Theater Key Retrieval (TKR)

A System for Automated KDM Delivery

1 Introduction

In Digital Cinema, the generation of KDMs is typically a highly automated process. However the delivery of those KDMs to the equipment in the field has been performed by various ad hoc delivery mechanisms. Worse, these mechanisms either rely on proprietary VPNs or are plagued with manual workflows (e.g. email with attachments, USB sticks, etc.).

This document will provide a simple standardized framework for the automated delivery of KDMs from service providers to equipment in the theaters using the Internet. In addition, TKR aims to be both secure and easy to implement for device vendors as well as service providers.

2 Overview

So far, most of the proposed network-based delivery mechanisms require that a theater enable a server that listens for incoming connections from the Internet. In such an approach, each theater would be burdened with such tasks as: obtaining static IP addresses (or coping with the challenges of dynamic ones), managing DNS records, configuring proper firewalls to permit inbound connections, and maintaining the specifics in the TDL.

TKR attempts to resolve these issues by choosing that devices *in the theater* initiate the network connection. Doing so eliminates all of the above IT requirements at the theater.

In TKR, KDMs are simply published on a website, and automatically retrieved by devices in the field. These devices will, in essence, identify URLs from within their CPLs and use these URLs to retrieve their KDMs.

3 Requirements

The requirements associated with TKR are split across two entities: the *Content Author* and the *In-Theater Device*.

3.1 Content Requirements

TKR enabled content shall be identified by the content's Composition Playlist. The CPL's `Issuer` element shall contain the XML attribute: `language="x-TKR"`. The text value of the `Issuer` element shall be a URL whose scheme is either "`http`" or "`https`". This URL, when concatenated with the hex encoded thumbprint of a Security Manager's leaf certificate, shall resolve to a KDM Bundle containing all authorized KDMs for that combination of device and CPL.

Note: The URL found in the `Issuer` field of the CPL is termed the "Base URL", while the final URL formed by concatenating the thumbprint is termed the "Bundle URL".

The Base URL shall be unique to the CPL in which it is contained. This uniqueness may be achieved using that CPL's own `Id` value.

3.1.1 Certificate Thumbprint

The Certificate Thumbprint used to form the Bundle URL shall be computed as per Section 5.4 of SMPTE 430-2. In order to be URL safe (i.e. not to require special URL encoding), the value shall be represented in base-16 (i.e. hex) using the symbols `0-9` and the lower-case symbols `a-f`.

3.2 Device Requirements

In the theater, TKR capable devices may include Screen Management Systems, Theater Management Systems or Security Managers. Regardless of the type, the requirements are identical. The following section outlines the requirements for in-theater devices that support TKR.

3.2.1 Internet Connectivity

TKR capable devices shall have outbound access to the Internet, and should be configured to resolve hostnames with DNS. Outbound TCP connections on port 80 and 443 shall not be restricted. There is no requirement for incoming connections from the Internet.

3.2.2 KDM Retrieval

A TKR device shall periodically perform the following steps on each piece of *encrypted* content to which it has access[1]:

1) Examine the `Issuer` element of the CPL. If its `language` attribute is "`x-TKR`" then proceed.
2) Extract the text value of the `Issuer` element which shall be the Base URL.
3) Form the Bundle URL by appending the hex encoded thumbprint of the Security Manager's leaf certificate to the Base URL.
4) Perform an HTTP GET[2] on the Bundle URL.

[1] If the TKR device is acting on behalf of more than one Security Manager (e.g. a TMS), then it should in turn, perform these steps for each Security Manager to which is has access.

5) The response shall be a KDM Bundle (served with the HTTP Header "`Content-Type: application/tar`").

6) Unpack the KDM Bundle and ingest all of the resultant KDMs that have not yet been ingested.

If no KDMs are authorized at that moment, the device should expect the server to respond with the HTTP Status "`404 Not Found`". Such a response shall imply nothing about the future availability of KDMs.

3.2.3 KDM Delivery Receipt

TKR enabled devices should acknowledge the successful ingest of all *new* KDMs they receive. This acknowledgment shall be made by performing an HTTP POST request to the corresponding CPL's Base URL once for each new KDM ingested. The content of the request shall be the `MessageId` of the ingested KDM.

If the server responds with the HTTP Status "`405 Method Not Allowed`" then the device should not retry. On all other errors, the device should retry the POST each day until either success or the KDM has expired.

3.2.4 Automated Polling Interval

TKR capable devices should automatically perform the steps outlined in Section 3.2.2 once per hour per applicable CPL. This rate ensures a balance between the operational needs of the exhibitor and the desire to minimize load on the KDM host. This interval should be extended to 6 hours for any CPL currently unlocked with an active KDM that does not expire in the next 24 hours.

3.2.5 Manual Polling

The Graphical User Interface (GUI) of a device supporting TKR should provide the means for an operator to manually initiate a request for KDMs with no regard to the above Polling Interval.

3.2.6 HTTP Feature Support

TKR capable devices shall include support for the following features of HTTP:

1) HTTP Redirects

2) Basic Access Authentication including the ability to extract credentials from URLs.

TKR capable devices should support:

1) ETags when requesting KDM Bundles in order to promote efficient caching.

2) Persistent Connections (a.k.a. HTTP keep-alive).

[2] Implementations may perform multiple KDM Bundle requests asynchronously so as to preclude any one host from blocking timely access to others.

4 Samples (Informative)

4.1 CompositionPlaylist Sample

The following CompositionPlaylist is a valid instance of a TKR enabled CPL.

```
<?xml version="1.0" encoding="UTF-8"?>
<CompositionPlaylist xmlns="http://www.smpte-ra.org/schemas/429-7/2006/CPL">
  <Id>urn:uuid:bddf9ba8-bb98-4bdc-97b0-4e4e0cf13d13</Id>
  <IssueDate>2011-11-01T18:41:09-07:00</IssueDate>
  <Issuer language="x-TKR">http://example.org/bddf9ba8-bb98-4bdc-97b0-4e4e0cf13d13/</Issuer>
  <Creator>Studio A</Creator>
  <ContentTitleText>The Jazz Singer</ContentTitleText>
  <ContentKind>feature</ContentKind>
...
```

4.2 Base URL Samples

The following are example Base URLs that could be found within a CompositionPlaylist having an `Id` of `bddf9ba8-bb98-4bdc-97b0-4e4e0cf13d13`. They highlight the different approaches that a service provider might take in designing both their URLs and server-side architecture:

```
http://example.org/kdm-download.php?cpl-id=bddf9ba8-bb98-4bdc-97b0-4e4e0cf13d13&dev-thumbprint=

https://bob:secret@provider.com/bddf9ba8-bb98-4bdc-97b0-4e4e0cf13d13/

https://kdms.studio.com/bddf9ba8-bb98-4bdc-97b0-4e4e0cf13d13/
```

Each Base URL above is designed to have appended any Certificate Thumbprint to form the Bundle URL. For example in the case of the last URL above, a server with the base64 Certificate Thumbprint "`HJgYRs2pYrt6NI390gPtdfZhs9g=`" would append "`1c981846cda962bb7a348dfdd203ed75f661b3d8`", resulting in the following Bundle URL:

```
https://kdms.studio.com/bddf9ba8-bb98-4bdc-97b0-4e4e0cf13d13/1c981846cda962bb7a348dfdd203ed75f661b3d8
```

5 References

[RFC1738] "Uniform Resource Locators (URL)", 1994. IETF RFC 1738. See:
http://www.ietf.org/rfc/rfc1738.txt

[RFC2616] "Hypertext Transfer Protocol – HTTP/1.1", 1999. IETF RFC 2616. See:
http://www.ietf.org/rfc/rfc2616.txt

[HTTP AUTH] "HTTP Authentication: Basic and Digest Access Authentication", 1999. IETF RFC 2617. See
http://www.ietf.org/rfc/rfc2617.txt

[KDM] SMPTE 430-1-2006, D-Cinema Operations – Key Delivery Message

[KDMb] SMPTE 430-9-2008, D-Cinema Operations – Key Delivery Bundle

[DCERT] SMPTE 430-2-2006, D-Cinema Operations – Digital Certificate

[CPL] SMPTE 429-7-2006, D-Cinema Packaging – Composition Playlist