan dalam spesifikasi ini. Enkripsi membuat panggilan API ke penyedia kunci Anda.

Note

Contoh kode dalam spesifikasi ini hanya untuk tujuan ilustrasi. Anda tidak dapat menjalankan contoh karena mereka bukan bagian dari implementasi SPEKE yang lengkap.

Secure Packager dan Encoder Key Exchange menggunakan definisi struktur data DASH Industry Forum Content Protection Information Exchange Format (DASH-IF-CPIX) untuk pertukaran kunci, dengan beberapa batasan. DASH-IF-CPIX mendefinisikan skema untuk menyediakan pertukaran multi-DRM yang dapat diperluas dari platform DRM ke enkripsi. Ini memungkinkan enkripsi konten untuk semua format kemasan bitrate adaptif pada saat kompresi dan pengemasan konten. Format kemasan bitrate adaptif termasuk HLS, DASH, dan MSS.

Dimulai dengan versi 2.0-nya, SPEKE disejajarkan pada versi CPIX tertentu:

Di sisi SPEKE, ini diberlakukan melalui penggunaan header `X-Speke-Version` HTTP, dan di sisi CPIX melalui penggunaan atribut `CPIX@version`. Kurangnya elemen-elemen ini dalam permintaan adalah tipikal alur kerja lama SPEKE v1. Dalam alur kerja SPEKE v2, penyedia kunci diharapkan untuk memproses dokumen CPIX hanya jika mendukung kedua parameter versi.

Untuk informasi rinci tentang format pertukaran, lihat spesifikasi DASH Industry Forum [CPIX 2.3](#).

Secara keseluruhan, SPEKE v2.0 membawa evolusi berikut dibandingkan dengan SPEKE v1.0:

- Semua tag dari namespace SPEKE XHTML tidak digunakan lagi demi tag yang setara di namespace CPIX XHTML
- `SPEKE:ProtectionHeader` tidak digunakan lagi dan diganti dengan `CPIX:DRMSystem.SmoothStreamingProtectionHeaderData`
- `CPIX:URIExtXKey`, `SPEKE:KeyFormat` dan `SPEKE:KeyFormatVersions` tidak digunakan lagi dan diganti dengan `CPIX:DRMSystem.HLSSignalingData`
- `CPIX@id` digantikan oleh `CPIX@contentId`
- Atribut CPIX wajib baru: `CPIX@version ContentKey@commonEncryptionScheme`
- Elemen CPIX opsional baru: `DRMSystem.ContentProtectionData`
- Support untuk beberapa kunci konten
- Mekanisme cross-versioning antara SPEKE dan CPIX
- Evolusi header HTTP: `X-Speke-Version` header baru, `Speke-User-Agent` header diganti namanya menjadi `X-Speke-User-Agent`
- penghentian API detak jantung

Karena spesifikasi SPEKE v1.0 tetap tidak berubah, implementasi yang ada tidak perlu diubah untuk terus mendukung alur kerja SPEKE v1.0.

Topik

- [SPEKE API v2 - Kustomisasi dan kendala untuk spesifikasi DASH-IF](#)
- [SPEKE API v2 - Komponen muatan standar](#)
- [SPEKE API v2 - Kontrak enkripsi](#)
- [SPEKE API v2 - Contoh panggilan metode alur kerja langsung](#)
- [SPEKE API v2 - contoh panggilan metode alur kerja VOD](#)
- [SPEKE API v2 - Enkripsi kunci konten](#)
- [SPEKE API v2 - Mengganti pengenalan kunci](#)

SPEKE API v2 - Kustomisasi dan kendala untuk spesifikasi DASH-IF

[Spesifikasi DASH Industry Forum CPIX 2.3](#) mendukung sejumlah kasus penggunaan dan topologi. Spesifikasi SPEKE API v2.0 mendefinisikan Profil CPIX dan API untuk CPIX. Untuk mencapai dua tujuan ini, ia mematuhi spesifikasi CPIX dengan penyesuaian dan kendala berikut:

Profil CPIX

- SPEKE mengikuti alur kerja Encryptor Consumer.
- Untuk kunci konten terenkripsi, SPEKE menerapkan batasan berikut:
 - SPEKE tidak mendukung verifikasi tanda tangan digital (XMLDSIG) untuk muatan permintaan atau respons.
 - SPEKE membutuhkan 2048 sertifikat berbasis RSA.
- SPEKE hanya memanfaatkan sebagian dari fungsionalitas CPIX:
 - SPEKE menghilangkan fungsionalitas `UpdateHistoryItemList` jika daftar hadir dalam tanggapan, SPEKE mengabaikannya.
 - SPEKE menghilangkan fungsionalitas kunci akar/daun. Jika `ContentKey@dependsOnKey` atribut hadir dalam respons, SPEKE mengabaikannya.
 - SPEKE menghilangkan `BitrateFilter` elemen dan atribut `VideoFilter@wgc` jika elemen atau atribut ini ada dalam muatan CPIX, SPEKE mengabaikannya.
- Hanya elemen atau atribut yang dirujuk sebagai 'Didukung' pada [halaman Komponen Muatan Standar atau halaman kontrak Enkripsi](#) yang dapat digunakan dalam dokumen CPIX yang dipertukarkan dengan SPEKE v2.
- Ketika disertakan dalam permintaan CPIX oleh enkripsi, semua elemen dan atribut harus membawa nilai yang valid dalam respons CPIX penyedia kunci. Jika tidak, enkripsi akan berhenti dan melempar kesalahan.
- SPEKE mendukung rotasi kunci dengan `KeyPeriodFilter` elemen. SPEKE hanya menggunakan `ContentKeyPeriod@index` untuk melacak periode kunci.
- Untuk pensinyalan HLS, beberapa `DRMSystem.HLSSignalingData` elemen harus digunakan: satu dengan nilai `DRMSystem.HLSSignalingData@playlist` atribut 'media', dan satu lagi dengan nilai `DRMSystem.HLSSignalingData@playlist` atribut 'master'.
- Saat meminta kunci, enkripsi mungkin menggunakan `@explicitIV` atribut opsional pada elemen `ContentKey`. Penyedia kunci dapat merespons dengan menggunakan `IV@explicitIV`, bahkan jika atribut tidak termasuk dalam permintaan.
- Enkripsi membuat pengenalan kunci (KID), yang tetap sama untuk setiap ID konten dan periode kunci tertentu. Penyedia kunci memasukkan KID dalam tanggapannya terhadap dokumen permintaan.
- Enkripsi harus menyertakan nilai untuk atribut `CPIX@contentId`. Saat menerima nilai kosong untuk atribut ini, penyedia kunci akan mengembalikan kesalahan dengan deskripsi 'Missing CPIX @contentId'. `CPIX@contentId` nilai tidak dapat diganti oleh penyedia kunci.

`CPIX@id` nilai, jika tidak null, akan diabaikan oleh penyedia kunci.

- Enkripsi harus menyertakan nilai untuk atribut. `CPIX@version` Saat menerima nilai kosong untuk atribut ini, penyedia kunci akan mengembalikan kesalahan dengan deskripsi 'Missing CPIX @version '. Saat menerima permintaan dengan versi yang tidak didukung, deskripsi kesalahan yang dikembalikan oleh penyedia kunci adalah 'CPIX @version Tidak Didukung '.

`CPIX@version` nilai tidak dapat diganti oleh penyedia kunci.

- Enkripsi harus menyertakan nilai untuk `ContentKey@commonEncryptionScheme` atribut untuk setiap kunci yang diminta. Saat menerima nilai kosong untuk atribut ini, penyedia kunci akan mengembalikan kesalahan dengan deskripsi 'Missing ContentKey @ commonEncryptionScheme for id KID'.

Dokumen CPIX unik tidak dapat mencampur beberapa nilai untuk atribut yang berbeda `ContentKey@commonEncryptionScheme`. Saat menerima kombinasi seperti itu, penyedia kunci akan mengembalikan kesalahan dengan deskripsi 'Non compliant ContentKey @ commonEncryptionScheme combination'.

Tidak semua `ContentKey@commonEncryptionScheme` nilai kompatibel dengan semua teknologi DRM. Saat menerima kombinasi seperti itu, penyedia kunci akan mengembalikan kesalahan dengan deskripsi 'ContentKey@ commonEncryptionScheme tidak kompatibel dengan DRMSystemid'.

`ContentKey@commonEncryptionScheme` nilai tidak dapat diganti oleh penyedia kunci.

- Saat menerima nilai yang berbeda untuk `DRMSystem@PSSH` dan `<pssh>` elemen `DRMSystem.ContentProtectionData` innerXML di badan respons CPIX, enkripsi akan berhenti dan menimbulkan kesalahan.

API untuk CPIX

- Penyedia kunci harus menyertakan nilai untuk header respons `X-Speke-User-Agent` HTTP.
- Sebuah enkripsi Speke-compliant bertindak sebagai klien dan mengirimkan operasi POST ke endpoint penyedia kunci.
- Enkripsi harus menyertakan nilai untuk header permintaan `X-Speke-Version` HTTP, dengan versi SPEKE yang digunakan dengan permintaan, dirumuskan sebagai. `MajorVersion` `MinorVersion`, seperti '2.0' untuk SPEKE v2.0. Jika penyedia kunci tidak mendukung versi SPEKE yang digunakan oleh enkripsi untuk permintaan saat ini, penyedia kunci akan mengembalikan

kesalahan dengan deskripsi 'Versi SPEKE Tidak Didukung' dan tidak mencoba memproses dokumen CPIX dengan upaya terbaik.

Nilai `X-Speke-Version` header yang ditentukan oleh enkripsi tidak dapat dimodifikasi oleh penyedia kunci dalam menanggapi permintaan.

- Saat menerima kesalahan di badan respons, enkripsi akan melempar kesalahan dan tidak mencoba lagi permintaan dengan versi SPEKE v1.0.

Jika penyedia kunci tidak mengembalikan kesalahan tetapi gagal mengembalikan dokumen CPIX yang menyertakan informasi wajib, enkripsi harus berhenti dan menimbulkan kesalahan.

Tabel berikut merangkum pesan standar yang harus dikembalikan oleh penyedia kunci di badan pesan. Kode respons HTTP dalam kasus kesalahan harus berupa 4XX atau 5XX, tidak pernah 200. Kode kesalahan 422 dapat digunakan untuk semua kesalahan yang terkait dengan SPEKE/CPIX.

Kasus kesalahan	Pesan kesalahan
CPIX @contentId tidak ditentukan	CPIX @contentId tidak ada
CPIX @version tidak ditentukan	CPIX @version tidak ada
CPIX @version tidak didukung	CPIX @version tidak didukung
ContentKey@ commonEncryptionScheme tidak didefinisikan	Hilang ContentKey @ commonEncryptionScheme untuk KID id (di mana id sama dengan nilai ContentKey @kid)
Beberapa commonEncryptionScheme nilai ContentKey @ yang digunakan dalam satu dokumen CPIX	Kombinasi ContentKey @ commonEncryptionScheme yang tidak sesuai
ContentKey@ commonEncryptionScheme tidak kompatibel dengan teknologi DRM	ContentKey@ commonEncryptionScheme tidak kompatibel dengan DRMsystem id (di mana id sama dengan nilai DRMsystem @systemId)
Nilai header X-Speke-Version bukan versi SPEKE yang didukung	Versi SPEKE yang tidak didukung
Kontrak enkripsi cacat	Kontrak enkripsi cacat

Kasus kesalahan	Pesan kesalahan
Kontrak enkripsi bertentangan dengan batasan tingkat keamanan DRM	Kontrak enkripsi CPIX yang diminta tidak didukung
Kontrak enkripsi tidak termasuk AudioFilter elemen VideoFilter atau	Kontrak enkripsi CPIX tidak ada

SPEKE API v2 - Komponen muatan standar

Melalui permintaan SPEKE tunggal, enkripsi dapat meminta beberapa kunci konten, bersama dengan pensinyalan manifest yang diperlukan untuk beberapa format kemasan, sesuai dengan kontrak enkripsi yang ditentukan untuk konten tertentu.

Untuk mencakup semua aspek ini, dokumen CPIX standar terdiri dari tiga bagian daftar wajib, ditambah bagian daftar opsional untuk rotasi kunci konten langsung.

<cpix:CPIX><cpix: ContentKeyList > bagian dan elemen tingkat atas

Ini adalah bagian wajib, relevan untuk streaming Langsung dan VOD, menentukan kunci konten berbeda yang perlu digunakan oleh enkripsi. <cpix:ContentKeyList>Elemen dapat berisi satu atau beberapa elemen <cpix:ContentKey> anak, masing-masing menggambarkan kunci konten yang berbeda.

Sesuai spesifikasi CPIX, nilai ContentKey@commonEncryptionScheme atribut yang mungkin didefinisikan dalam enkripsi umum dalam spesifikasi file format file media dasar ISO (ISO/IEC 23001-7:2016):

- 'cenc': Mode AES-CTR sampel lengkap dan enkripsi Subsample NAL video
- 'cbc1': Contoh lengkap mode AES-CBC dan enkripsi Subsample NAL video
- 'cens': Enkripsi pola NAL video parsi mode AES-CTR
- 'cbcs': Enkripsi pola NAL video parsi mode AES-CBC

Contoh berikut menunjukkan dokumen CPIX dengan kunci konten tunggal yang tidak terenkripsi:

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
```

```

<cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs">
    <cpix:Data>
      <pskc:Secret>
        <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
      </pskc:Secret>
    </cpix:Data>
  </cpix:ContentKey>
</cpix:ContentKeyList>
...
</cpix:CPIX>
    
```

Secara default, kunci konten tidak dienkripsi, seperti pada contoh di bawah ini. Tetapi enkripsi kunci konten dapat diminta oleh enkripsi melalui penyertaan elemen <cpix : >. DeliveryDataList Silakan merujuk ke bagian Enkripsi Kunci Konten untuk lebih jelasnya.

Elemen didukung oleh SPEKE	Atribut wajib	Atribut opsional	Elemen anak wajib	Elemen anak opsional
<cpix:CPIX>	ContentID, versi, xmlns:cpix, xmlns:pskc	nama, xmlns:enc	satu <cpix:ContentKeyList>, satu<cPix:DRM >, satu SystemList <cpix :>ContentKeyUsageRuleList	satu <cpix:DeliveryDataList>, satu <cpix :>ContentKeyPeriodList
<cpix :>ContentKeyList	-	id	setidaknya satu <cpix :>ContentKey	-
<cpix :>ContentKey	anak, commonEncryptionScheme, Data	id, Algoritma, ExplicitIV	satu <pskc:Secret>	-

Elemen didukung oleh SPEKE	Atribut wajib	Atribut opsional	Elemen anak wajib	Elemen anak opsional
<pskc:Secret>	PlainValue atau EncryptedValue	ValueMac	-	<enc:EncryptionMethod>, <enc:CipherData>

<CPix:DRM>SystemListbagian

Ini adalah bagian wajib, relevan untuk streaming Langsung dan VOD, mendefinisikan berbagai sistem DRM yang perlu dimanfaatkan bersama dengan kunci konten.

Contoh berikut menunjukkan daftar sistem DRM dengan spesifikasi sistem PlayReady DRM tunggal:

```
<cpix:DRMSystemList>
  <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
    systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">HicXmbZ2m[...]4==</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">HicXmbZ2m[...]jEi</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>t7WwH24FI[...]YCC</cpix:ContentProtectionData>
    <cpix:PSSH>FFFFanBzc[...]A==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>s5RrJ12HL[...]UBB</
cpix:SmoothStreamingProtectionHeaderData>
  </cpix:DRMSystem>
</cpix:DRMSystemList>
```

Untuk daftar lengkap DRM SystemIds, silakan merujuk ke [bagian Perlindungan Konten](#) dari repositori DASH-IF Identifiers.

Elemen didukung oleh SPEKE	Atribut wajib	Atribut opsional	Elemen anak wajib	Elemen anak opsional
<CPix:DRM>SystemList	-	id	setidaknya satu <cpix:DRMSystem>	-

Elemen didukung oleh SPEKE	Atribut wajib	Atribut opsional	Elemen anak wajib	Elemen anak opsional
<cpix:DRM System>	anak, SystemID	id, nama, PSSH	-	ContentProtectionData, SmoothStreamingProtectionHeaderData, dua SignalingData <cpix:HLS>elemen dengan nilai atribut playlist yang berbeda

DRMSystem@PSSHwajib jika enkapsulasi ISO-BMFF diterapkan pada segmen media.

DRMSystem.ContentProtectionData<pssh>Elemen innerXML dimanfaatkan oleh enkripsi hanya untuk tujuan pensinyalan manifes.

Jika DRMSystem@PSSH hadir dan DRMSystem.ContentProtectionData berisi <pssh> elemen innerXML, kedua nilai harus identik.

Jika DRMSystem pensinyalan harus dilakukan dalam manifes HLS, <cpix:HLSSignalingData playlist="master"> elemen a <cpix:HLSSignalingData playlist="media"> dan a harus dimasukkan dalam permintaan dan respons CPIX.

<cpix : >bagian ContentKeyPeriodList

Ini adalah bagian opsional, hanya relevan untuk Streaming langsung, yang menentukan periode kriptografi yang diterapkan pada konten.

<cpix:ContentKeyPeriodList>Elemen tersebut dapat berisi satu atau beberapa elemen <cpix:ContentKeyPeriod> anak, masing-masing menggambarkan periode kriptografi yang berbeda dalam timeline langsung. Menggunakan UUID sebagai bagian dari nilai atribut id adalah pendekatan yang umum digunakan.

```
<cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f" index="1" /
>
</cpix:ContentKeyPeriodList>
```

Elemen didukung oleh SPEKE	Atribut wajib	Atribut opsional	Elemen anak wajib	Elemen anak opsional
<cpix : >ContentKeyPeriodList	-	id	setidaknya satu <cpix : >ContentKeyPeriod	-
<cpix : >ContentKeyPeriod	id, indeks	-	-	-

Jika periode krypto digunakan, kunci enkripsi juga harus dilampirkan ke salah satu periode krypto dalam dokumen CPIX, seperti yang ditunjukkan pada bagian di bawah ini.

```
<cpix : >bagian ContentKeyUsageRuleList
```

Ini adalah bagian wajib, relevan untuk streaming Langsung dan VOD, yang menentukan bagaimana kunci konten yang berbeda akan melindungi trek di dalam streamset dan di seluruh periode krypto.

Elemen <cpix: ContentKeyUsageRuleList > dapat berisi satu atau beberapa <cpix: ContentKeyUsageRule > elemen anak, masing-masing menggambarkan trek yang diterapkan kunci konten tertentu oleh enkripsi, berpotensi selama periode krypto tertentu. Setidaknya satu <cpix: AudioFilter > atau satu <cpix: VideoFilter > elemen diperlukan untuk hadir dalam elemen<cpix : >. ContentKeyUsageRule

Contoh berikut menunjukkan daftar sederhana dengan hanya satu aturan yang menerapkan satu kunci konten ke semua trek audio dan video selama periode krypto tertentu.

```
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  intendedTrackType="ALL">
```

```

<cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
<cpix:AudioFilter />
<cpix:VideoFilter />
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>

```

Elemen didukung oleh SPEKE	Atribut wajib	Atribut opsional	Elemen anak wajib	Elemen anak opsional
<cpix : >ContentKeyUsageRuleList	-	id	setidaknya satu <cpix : >ContentKeyUsageRule	-
<cpix : >ContentKeyUsageRule	anak, intendedTrackType	-	setidaknya satu <cpix: AudioFilter > atau satu <cpix : >(*) VideoFilter	<cpix : >KeyPeriodFilter
<cpix : >KeyPeriodFilter	periodID	-	-	-
<cpix : >AudioFilter	-	MinChannels, MaxChannels	-	-
<cpix : >VideoFilter	-	minPixels, MaxPixels, hdr, minFP, MaxFP	-	-

(*) Untuk penjelasan rinci tentang penggunaan satu atau beberapa kunci konten untuk melindungi satu atau beberapa trek dalam streamset, silakan merujuk ke bagian dokumentasi [Kontrak Enkripsi](#).

SPEKE API v2 - Kontrak enkripsi

Kontrak enkripsi menentukan kunci konten mana yang melindungi trek mana di dalam streamset tertentu, berdasarkan karakteristik trek.

Menggunakan beberapa tombol konten untuk trek yang berbeda dalam streamset, meskipun merupakan praktik terbaik industri yang direkomendasikan, tidak wajib, tetapi direkomendasikan - setidaknya dua tombol konten yang berbeda, satu untuk trek audio dan satu untuk trek video. Menggunakan kunci konten tunggal untuk mengenkripsi beberapa trek dimungkinkan tetapi perlu secara eksplisit ditandai dalam dokumen CPIX yang dikirim oleh enkripsi ke penyedia kunci. Secara umum, enkripsi selalu menjelaskan dengan tepat berapa banyak kunci konten yang diperlukan dan bagaimana mereka dimanfaatkan untuk mengenkripsi berbagai trek media.

Prinsip

Kontrak enkripsi terletak di `<cpix:ContentKeyUsageRuleList>` bagian dokumen CPIX. Pada bagian ini, setiap kunci konten yang didefinisikan dalam `<cpix:ContentKeyList>` bagian sesuai dengan `<cpix:ContentKeyUsageRule>` elemen tertentu, yang harus mencakup:

- `ContentKeyUsageRule@intendedTrackType` atribut yang dapat mereferensikan satu atau lebih sub-komponen, dipisahkan oleh tanda '+' jika beberapa sub-komponen digunakan. Nilai `ContentKeyUsageRule@intendedTrackType` harus unik dalam kontrak enkripsi, dan tidak dapat digunakan dalam beberapa `ContentKeyUsageRule` elemen.
- satu atau lebih `<cpix:AudioFilter>` atau elemen `<cpix:VideoFilter>` anak, tergantung pada nilai `ContentKeyUsageRule@intendedTrackType` atribut.

Aturan yang mengatur hubungan ini adalah sebagai berikut:

- Ketika semua trek audio dan video streamset perlu dilindungi dengan kunci konten yang unik, string 'ALL' harus digunakan sebagai nilai `ContentKeyUsageRule@intendedTrackType` atribut. Contoh 1 menunjukkan kasus penggunaan seperti itu. Dalam situasi ini, elemen `<cpix:AudioFilter />` dan `<cpix:VideoFilter />` anak tanpa atribut apa pun harus disertakan. Kombinasi `<cpix:AudioFilter>` dan/atau `<cpix:VideoFilter>` elemen lainnya tidak valid dalam konteks khusus ini.
- Untuk semua kasus penggunaan lainnya, nilai `ContentKeyUsageRule@intendedTrackType` atribut dapat didefinisikan secara bebas, dan jumlah `<cpix:AudioFilter />` dan elemen `<cpix:VideoFilter />` anak harus sesuai dengan jumlah sub-komponen yang dikumpulkan melalui tanda '+'. Contoh 2/3/4/5/6/7/9/10 menggambarkan persyaratan ini, ketika satu sub-komponen hadir dalam nilai atribut. `ContentKeyUsageRule@intendedTrackType` Contoh 8 mengilustrasikannya ketika beberapa sub-komponen `ContentKeyUsageRule@intendedTrackType="SD+HD"` digunakan: dijelaskan oleh dua elemen `<cpix:VideoFilter>` anak yang berbeda dengan nilai atribut yang berbeda,

dan `ContentKeyUsageRule@intendedTrackType="HDR+HFR+UHD"` dijelaskan oleh tiga elemen `<cpix:VideoFilter>` anak yang berbeda dengan nilai atribut yang berbeda.

Filter

CPIX mendefinisikan beberapa elemen penyaringan dan atribut, tetapi SPEKE hanya mendukung sebagian dari itu. Tabel berikut merangkum perbedaan-perbedaan ini:

Jenis filter CPIX	Dukungan SPEKE secara keseluruhan	Filter atribut yang didukung oleh SPEKE	Atribut filter tidak didukung oleh SPEKE
<code><cpix : >VideoFilter</code>	Ya	minPixels, MaxPixels, hdr, minFP, MaxFPS (atribut opsional)	wcg
<code><cpix : >AudioFilter</code>	Ya	minChannels, maxChannels (atribut opsional)	
<code><cpix : >KeyPeriodFilter</code>	Ya	periodID (atribut wajib)	
<code><cpix : >BitrateFilter</code>	Tidak	N/A	N/A
<code><cpix : >LabelFilter</code>	Tidak	N/A	N/A

Sesuai spesifikasi CPIX untuk VideoFilter, [minPixels, MaxPixels] adalah rentang semua inklusif di kedua dimensi, sedangkan (minFP, MaxFP] hanya inklusif untuk dimensi MaxFPS. Untuk AudioFilter, [minChannels, maxChannels] adalah rentang inklusif di kedua dimensi.

Situasi bermasalah

Ada situasi di mana informasi yang diberikan dalam kontrak enkripsi mungkin sebagian, ambigu atau salah. Dalam kasus ini, penting bahwa enkripsi dan penyedia kunci berperilaku dengan tepat dan menjamin perlindungan konten yang tepat. Tabel berikut menyajikan perilaku yang direkomendasikan dalam situasi ini:

Dalam situasi ini	Enkripsi harus/harus...	Penyedia kunci harus/harus...
Tidak ada aturan yang berlaku untuk satu atau beberapa trek di streamset (lihat contoh 3 di bawah)	Enkripsi harus melihat konfigurasinya (di luar muatan CPIX) dan memverifikasi bahwa trek yang bersangkutan tidak memerlukan enkripsi. Jika bukan harapan, enkripsi harus melempar kesalahan dan menghentikan pemrosesan.	Tidak relevan: penyedia kunci tidak memiliki pengetahuan tentang struktur streamset.
Beberapa aturan tumpang tindih dan menyarankan beberapa kunci konten untuk mengenkripsi trek tertentu	Enkripsi harus menerapkan yang terakhir ContentKeyUsageRule berhasil dievaluasi dalam urutan dokumen.	Tidak relevan: penyedia kunci tidak memiliki pengetahuan tentang struktur streamset.
Kontrak enkripsi berubah dalam satu siklus permintaan/respons SPEKE	Enkripsi harus mengajukan pengecualian dan menghentikan pemrosesan, karena penyedia kunci tidak bertanggung jawab untuk menentukan kontrak enkripsi.	Untuk mencegah situasi ini terjadi sejak awal, penyedia kunci tidak boleh memodifikasi kontrak enkripsi yang diterima dalam muatan CPIX dari permintaan SPEKE.
Kontrak enkripsi cacat: intendedTrackType /Filter pengecualian kendala kardinalitas, filter atau atribut yang tidak didukung	Enkripsi harus mengajukan pengecualian, menghentikan pemrosesan dan tidak mengirim permintaan SPEKE ke penyedia kunci, karena kemungkinan besar akan mengakibatkan perlindungan konten yang salah atau meninggalkan beberapa trek yang tidak terlindungi.	Penyedia kunci harus mengajukan pengecualian dan mengembalikan kesalahan 'Kontrak enkripsi yang salah bentuk'.

Dalam situasi ini	Enkripsi harus/harus...	Penyedia kunci harus/harus...
Kontrak enkripsi yang terbentuk dengan baik, tetapi melanggar batasan tingkat keamanan DRM: sebagai contoh, satu kunci konten diminta untuk melindungi trek audio dan trek video UHD	Jika enkripsi memiliki pengetahuan tentang kendala tingkat keamanan DRM, itu harus menimbulkan pengecualian, menghentikan pemrosesan dan tidak mengirim permintaan SPEKE ke penyedia kunci, karena kemungkinan besar akan menghasilkan perlindungan konten yang salah.	Penyedia kunci harus mengajukan pengecualian dan mengembalikan kesalahan 'Kontrak enkripsi CPIX yang diminta tidak didukung'.
Kontrak enkripsi tidak ada	Enkripsi tidak akan mengirim dokumen CPIX yang tidak mengandung elemen atau apa pun. VideoFilter AudioFilter	Penyedia kunci akan mengajukan pengecualian dan mengembalikan kesalahan 'Kontrak enkripsi CPIX yang hilang'.

Contoh Kontrak Enkripsi

Contoh 1: satu kunci konten untuk semua trek audio dan video

```
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
    intendedTrackType="ALL">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:AudioFilter />
    <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
```

Contoh 2: satu kunci konten untuk semua trek video, satu kunci konten untuk semua trek audio

```
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
    intendedTrackType="VIDEO">
```



```

    <cpix:KeyPeriodFilter
periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
    <cpix:KeyPeriodFilter
periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:AudioFilter />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>

```

Contoh 3: satu kunci konten untuk semua trek video, trek audio yang tidak terenkripsi

```

<cpix:ContentKeyUsageRuleList>
<cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="VIDEO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter />
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>

```

Contoh 4: beberapa tombol konten untuk trek video yang berbeda (SD/HD), satu kunci konten untuk semua trek audio

```

<cpix:ContentKeyUsageRuleList>
  <!-- Rule for SD video tracks (up to 1024x576) -->
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="SD">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter maxPixels="589824" />
  </cpix:ContentKeyUsageRule>
  <!-- Rule for HD video tracks (more than 1024x576) -->
  <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
intendedTrackType="HD">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter minPixels="589825" />
  </cpix:ContentKeyUsageRule>
  <!-- Rule for all audio tracks -->
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:AudioFilter />

```

```

</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>

```

Contoh 5: beberapa tombol konten untuk trek video yang berbeda (SD/HD/UHD), satu kunci konten untuk semua trek audio

```

<cpix:ContentKeyUsageRuleList>
  <!-- Rule for SD video tracks (up to 1024x576) -->
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  intendedTrackType="SD">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter maxPixels="589824" />
  </cpix:ContentKeyUsageRule>
  <!-- Rule for HD video tracks (more than 1024x576, up to 1920x1080) -->
  <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
  intendedTrackType="HD">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter minPixels="589825" maxPixels="2073600" />
  </cpix:ContentKeyUsageRule>
  <!-- Rule for UHD video tracks (more than 1920x1080) -->
  <cpix:ContentKeyUsageRule kid="75c6fa78-8b5d-6d75-9653-26f41b78d1a3"
  intendedTrackType="UHD">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter minPixels="2073601" />
  </cpix:ContentKeyUsageRule>
  <!-- Rule for all audio tracks -->
  <cpix:ContentKeyUsageRule kid="53abda2-f210-43cb-bc90-f18f9a890a02"
  intendedTrackType="AUDIO">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:AudioFilter />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>

```

Contoh 6: beberapa tombol konten untuk trek video yang berbeda (SD/HD/UHD1/UHD2), satu kunci konten untuk semua trek audio

```

<cpix:ContentKeyUsageRuleList>
  <!-- Rule for SD video tracks (up to 1024x576) -->
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
  intendedTrackType="SD">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter maxPixels="589824" />

```

```

</cpix:ContentKeyUsageRule>
<!-- Rule for HD video tracks (more than 1024x576, up to 1920x1080) -->
<cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
intendedTrackType="HD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="589825" maxPixels="2073600" />
</cpix:ContentKeyUsageRule>
<!-- Rule for UHD1 video tracks (more than 1920x1080, up to 4096x2160) -->
<cpix:ContentKeyUsageRule kid="75c6fa78-8b5d-6d75-9653-26f41b78d1a3"
intendedTrackType="UHD1">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="2073601" maxPixels="8847360" />
</cpix:ContentKeyUsageRule>
<!-- Rule for UHD2 video tracks (more than 4096x2160) -->
<cpix:ContentKeyUsageRule kid="63d2ec36-6b7c-9f34-4546-97d01f36f7c5"
intendedTrackType="UHD2">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="8847361" />
</cpix:ContentKeyUsageRule>
<!-- Rule for all audio tracks -->
<cpix:ContentKeyUsageRule kid="53abda2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>

```

Contoh 7: beberapa tombol konten untuk trek video yang berbeda (SD/HD1/HD2/UHD1/UHD2), satu kunci konten untuk semua trek audio

```

<cpix:ContentKeyUsageRuleList>
<!-- Rule for SD video tracks (up to 1024x576) -->
<cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="SD">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter maxPixels="589824" />
</cpix:ContentKeyUsageRule>
<!-- Rule for HD1 video tracks (more than 1024x576, up to 1280x720) -->
<cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
intendedTrackType="HD1">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="589825" maxPixels="921600" />
</cpix:ContentKeyUsageRule>

```

```

    <!-- Rule for HD2 video tracks (more than 1280x720, up to 1920x1080) -->
    <cpix:ContentKeyUsageRule kid="cda406d8-9d87-4f76-92da-31110e756176"
intendedTrackType="HD2">
      <cpix:KeyPeriodFilter
periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
      <cpix:VideoFilter minPixels="921601" maxPixels="2073600" />
    </cpix:ContentKeyUsageRule>
<!-- Rule for UHD1 video tracks (more than 1920x1080, up to 4096x2160) -->
<cpix:ContentKeyUsageRule kid="75c6fa78-8b5d-6d75-9653-26f41b78d1a3"
intendedTrackType="UHD1">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="2073601" maxPixels="8847360" />
</cpix:ContentKeyUsageRule>
<!-- Rule for UHD2 video tracks (more than 4096x2160) -->
<cpix:ContentKeyUsageRule kid="63d2ec36-6b7c-9f34-4546-97d01f36f7c5"
intendedTrackType="UHD2">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter minPixels="8847361" />
</cpix:ContentKeyUsageRule>
<!-- Rule for all audio tracks -->
<cpix:ContentKeyUsageRule kid="53abda2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>

```

Contoh 8: beberapa tombol konten untuk trek video yang berbeda (berdasarkan beberapa jenis atribut), satu kunci konten untuk semua trek audio

```

<cpix:ContentKeyUsageRuleList>
  <!-- Rule for SD and HD video tracks-->
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="SD+HD">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter maxPixels="442368" maxFps="30" hdr="false"/>
    <cpix:VideoFilter minPixels="442369" maxPixels="2073600" maxFps="30" hdr="false"/>
  </cpix:ContentKeyUsageRule>
  <!-- Rule for HDR, HFR and UHD video tracks-->
  <cpix:ContentKeyUsageRule kid="37e3de05-9a3b-4c69-8970-63c17a95e0b7"
intendedTrackType="HDR+HFR+UHD">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter hdr="true" />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>

```

```

<cpix:VideoFilter minFps="30" />
<cpix:VideoFilter minPixels="20736001" />
</cpix:ContentKeyUsageRule>
<!-- Rule for all audio tracks-->
<cpix:ContentKeyUsageRule kid="53abda2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>

```

Contoh 9: satu tombol konten untuk semua trek video, beberapa tombol konten untuk trek audio stereo dan multichannel

```

<cpix:ContentKeyUsageRuleList>
  <!-- Rule for video tracks-->
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="VIDEO">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
  <!-- Rule for stereo audio tracks-->
  <cpix:ContentKeyUsageRule kid="53abda2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="STEREO_AUDIO">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:AudioFilter maxChannels="2"/>
  </cpix:ContentKeyUsageRule>
  <!-- Rule for multichannel audio tracks-->
  <cpix:ContentKeyUsageRule kid="7ae8e96f-309e-42c3-a510-24023d923373"
intendedTrackType="MULTICHANNEL_AUDIO">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <AudioFilter minChannels="3"/>
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>

```

Contoh 10: satu tombol konten untuk semua trek video, beberapa tombol konten untuk stereo dan dua jenis trek audio multichannel

```

<cpix:ContentKeyUsageRuleList>
  <!-- Rule for video tracks-->
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="VIDEO">

```

```

<cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
<cpix:VideoFilter />
</cpix:ContentKeyUsageRule>
<!-- Rule for stereo audio tracks-->
<cpix:ContentKeyUsageRule kid="53abda2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="STEREO_AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter maxChannels="2"/>
</cpix:ContentKeyUsageRule>
<!-- Rule for multichannel audio tracks (3 to 6 channels)-->
<cpix:ContentKeyUsageRule kid="7ae8e96f-309e-42c3-a510-24023d923373"
intendedTrackType="MULTICHANNEL_AUDIO_3_6">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter minChannels="3" maxChannels="6"/>
</cpix:ContentKeyUsageRule>
<!-- Rule for multichannel audio tracks (7 channels and more)-->
<cpix:ContentKeyUsageRule kid="81eb3761-55ff-4d22-a31d-94f01bbfd8ba"
intendedTrackType="MULTICHANNEL_AUDIO_7">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter minChannels="7"/>
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>

```

SPEKE API v2 - Contoh panggilan metode alur kerja langsung

Minta Contoh Sintaks

URL berikut adalah contoh dan tidak menunjukkan format tetap:

```
POST https://speke-compatible-server/speke/v2.0/copyProtection
```

Permintaan Badan

Dokumen CPIX.

Permintaan Header

Nama	Tipe	Terjadi	Deskripsi
AWS Authoriza tion	String	1.. 1	Lihat AWS Sigv4

Nama	Tipe	Terjadi	Deskripsi
X-Amz-Security-Token	String	1.. 1	Lihat AWS Sigv4
X-Amz-Date	String	1.. 1	Lihat AWS Sigv4
Content-Type	String	1.. 1	aplikasi/xml.
X-Speke-Version	String	1.. 1	Versi SPEKE API digunakan dengan permintaan, dirumuskan sebagai. MajorVersion MinorVersion, seperti '2.0' untuk SPEKE v2.0

Header Respons

Nama	Tipe	Terjadi	Deskripsi
X-Speke-User-Agent	String	1.. 1	String yang mengidentifikasi penyedia kunci
Content-Type	String	1.. 1	aplikasi/xml.
X-Speke-Version	String	1.. 1	Versi SPEKE API digunakan dengan permintaan, dirumuskan sebagai. MajorVersion MinorVersion, seperti '2.0' untuk SPEKE v2.0

Permintaan Respon

KODE HTTP	Nama Muatan	Terjadi	Deskripsi
200 (Success)	CPIX	1.. 1	Respons muatan DASH-CPIX
4XX (Client error)	Pesan kesalahan klien	1.. 1	Deskripsi kesalahan klien
5XX (Server error)	Pesan kesalahan server	1.. 1	Deskripsi kesalahan server

Note

Contoh di bagian ini tidak termasuk enkripsi kunci konten. Untuk informasi tentang cara menambahkan enkripsi kunci konten, lihat [Enkripsi kunci konten](#).

Contoh Langsung Minta Payload dengan Kunci di Clear

Contoh berikut menunjukkan payload permintaan langsung khas dari enkripsi ke penyedia kunci DRM, dengan satu kunci konten untuk semua trek video dan satu kunci konten untuk semua trek audio:

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs"></cpix:ContentKey>
    <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abdba2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs"></cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- FairPlay -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
      <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
    </cpix:DRMSystem>
```



```

<cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
  <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
</cpix:DRMSystem>
<!-- Widevine -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
  <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  <cpix:ContentProtectionData></cpix:ContentProtectionData>
  <cpix:PSSH></cpix:PSSH>
</cpix:DRMSystem>
<cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
  <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  <cpix:ContentProtectionData></cpix:ContentProtectionData>
  <cpix:PSSH></cpix:PSSH>
</cpix:DRMSystem>
<!-- Playready -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
  <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  <cpix:ContentProtectionData></cpix:ContentProtectionData>
  <cpix:PSSH></cpix:PSSH>
  <cpix:SmoothStreamingProtectionHeaderData></
cpix:SmoothStreamingProtectionHeaderData>
</cpix:DRMSystem>
<cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
  <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  <cpix:ContentProtectionData></cpix:ContentProtectionData>
  <cpix:PSSH></cpix:PSSH>
  <cpix:SmoothStreamingProtectionHeaderData></
cpix:SmoothStreamingProtectionHeaderData>
</cpix:DRMSystem>
</cpix:DRMSystemList>
<cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
</cpix:ContentKeyPeriodList>

```

```

<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="VIDEO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter />
</cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>

```

Muatan Respons Contoh Langsung dengan Kunci di Clear

Contoh berikut menunjukkan muatan respons tipikal dari penyedia kunci DRM (nilai yang dikembalikan telah dipersingkat dengan [...] untuk keterbacaan):

```

<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="CBCS">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
    <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abdba2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="CBCS">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>h3toSFilyAYpfXVQ795m6x==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- FairPlay -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">

```

```

    <cpix:HLSSignalingData playlist="media">aHR0cHM6L[...]WZm</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">Y29tLmFwc[...]XJ5</cpix:HLSSignalingData>
</cpix:DRMSystem>
<cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
    <cpix:HLSSignalingData playlist="media">trBANbMcyj[...]u44</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">mn626PjyR[...]2fi</cpix:HLSSignalingData>
</cpix:DRMSystem>
<!-- Widevine -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
    <cpix:HLSSignalingData playlist="media">Ifa2V5LW1[...]nNB</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd2l</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
    <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
</cpix:DRMSystem>
<cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
    <cpix:HLSSignalingData playlist="media">1TznjvtzL[...]GfJ</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">XgzdzQH7p[...]zeX</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>TdgRnuJsZ[...]wDw</cpix:ContentProtectionData>
    <cpix:PSSH>mYZbjpWdS[...]D==</cpix:PSSH>
</cpix:DRMSystem>
<!-- Playready -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">HicXmbZ2m[...]4==</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">GVzdCIfa2[...]Eta</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>t7WwH24FI[...]YCC</cpix:ContentProtectionData>
    <cpix:PSSH>FFFFanBzc[...]A==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>s5RrJ12HL[...]UBB</
cpix:SmoothStreamingProtectionHeaderData>
</cpix:DRMSystem>
<cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">BptGzwis2[...]Iej</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">3c9SXdVa0[...]MBH</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>HotJCMQyc[...]GpU</cpix:ContentProtectionData>
    <cpix:PSSH>S6UD43ybN[...]f==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>VBFUv2or0[...]JeP</
cpix:SmoothStreamingProtectionHeaderData>
</cpix:DRMSystem>
</cpix:DRMSystemList>
<cpix:ContentKeyPeriodList>

```

```

<cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
</cpix:ContentKeyPeriodList>
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="VIDEO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter />
</cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:AudioFilter />
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>

```

SPEKE API v2 - contoh panggilan metode alur kerja VOD

Minta Contoh Sintaks

URL berikut adalah contoh dan tidak menunjukkan format tetap.

```
POST https://speke-compatible-server/speke/v2.0/copyProtection
```

Permintaan Badan

Dokumen CPIX.

Permintaan Header

Nama	Tipe	Terjadi	Deskripsi
AWS Authoriza tion	String	1.. 1	Lihat AWS Sigv4
X-Amz-Security- Token	String	1.. 1	Lihat AWS Sigv4
X-Amz-Date	String	1.. 1	Lihat AWS Sigv4
Content-Type	String	1.. 1	aplikasi/xml.

Nama	Tipe	Terjadi	Deskripsi
X-Speke-Version	String	1.. 1	Versi SPEKE API digunakan dengan permintaan, dirumuskan sebagai. MajorVersion MinorVersion, seperti '2.0' untuk SPEKE v2.0

Header Respons

Nama	Tipe	Terjadi	Deskripsi
X-Speke-User-Agent	String	1.. 1	String yang mengidentifikasi penyedia kunci
Content-Type	String	1.. 1	aplikasi/xml.
X-Speke-Version	String	1.. 1	Versi SPEKE API digunakan dengan permintaan, dirumuskan sebagai. MajorVersion MinorVersion, seperti '2.0' untuk SPEKE v2.0

Permintaan Respon

KODE HTTP	Nama Muatan	Terjadi	Deskripsi
200 (Success)	CPIX	1.. 1	Respons muatan DASH-CPIX

KODE HTTP	Nama Muatan	Terjadi	Deskripsi
4XX (Client error)	Pesan kesalahan klien	1.. 1	Deskripsi kesalahan klien
5XX (Server error)	Pesan kesalahan server	1.. 1	Deskripsi kesalahan server

Note

Contoh di bagian ini tidak termasuk enkripsi kunci konten. Untuk informasi tentang cara menambahkan enkripsi kunci konten, lihat [Enkripsi kunci konten](#).

Contoh VOD Minta Payload dengan Kunci di Clear

Contoh berikut menunjukkan muatan permintaan VOD tipikal dari enkripsi ke penyedia kunci DRM, dengan satu kunci konten untuk semua trek video dan satu kunci konten untuk semua trek audio:

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs"></cpix:ContentKey>
    <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abda2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs"></cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- FairPlay -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
      <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
    </cpix:DRMSystem>
    <cpix:DRMSystem kid="53abda2-f210-43cb-bc90-f18f9a890a02"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
      <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
    </cpix:DRMSystem>
    <!-- Widevine -->
```

```

<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
  <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  <cpix:ContentProtectionData></cpix:ContentProtectionData>
  <cpix:PSSH></cpix:PSSH>
</cpix:DRMSystem>
<cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
  <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  <cpix:ContentProtectionData></cpix:ContentProtectionData>
  <cpix:PSSH></cpix:PSSH>
</cpix:DRMSystem>
<!-- Playready -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
  <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  <cpix:ContentProtectionData></cpix:ContentProtectionData>
  <cpix:PSSH></cpix:PSSH>
  <cpix:SmoothStreamingProtectionHeaderData></
cpix:SmoothStreamingProtectionHeaderData>
</cpix:DRMSystem>
<cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
  <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>
  <cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
  <cpix:ContentProtectionData></cpix:ContentProtectionData>
  <cpix:PSSH></cpix:PSSH>
  <cpix:SmoothStreamingProtectionHeaderData></
cpix:SmoothStreamingProtectionHeaderData>
</cpix:DRMSystem>
</cpix:DRMSystemList>
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="VIDEO">
  <cpix:VideoFilter />
</cpix:ContentKeyUsageRule>
  <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
  <cpix:AudioFilter />
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>

```

```
</cpix:CPIX>
```

VOD Contoh Respons Payload dengan Keys di Clear

Contoh berikut menunjukkan muatan respons tipikal dari penyedia kunci DRM (nilai yang dikembalikan telah dipersingkat dengan [...] untuk keterbacaan):

```
<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-a20d-163a-
e382420c6eff" commonEncryptionScheme="cbcs">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
    <cpix:ContentKey explicitIV="L6jzdXrXAFbCJGBuMrrKrG==" kid="53abdba2-f210-43cb-bc90-
f18f9a890a02" commonEncryptionScheme="cbcs">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>h3toSFilyAYpfXVQ795m6x==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- FairPlay -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
      <cpix:HLSSignalingData playlist="media">aHR0cHM6L[...]WZm</cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master">Y29tLmFwc[...]XJ5</cpix:HLSSignalingData>
    </cpix:DRMSystem>
    <cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="94ce86fb-07ff-4f43-adb8-93d2fa968ca2">
      <cpix:HLSSignalingData playlist="media">trBANbMcj[...]u44</cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master">mn626PjyR[...]2fi</cpix:HLSSignalingData>
    </cpix:DRMSystem>
    <!-- Widevine -->
    <cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
      <cpix:HLSSignalingData playlist="media">Ifa2V5LW1[...]nNB</cpix:HLSSignalingData>
```



```

    <cpix:HLSSignalingData playlist="master">oIARIQeSI[...]Nd2l</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>RoNd2lkZXZ[...]Nib</cpix:ContentProtectionData>
    <cpix:PSSH>AAAAanBzc[...]A==</cpix:PSSH>
</cpix:DRMSystem>
<cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
    <cpix:HLSSignalingData playlist="media">1TznjvtzL[...]GfJ</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">XgzdzQH7p[...]zeX</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>TdgRnuJsZ[...]wDw</cpix:ContentProtectionData>
    <cpix:PSSH>mYZbjpWdS[...]D==</cpix:PSSH>
</cpix:DRMSystem>
<!-- Playready -->
<cpix:DRMSystem kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">HicXmbZ2m[...]4==</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">GVzdCIfa2[...]Eta</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>t7WwH24FI[...]YCC</cpix:ContentProtectionData>
    <cpix:PSSH>FFFFanBzc[...]A==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>s5RrJ12HL[...]UBB</
cpix:SmoothStreamingProtectionHeaderData>
</cpix:DRMSystem>
<cpix:DRMSystem kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
systemId="9a04f079-9840-4286-ab92-e65be0885f95">
    <cpix:HLSSignalingData playlist="media">BptGzwis2[...]Iej</cpix:HLSSignalingData>
    <cpix:HLSSignalingData playlist="master">3c9SXdVa0[...]MBH</cpix:HLSSignalingData>
    <cpix:ContentProtectionData>HotJCMQyc[...]GpU</cpix:ContentProtectionData>
    <cpix:PSSH>S6UD43ybN[...]f==</cpix:PSSH>
    <cpix:SmoothStreamingProtectionHeaderData>VBFUv2or0[...]JeP</
cpix:SmoothStreamingProtectionHeaderData>
</cpix:DRMSystem>
</cpix:DRMSystemList>
<cpix:ContentKeyUsageRuleList>
    <cpix:ContentKeyUsageRule kid="98ee5596-cd3e-a20d-163a-e382420c6eff"
intendedTrackType="VIDEO">
        <cpix:VideoFilter />
    </cpix:ContentKeyUsageRule>
    <cpix:ContentKeyUsageRule kid="53abdba2-f210-43cb-bc90-f18f9a890a02"
intendedTrackType="AUDIO">
        <cpix:AudioFilter />
    </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>

```

SPEKE API v2 - Enkripsi kunci konten

Anda dapat menambahkan enkripsi kunci konten secara opsional ke implementasi SPEKE Anda. Enkripsi kunci konten menjamin end-to-end perlindungan penuh dengan mengenkripsi kunci konten untuk transit, selain mengenkripsi konten itu sendiri. Jika Anda tidak menerapkan ini untuk penyedia kunci Anda, Anda mengandalkan enkripsi lapisan transport ditambah otentikasi yang kuat untuk keamanan.

Untuk menggunakan enkripsi kunci konten untuk enkripsi yang berjalan di AWS Cloud, pelanggan mengimpor sertifikat ke AWS Certificate Manager dan kemudian menggunakan ARN sertifikat yang dihasilkan untuk aktivitas enkripsi mereka. Enkripsi menggunakan ARN sertifikat dan layanan ACM untuk menyediakan kunci konten terenkripsi ke penyedia kunci DRM.

Pembatasan

SPEKE mendukung enkripsi kunci konten sebagaimana ditentukan dalam spesifikasi DASH-IF CPIX dengan batasan berikut:

- SPEKE tidak mendukung verifikasi tanda tangan digital (XMLDSIG) untuk muatan permintaan atau respons.
- SPEKE membutuhkan 2048 sertifikat berbasis RSA.

Pembatasan ini juga tercantum dalam [Kustomisasi dan kendala](#) untuk spesifikasi DASH-IF.

Menerapkan enkripsi kunci konten

Untuk menyediakan enkripsi kunci konten, sertakan yang berikut ini dalam implementasi penyedia kunci DRM Anda:

- Tangani elemen `<cpix:DeliveryDataList>` dalam permintaan dan muatan respons.
- Berikan nilai terenkripsi dalam `<cpix:ContentKeyList>` muatan respons.

Untuk informasi lebih lanjut tentang elemen-elemen ini, lihat spesifikasi [DASH-IF CPIX 2.3](#).

Contoh Elemen Enkripsi Kunci Konten `<cpix:DeliveryDataList>` di Muatan Permintaan

```
<cpix:CPIX contentId="abc123"  
  version="2.3"  
  xmlns:cpix="urn:dashif:org:cpix"
```

```

xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:DeliveryDataList>
    <cpix:DeliveryData id="<ORIGIN SERVER ID>">
      <cpix:DeliveryKey>
        <ds:X509Data>
          <ds:X509Certificate><X.509 CERTIFICATE, BASE-64 ENCODED></
ds:X509Certificate>
          </ds:X509Data>
        </cpix:DeliveryKey>
      </cpix:DeliveryData>
    </cpix:DeliveryDataList>
    <cpix:ContentKeyList>
      ...
    </cpix:ContentKeyList>
  </cpix:CPIX>

```

Contoh Elemen Enkripsi Kunci Konten <cpix:DeliveryDataList> di Payload Respons

```

<cpix:CPIX contentId="abc123"
  version="2.3"
  xmlns:cpix="urn:dashif:org:cpix"
  xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:DeliveryDataList>
    <cpix:DeliveryData id="<ORIGIN SERVER ID>">
      <cpix:DeliveryKey>
        <ds:X509Data>
          <ds:X509Certificate><X.509 CERTIFICATE, BASE-64 ENCODED></
ds:X509Certificate>
          </ds:X509Data>
        </cpix:DeliveryKey>
        <cpix:DocumentKey Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc">
          <cpix:Data>
            <pskc:Secret>
              <pskc:EncryptedValue>
                <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#rsa-oaep-mgf1p" />
                <enc:CipherData>
                  <enc:CipherValue><RSA CIPHER VALUE></enc:CipherValue>
                </enc:CipherData>
              </pskc:EncryptedValue>
              <pskc:ValueMAC>qnei/5TsfUwDu+8bhsZrLjDRDngvmnUZD2eva7SfXWw=</
pskc:ValueMAC>
            </pskc:Secret>
          </cpix:Data>
        </cpix:DocumentKey>
      </cpix:DeliveryData>
    </cpix:DeliveryDataList>
  </cpix:CPIX>

```

```

        </cpix:Data>
    </cpix:DocumentKey>
    <cpix:MACMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#hmac-
sha512">
        <cpix:Key>
            <pskc:EncryptedValue>
                <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#rsa-oaep-mgf1p" />
                <enc:CipherData>
                    <enc:CipherValue><RSA CIPHER VALUE></enc:CipherValue>
                </enc:CipherData>
            </pskc:EncryptedValue>
            <pskc:ValueMAC>DGqdpHUffKxds09+EWrPjtdTCVfjPLwwtzEcFC/j0xY=</
pskc:ValueMAC>
        </cpix:Key>
    </cpix:MACMethod>
</cpix:DeliveryData>
</cpix:DeliveryDataList>
<cpix:ContentKeyList>
    ...
</cpix:ContentKeyList>
</cpix:CPIX>

```

Contoh Elemen Enkripsi Kunci Konten `<cpix:ContentKeyList>` di Payload Respons

Contoh berikut menunjukkan penanganan kunci konten terenkripsi dalam `<cpix:ContentKeyList>` elemen payload respons. Ini menggunakan `<pskc:EncryptedValue>` elemen:

```

<cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-
a20d-163a-e382420c6eff" commonEncryptionScheme="cbcs">
        <cpix:Data>
            <pskc:Secret>
                <pskc:EncryptedValue>
                    <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#aes256-cbc" />
                    <enc:CipherData>
                        <enc:CipherValue>NJYebfvJ2TdMm3k6v
+rLNvYb0NoTJoTLBBdbpe8nmilEfp82SKa7MkqTn2lmQBPB</enc:CipherValue>
                    </enc:CipherData>
                </pskc:EncryptedValue>
            </pskc:Secret>
        </cpix:Data>
    </cpix:ContentKey>
</cpix:ContentKeyList>

```

```

    <pskc:ValueMAC>t9lW4WCebfS1GP+dh0IicMs+2+jnrAmfDa4WU6VGHc4=</
pskc:ValueMAC>
    </pskc:Secret>
  </cpix:Data>
</cpix:ContentKey>
</cpix:ContentKeyList>

```

Sebagai perbandingan, contoh berikut menunjukkan muatan respons serupa dengan kunci konten yang dikirimkan tanpa enkripsi, sebagai kunci yang jelas. Ini menggunakan `<pskc:PlainValue>` elemen:

```

<cpix:ContentKeyList>
  <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw==" kid="98ee5596-cd3e-
a20d-163a-e382420c6eff" commonEncryptionScheme="cbcs">
    <cpix:Data>
      <pskc:Secret>
        <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
      </pskc:Secret>
    </cpix:Data>
  </cpix:ContentKey>
</cpix:ContentKeyList>

```

SPEKE API v2 - Mengganti pengenalan kunci

Enkripsi membuat pengenalan kunci baru (KID) setiap kali memutar kunci. Ini meneruskan KID ke penyedia kunci DRM dalam permintaannya. Hampir selalu, penyedia kunci merespons menggunakan KID yang sama, tetapi dapat memberikan nilai yang berbeda untuk KID dalam tanggapannya.

Berikut ini adalah contoh permintaan dengan KID11111111-1111-1111-1111-111111111111:

```

<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw=="
kid="11111111-1111-1111-1111-111111111111" commonEncryptionScheme="cbcs"></
cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- Widevine -->
    <cpix:DRMSystem kid="11111111-1111-1111-1111-111111111111"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
      <cpix:HLSSignalingData playlist="media"></cpix:HLSSignalingData>

```

```

<cpix:HLSSignalingData playlist="master"></cpix:HLSSignalingData>
<cpix:ContentProtectionData></cpix:ContentProtectionData>
<cpix:PSSH></cpix:PSSH>
</cpix:DRMSystem>
</cpix:DRMSystemList>
<cpix:ContentKeyPeriodList>
  <cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
</cpix:ContentKeyPeriodList>
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="11111111-1111-1111-1111-111111111111"
intendedTrackType="VIDEO">
    <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
    <cpix:VideoFilter />
  </cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>

```

Tanggapan berikut mengesampingkan KID ke: 22222222-2222-2222-2222-222222222222

```

<cpix:CPIX contentId="abc123" version="2.3" xmlns:cpix="urn:dashif:org:cpix"
xmlns:pskc="urn:ietf:params:xml:ns:keyprov:pskc">
  <cpix:ContentKeyList>
    <cpix:ContentKey explicitIV="0Fj2IjCsPJFfMAxmQxLGPw=="
kid="22222222-2222-2222-2222-222222222222" commonEncryptionScheme="cbcs">
      <cpix:Data>
        <pskc:Secret>
          <pskc:PlainValue>5dGAgwGuUYu4dHeHtNlxJw==</pskc:PlainValue>
        </pskc:Secret>
      </cpix:Data>
    </cpix:ContentKey>
  </cpix:ContentKeyList>
  <cpix:DRMSystemList>
    <!-- Widevine -->
    <cpix:DRMSystem kid="22222222-2222-2222-2222-222222222222"
systemId="edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
      <cpix:HLSSignalingData playlist="media">Ifa2V5LWl[... ]nNB</cpix:HLSSignalingData>
      <cpix:HLSSignalingData playlist="master">oIARIQeSI[... ]Nd2l</cpix:HLSSignalingData>
      <cpix:ContentProtectionData>RoNd2lkZXZ[... ]Nib</cpix:ContentProtectionData>
      <cpix:PSSH>AAAAanBzc[... ]A==</cpix:PSSH>
    </cpix:DRMSystem>
  </cpix:DRMSystemList>
  <cpix:ContentKeyPeriodList>

```

```
<cpix:ContentKeyPeriod id="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"
index="1" />
</cpix:ContentKeyPeriodList>
<cpix:ContentKeyUsageRuleList>
  <cpix:ContentKeyUsageRule kid="22222222-2222-2222-2222-222222222222"
intendedTrackType="VIDEO">
  <cpix:KeyPeriodFilter periodId="keyPeriod_0909829f-40ff-4625-90fa-75da3e53278f"/>
  <cpix:VideoFilter />
</cpix:ContentKeyUsageRule>
</cpix:ContentKeyUsageRuleList>
</cpix:CPIX>
```

Lisensi

Atribusi Creative Commons- ShareAlike 4.0 Lisensi Publik Internasional

Dengan menggunakan Hak Berlisensi (didefinisikan di bawah), Anda menerima dan setuju untuk terikat oleh syarat dan ketentuan Lisensi Publik Internasional Creative Commons Attribution-ShareAlike 4.0 International Public License ini ("Lisensi Publik"). Sejauh Lisensi Publik ini dapat ditafsirkan sebagai kontrak, Anda diberikan Hak Berlisensi dengan mempertimbangkan penerimaan Anda atas syarat dan ketentuan ini, dan Pemberi Lisensi memberi Anda hak tersebut dengan mempertimbangkan manfaat yang diterima Pemberi Lisensi dari membuat Materi Berlisensi tersedia berdasarkan syarat dan ketentuan ini.

Bagian 1 — Definisi.

- a. Materi yang Diadaptasi berarti materi yang tunduk pada Hak Cipta dan Hak Serupa yang berasal dari atau berdasarkan Materi Berlisensi dan di mana Materi Berlisensi diterjemahkan, diubah, diatur, diubah, atau dimodifikasi dengan cara yang memerlukan izin berdasarkan Hak Cipta dan Hak Serupa yang dimiliki oleh Pemberi Lisensi. Untuk tujuan Lisensi Publik ini, di mana Materi Berlisensi adalah karya musik, pertunjukan, atau rekaman suara, Materi Adaptasi selalu diproduksi di mana Materi Berlisensi disinkronkan dalam hubungan waktunya dengan gambar bergerak.
- b. Lisensi Adaptor berarti lisensi yang Anda terapkan pada Hak Cipta Anda dan Hak Serupa dalam kontribusi Anda pada Materi yang Diadaptasi sesuai dengan syarat dan ketentuan Lisensi Publik ini.
- c. Lisensi Kompatibel BY-SA berarti lisensi yang terdaftar di creativecommons.org/compatiblelicenses, yang disetujui oleh Creative Commons pada dasarnya setara dengan Lisensi Publik ini.

- d. Hak Cipta dan Hak Serupa berarti hak cipta dan/atau hak serupa yang terkait erat dengan hak cipta termasuk, tanpa batasan, kinerja, siaran, rekaman suara, dan Hak Basis Data Sui Generis, tanpa memperhatikan bagaimana hak tersebut diberi label atau dikategorikan. Untuk tujuan Lisensi Publik ini, hak yang ditentukan dalam Bagian 2 (b) (1) - (2) bukanlah Hak Cipta dan Hak Serupa.
- e. Tindakan Teknologi Efektif berarti langkah-langkah yang, jika tidak ada wewenang yang tepat, tidak dapat dielakkan berdasarkan undang-undang yang memenuhi kewajiban berdasarkan Pasal 11 Perjanjian Hak Cipta WIPO yang diadopsi pada tanggal 20 Desember 1996, dan/atau perjanjian internasional serupa.
- f. Pengecualian dan Batasan berarti penggunaan wajar, transaksi yang adil, dan/atau pengecualian atau pembatasan lainnya terhadap Hak Cipta dan Hak Serupa yang berlaku untuk penggunaan Materi Berlisensi oleh Anda.
- g. Elemen Lisensi berarti atribut lisensi yang tercantum dalam nama Lisensi Publik Creative Commons. Elemen Lisensi dari Lisensi Publik ini adalah Atribusi dan ShareAlike.
- h. Materi Berlisensi berarti karya artistik atau sastra, basis data, atau materi lain tempat Pemberi Lisensi menerapkan Lisensi Publik ini.
- i. Hak Berlisensi berarti hak yang diberikan kepada Anda tunduk pada syarat dan ketentuan Lisensi Publik ini, yang terbatas pada semua Hak Cipta dan Hak Serupa yang berlaku untuk penggunaan Materi Berlisensi oleh Anda dan bahwa Pemberi Lisensi memiliki wewenang untuk melisensikan.
- j. Pemberi Lisensi berarti individu atau entitas yang memberikan hak berdasarkan Lisensi Publik ini.
- k. Berbagi berarti menyediakan materi kepada publik dengan cara atau proses apa pun yang memerlukan izin berdasarkan Hak Berlisensi, seperti reproduksi, tampilan publik, kinerja publik, distribusi, penyebaran, komunikasi, atau impor, dan untuk membuat materi tersedia untuk umum termasuk dengan cara anggota masyarakat dapat mengakses materi dari suatu tempat dan pada waktu yang dipilih secara individual oleh mereka.
- l. Hak Basis Data Sui Generis berarti hak selain hak cipta yang dihasilkan dari Arahan 96/9/EC Parlemen Eropa dan Dewan 11 Maret 1996 tentang perlindungan hukum database, sebagaimana diubah dan/atau berhasil, serta hak-hak lain yang pada dasarnya setara di mana pun di dunia.
- m. Anda berarti individu atau entitas yang menjalankan Hak Berlisensi berdasarkan Lisensi Publik ini. Anda memiliki arti yang sesuai.

Bagian 2 — Lingkup.

- a. Pemberian lisensi.

1. Tunduk pada syarat dan ketentuan Lisensi Publik ini, Pemberi Lisensi dengan ini memberi Anda lisensi di seluruh dunia, bebas royalti, tidak dapat disublisensikan, non-eksklusif, tidak dapat dibatalkan untuk menggunakan Hak Berlisensi dalam Materi Berlisensi untuk:
 - A. mereproduksi dan Membagikan Materi Berlisensi, secara keseluruhan atau sebagian; dan
 - B. memproduksi, mereproduksi, dan Berbagi Materi yang Diadaptasi.
2. Pengecualian dan Batasan. Untuk menghindari keraguan, di mana Pengecualian dan Batasan berlaku untuk penggunaan Anda, Lisensi Publik ini tidak berlaku, dan Anda tidak perlu mematuhi syarat dan ketentuannya.
3. Istilah. Istilah Lisensi Publik ini ditentukan dalam Bagian 6 (a).
4. Media dan format; modifikasi teknis diperbolehkan. Pemberi Lisensi memberi wewenang kepada Anda untuk menggunakan Hak Berlisensi di semua media dan format baik yang sekarang diketahui atau selanjutnya dibuat, dan untuk membuat modifikasi teknis yang diperlukan untuk melakukannya. Pemberi Lisensi melepaskan dan/atau setuju untuk tidak menegaskan hak atau wewenang apa pun untuk melarang Anda membuat modifikasi teknis yang diperlukan untuk menggunakan Hak Berlisensi, termasuk modifikasi teknis yang diperlukan untuk menghindari Tindakan Teknologi yang Efektif. Untuk tujuan Lisensi Publik ini, hanya membuat modifikasi yang disahkan oleh Bagian 2 (a) (4) ini tidak pernah menghasilkan Materi yang Diadaptasi.
5. Penerima hilir.
 - A. Penawaran dari Pemberi Lisensi - Materi Berlisensi. Setiap penerima Materi Berlisensi secara otomatis menerima tawaran dari Pemberi Lisensi untuk menggunakan Hak Berlisensi berdasarkan syarat dan ketentuan Lisensi Publik ini.
 - B. Penawaran tambahan dari Pemberi Lisensi — Materi yang Diadaptasi. Setiap penerima Materi Adaptasi dari Anda secara otomatis menerima tawaran dari Pemberi Lisensi untuk menggunakan Hak Berlisensi dalam Materi yang Diadaptasi di bawah ketentuan Lisensi Adaptor yang Anda terapkan.
 - C. Tidak ada batasan hilir. Anda tidak boleh menawarkan atau memaksakan syarat atau ketentuan tambahan atau berbeda pada, atau menerapkan Tindakan Teknologi Efektif apa pun pada, Materi Berlisensi jika hal itu membatasi pelaksanaan Hak Berlisensi oleh penerima Materi Berlisensi mana pun.
6. Tidak ada dukungan. Tidak ada dalam Lisensi Publik ini yang merupakan atau dapat ditafsirkan sebagai izin untuk menegaskan atau menyiratkan bahwa Anda adalah, atau bahwa penggunaan Materi Berlisensi oleh Anda, terhubung dengan, atau disponsori, didukung, atau

diberikan status resmi oleh, Pemberi Lisensi atau orang lain yang ditunjuk untuk menerima atribusi sebagaimana diatur dalam Bagian 3 (a) (1) (A) (i).

b. Hak lainnya.

1. Hak moral, seperti hak integritas, tidak dilisensikan di bawah Lisensi Publik ini, juga publisitas, privasi, dan/atau hak kepribadian serupa lainnya; namun, sejauh mungkin, Pemberi Lisensi melepaskan dan/atau setuju untuk tidak menegaskan hak-hak tersebut yang dimiliki oleh Pemberi Lisensi sejauh yang diperlukan untuk memungkinkan Anda menggunakan Hak Berlisensi, tetapi tidak sebaliknya.
2. Hak paten dan merek dagang tidak dilisensikan berdasarkan Lisensi Publik ini.
3. Sedapat mungkin, Pemberi Lisensi melepaskan hak apa pun untuk mengumpulkan royalti dari Anda untuk pelaksanaan Hak Berlisensi, baik secara langsung atau melalui masyarakat pengumpul di bawah skema lisensi hukum atau wajib sukarela atau yang dapat diabaikan. Dalam semua kasus lain, Pemberi Lisensi secara tegas berhak untuk mengumpulkan royalti tersebut.

Bagian 3 - Ketentuan Lisensi.

Pelaksanaan Hak Berlisensi Anda secara tegas dibuat dengan tunduk pada ketentuan berikut.

a. Atribusi.

1. Jika Anda Membagikan Materi Berlisensi (termasuk dalam bentuk yang dimodifikasi), Anda harus:
 - A. mempertahankan hal-hal berikut jika disediakan oleh Pemberi Lisensi dengan Materi Berlisensi:

i . identification of the creator(s) of the Licensed Material and any others designated to receive attribution, in any reasonable manner requested by the Licensor (including by pseudonym if designated);

ii . a copyright notice;

iii . a notice that refers to this Public License;

iv . a notice that refers to the disclaimer of warranties;

v . a URI or hyperlink to the Licensed Material to the extent reasonably practicable;

- B. menunjukkan jika Anda memodifikasi Materi Berlisensi dan mempertahankan indikasi modifikasi sebelumnya; dan
 - C. menunjukkan Materi Berlisensi dilisensikan di bawah Lisensi Publik ini, dan termasuk teks, atau URI atau hyperlink ke, Lisensi Publik ini.
2. Anda dapat memenuhi ketentuan dalam Bagian 3 (a) (1) dengan cara apa pun yang wajar berdasarkan media, sarana, dan konteks di mana Anda Membagikan Materi Berlisensi. Misalnya, mungkin masuk akal untuk memenuhi persyaratan dengan menyediakan URI atau hyperlink ke sumber daya yang mencakup informasi yang diperlukan.
 3. Jika diminta oleh Pemberi Lisensi, Anda harus menghapus informasi apa pun yang diperlukan oleh Bagian 3 (a) (1) (A) sejauh dapat dipraktikkan secara wajar.
- b. ShareAlike. Selain ketentuan dalam Bagian 3 (a), jika Anda Membagikan Materi Adaptasi yang Anda hasilkan, ketentuan berikut juga berlaku.
1. Lisensi Adaptor yang Anda terapkan harus berupa lisensi Creative Commons dengan Elemen Lisensi yang sama, versi ini atau yang lebih baru, atau Lisensi Kompatibel BY-SA.
 2. Anda harus menyertakan teks, atau URI atau hyperlink ke, Lisensi Adaptor yang Anda terapkan. Anda dapat memenuhi kondisi ini dengan cara apa pun yang wajar berdasarkan media, sarana, dan konteks di mana Anda Membagikan Materi yang Diadaptasi.
 3. Anda tidak boleh menawarkan atau memaksakan syarat atau ketentuan tambahan atau berbeda pada, atau menerapkan Tindakan Teknologi Efektif apa pun pada, Materi yang Diadaptasi yang membatasi pelaksanaan hak yang diberikan berdasarkan Lisensi Adaptor yang Anda terapkan.

Bagian 4 - Hak Database Sui Generis.

Di mana Hak Berlisensi mencakup Hak Basis Data Sui Generis yang berlaku untuk penggunaan Materi Berlisensi oleh Anda:

- a. untuk menghindari keraguan, Bagian 2 (a) (1) memberi Anda hak untuk mengekstrak, menggunakan kembali, mereproduksi, dan Membagikan semua atau sebagian besar isi database;
- b. jika Anda memasukkan semua atau sebagian besar konten database dalam database di mana Anda memiliki Hak Basis Data Sui Generis, maka basis data tempat Anda memiliki Hak Basis Data

Sui Generis (tetapi bukan konten individualnya) adalah Materi yang Diadaptasi, termasuk untuk tujuan Bagian 3 (b); dan

- c. Anda harus mematuhi ketentuan dalam Bagian 3 (a) jika Anda Membagikan semua atau sebagian besar isi database. Untuk menghindari keraguan, Bagian 4 ini melengkapi dan tidak menggantikan kewajiban Anda berdasarkan Lisensi Publik ini di mana Hak Berlisensi mencakup Hak Cipta dan Hak Serupa lainnya.

Bagian 5 — Penafian Jaminan dan Batasan Tanggung Jawab.

- a. Kecuali jika dilakukan secara terpisah oleh Pemberi Lisensi, sejauh mungkin, Pemberi Lisensi menawarkan Materi Berlisensi apa adanya dan apa pun yang tersedia, dan tidak membuat pernyataan atau jaminan apa pun mengenai Materi Berlisensi, baik tersurat, tersirat, menurut undang-undang, atau lainnya. Ini termasuk, tanpa batasan, jaminan kepemilikan, kelayakan untuk diperjualbelikan, kesesuaian untuk tujuan tertentu, non-pelanggaran, tidak adanya cacat laten atau lainnya, akurasi, atau ada atau tidak adanya kesalahan, baik diketahui atau dapat ditemukan atau tidak. Jika penafian jaminan tidak diizinkan secara penuh atau sebagian, penafian ini mungkin tidak berlaku untuk Anda.
- b. Sedapat mungkin, dalam keadaan apa pun Pemberi Lisensi tidak akan bertanggung jawab kepada Anda atas teori hukum apa pun (termasuk, tanpa batasan, kelalaian) atau lainnya untuk kerugian langsung, khusus, tidak langsung, insidental, konsekuensial, hukuman, teladan, atau kerugian lainnya, biaya, pengeluaran, atau kerusakan yang timbul dari Lisensi Publik ini atau penggunaan Materi Berlisensi, bahkan jika Pemberi Lisensi telah diberitahu tentang kemungkinan kerugian, biaya tersebut, biaya, atau kerusakan. Jika pembatasan tanggung jawab tidak diperbolehkan secara penuh atau sebagian, batasan ini mungkin tidak berlaku untuk Anda.
- c. Penafian jaminan dan pembatasan tanggung jawab yang diberikan di atas harus ditafsirkan dengan cara yang, sejauh mungkin, paling mendekati penafian mutlak dan pengabaian semua tanggung jawab.

Bagian 6 - Jangka Waktu dan Pengakhiran.

- a. Lisensi Publik ini berlaku untuk jangka waktu Hak Cipta dan Hak Serupa yang dilisensikan di sini. Namun, jika Anda gagal mematuhi Lisensi Publik ini, maka hak Anda berdasarkan Lisensi Publik ini berakhir secara otomatis.
- b. Jika hak Anda untuk menggunakan Materi Berlisensi telah diakhiri berdasarkan Bagian 6 (a), hak Anda untuk menggunakan Materi Berlisensi telah berakhir berdasarkan Bagian 6 (a), hak tersebut mengembalikan:

1. secara otomatis pada tanggal pelanggaran disembuhkan, asalkan disembuhkan dalam waktu 30 hari sejak Anda menemukan pelanggaran; atau
 2. setelah pemulihan ekspres oleh Pemberi Lisensi.
- c. Untuk menghindari keraguan, Bagian 6 (b) ini tidak memengaruhi hak apa pun yang mungkin dimiliki Pemberi Lisensi untuk mencari solusi atas pelanggaran Anda terhadap Lisensi Publik ini.
- d. Untuk menghindari keraguan, Pemberi Lisensi juga dapat menawarkan Materi Berlisensi berdasarkan syarat atau ketentuan terpisah atau berhenti mendistribusikan Materi Berlisensi kapan saja; namun, hal itu tidak akan mengakhiri Lisensi Publik ini.
- e. Bagian 1, 5, 6, 7, dan 8 bertahan dari penghentian Lisensi Publik ini.

Bagian 7 - Syarat dan Ketentuan Lainnya.

- a. Pemberi Lisensi tidak akan terikat oleh syarat atau ketentuan tambahan atau berbeda yang dikomunikasikan oleh Anda kecuali secara tegas disetujui.
- b. Setiap pengaturan, pemahaman, atau perjanjian mengenai Materi Berlisensi yang tidak disebutkan di sini terpisah dari dan tidak tergantung pada syarat dan ketentuan Lisensi Publik ini.

Bagian 8 — Interpretasi.

- a. Untuk menghindari keraguan, Lisensi Publik ini tidak, dan tidak boleh ditafsirkan, mengurangi, membatasi, membatasi, atau memaksakan ketentuan pada setiap penggunaan Materi Berlisensi yang secara sah dapat dibuat tanpa izin berdasarkan Lisensi Publik ini.
- b. Sedapat mungkin, jika ada ketentuan dari Lisensi Publik ini yang dianggap tidak dapat dilaksanakan, maka akan secara otomatis direformasi sejauh minimum yang diperlukan untuk membuatnya dapat ditegakkan. Jika ketentuan tidak dapat direformasi, itu akan diputuskan dari Lisensi Publik ini tanpa mempengaruhi keberlakuan syarat dan ketentuan yang tersisa.
- c. Tidak ada syarat atau ketentuan Lisensi Publik ini yang akan dibebaskan dan tidak ada kegagalan untuk mematuhi persetujuan kecuali secara tegas disetujui oleh Pemberi Lisensi.
- d. Tidak ada dalam Lisensi Publik ini yang merupakan atau dapat ditafsirkan sebagai pembatasan, atau pengabaian, hak istimewa dan kekebalan apa pun yang berlaku untuk Pemberi Lisensi atau Anda, termasuk dari proses hukum yurisdiksi atau otoritas mana pun.

Riwayat dokumen

Tabel berikut menjelaskan perubahan pada dokumentasi SPEKE.

SPEKE v1

Perubahan	Deskripsi	Tanggal
Matriks dukungan: Layanan dan produk AWS Partner	Menambahkan bagian baru untuk Dukungan SPEKE di layanan dan produk AWS Partner, mencantumkan layanan Bitmovin.	13 Januari 2023
Pembaruan untuk penyedia platform DRM	Menambahkan tautan dan informasi mitra baru ke daftar penyedia platform DRM.	24 Januari 2019
Sertakan enkripsi pihak ketiga	Memperbarui arsitektur dan deskripsi untuk memperhitungkan enkripsi pihak ketiga.	20 November 2018
Enkripsi Kunci Konten	Ditambahkan pilihan untuk mengenkripsi kunci konten. Sebelum ini, Secure Packager dan Encoder Key Exchange hanya mendukung pengiriman kunci yang jelas.	30 Oktober 2018
Matriks Dukungan - AWS Elemental Live	Menambahkan matriks dukungan AWS Elemental Live.	27 September 2018
Komponen muatan standar	Ditambahkan bagian yang mendefinisikan elemen utama dalam payload JSON.	27 September 2018

Perubahan	Deskripsi	Tanggal
KID mengesampingkan	Menambahkan bagian tentang penggantian KID oleh penyedia kunci.	27 September 2018
Tautan yang dikoreksi ke situs DASH-IF	Tautan yang dikoreksi ke situs DASH IF untuk spesifikasi CPIX dan untuk halaman ID sistem.	27 September 2018
Salinan rilis untuk AWS Elemental Live	Memperbarui dokumentasi SPEKE untuk menyertakan produk AWS Elemental.	Juli 20, 2018
CMAF	Memperbarui tabel matriks dukungan untuk layanan untuk menyertakan Format Aplikasi Media Umum (CMAF).	27 Juni 2018
Rilis awal	Rilis awal Secure Packager dan Encoder Key Exchange (SPEKE) versi 1, spesifikasi untuk komunikasi antara enkripsi konten dan penyedia kunci DRM. Penyedia kunci DRM mengekspos Secure Packager dan Encoder Key Exchange API untuk menangani permintaan kunci yang masuk.	27 November 2017

SPEKE v2

Perubahan	Deskripsi	Tanggal
Pembaruan untuk bagian penyedia platform DRM	Menambahkan mitra baru yang memenuhi syarat ke	9 Agustus 2023

Perubahan	Deskripsi	Tanggal
	kolom SPEKE v2 dari daftar penyedia platform DRM.	
Pembaruan untuk bagian contoh panggilan metode alur kerja Live dan VOD	Menambahkan header respons X-Speke-Version yang hilang di bagian contoh panggilan metode alur kerja SPEKE v2 Live dan VOD.	13 Januari 2023
Pembaruan untuk penyedia platform DRM dan bagian kontrak Enkripsi	Menambahkan mitra baru yang memenuhi syarat ke kolom SPEKE v2 dari daftar penyedia platform DRM. Menambahkan dua contoh baru kontrak Enkripsi, dan mengubah resolusi SD max menjadi 1024x576 di semua contoh yang bersangkutan.	27 Januari 2022
Rilis awal	Rilis awal Secure Packager dan Encoder Key Exchange (SPEKE) versi 2.0, spesifikasi untuk komunikasi antara enkripsi konten dan penyedia kunci DRM. Penyedia kunci DRM mengekspos Secure Packager dan Encoder Key Exchange API untuk menangani permintaan kunci yang masuk.	7 September 2021

Glosarium AWS

Lihat terminologi AWS terbaru di [AWS glosarium](#) dalam Referensi Glosarium AWS.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.