WIDEVINE®

CYPHER FOR DIGITAL MEDIA

BROWSER CLIENT INTEGRATION

VERSION: 1.5

Widevine Technologies

901 5th Ave, Suite 3400

Seattle, WA 98164 USA

www.widevine.com

206.254.3000 voice

206.254.3001 fax

sales@widevine.com

WIDEVINE®

CONTENTS

Document Status Sheet

Document Name	Widevine_Cypher_Browser_Client_Integration.docx			
Status	~~Work In Progress~~	~~Draft~~	Issued	~~Closed~~
Distribution Restrictions	~~Author~~	~~Internal~~	Partner/Customer	~~Public~~

Key to Document Status Codes:

Status

- Work In Progress – An incomplete document, designed to guide discussion and generate feedback. This may include multiple alternatives for consideration.
- Draft – A document that is, for the most part, complete, but not reviewed. Drafts are susceptible to substantial change.
- Issued – A stable document which has undergone rigorous review and is suitable for product development, cross-vendor interoperability, and certification testing.
- Closed – A static document that has been reviewed, tested, validated and closed to all further change requests. A document that represents the product "AS IS".

Distribution Restrictions

- Author – This document may be consumed by the document author or authors.
- Internal – This document may be consumed by Widevine employees only.
- Partner / Customer – This document may be consumed by Widevine partners and customers.
- Public – This document may be consumed by anyone.

Version	Date	Description	By
1.0	08/30/2010	Updates for 4.4.5 release	Alex Lee
1.1	10/11/2010	Updates for 4.5.0 release	Alex Lee
1.2	1/24/2011	Updated newer client releases Added how to sign browser plugins	Alex Lee
1.3	4/11/2011	Updated client release and supported platforms Add section on user-level IE plugin	Alex Lee
1.4	4/30/2011	Updated client release – 4.5.0.3485	Alex Lee
1.5	6/25/2011	Updated client release – 4.5.0.3913 Added description of Flash demo player	Alex Lee

1. PURPOSE

The purpose of this document is to describe the Widevine browser plugin client integration in a Flash video player application.

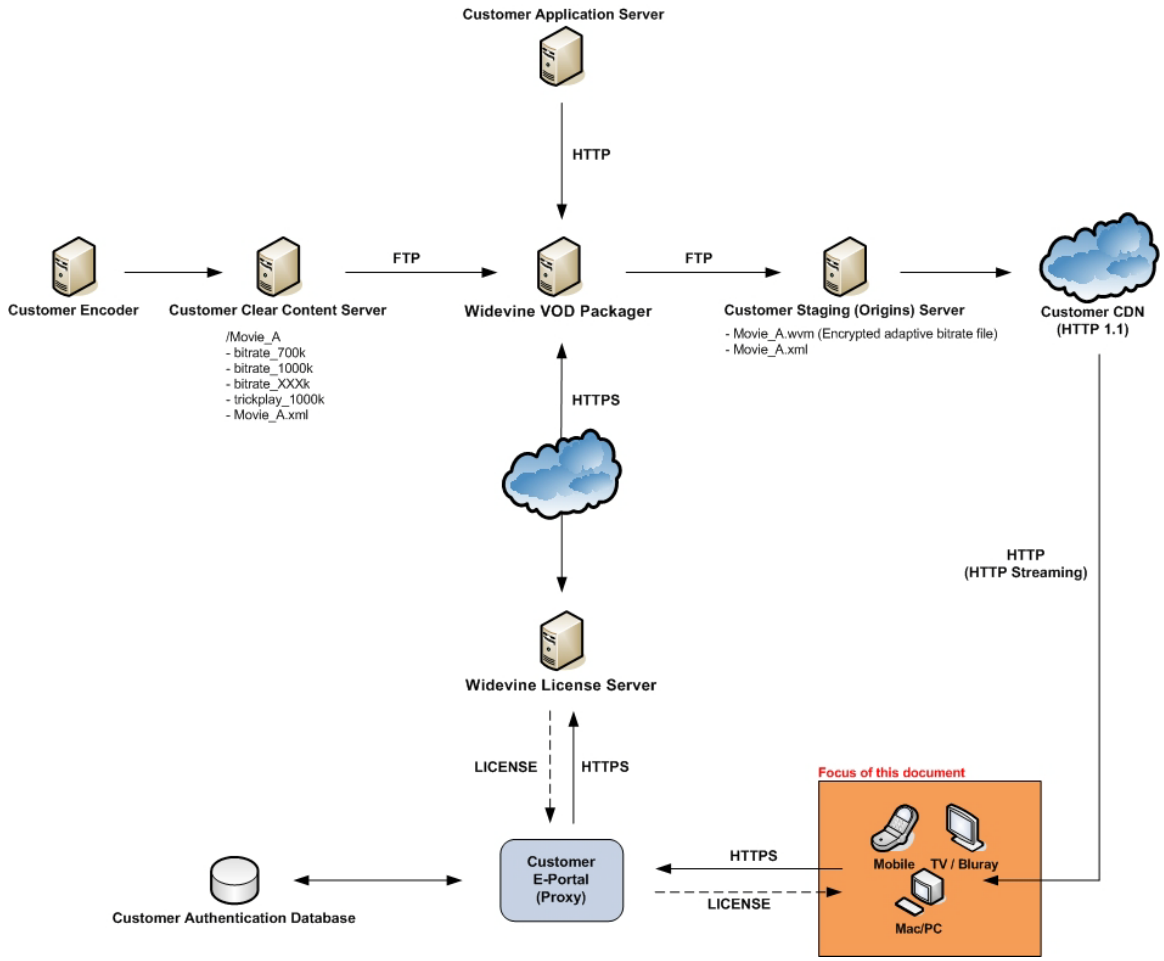

FIGURE 1 – CYPHER DIGITAL MEDIA VOD COMPONENT DIAGRAM

1.1. CYPHER FOR DIGITAL MEDIA CLIENT

The client software resides on the Device (Internet connected TV, Blu-ray player, PC/Apple product, gaming platform, mobile, etc.). The client is responsible for the DRM, adaptive streaming, fast startup, DVD-like trick-play and chaptering.

2. TERMS AND ABBREVIATIONS

- **Asset -** Physical media such as H.264-encoded movie
- **Catcher** - A temporary storage device used to collect on- demand files and request missing parts (due to unreliable transport) prior to provisioning of content to the video delivery servers
- **Container -** A container format is a computer file format that can contain various types of data, compressed by means of standardized audio/video codecs
- **Content -** Assets and metadata files
- **Digital Rights Management (DRM)**-security software to allow a Service Provider to implement business rules which control a consumer's access to digital media.
- **Client device -** the equipment used by consumers to view digital media.
- **License**- Encrypted data that contains the viewing rights associated with digital media and the key to unlock the content key.
- **E-portal-** The software external to, and interacting with Widevine to facilitate the delivery of secure content to the client device.
- **ID** – Identification
- **Virtual Smart Card (VSC)** – the Widevine for Digital Media DRM client.

3. FILE LOCATIONS

1. Release Notes
    a. 4.5.0.3913
        i. http://wstfcps005.shibboleth.tv/demo/450/4503913.Release.Notes.pdf
2. Browser plugin clients
    a. 4.5.0.3913
        i. http://wstfcps005.shibboleth.tv/demo/450/plugins.4503913.tar.gz
3. Flash demo player application
    a. 4.5.0.3913
        i. http://wstfcps005.shibboleth.tv/demo/450/demo_player_4503913.tar.gz
4. Flash Actionscript libraries
    a. 4.5.0.3913
        i. http://wstfcps005.shibboleth.tv/demo/450/com.4503913.tar.gz

3.1. USING THE WIDEVINE FLASH DEMO PLAYER (BROWSER PLUGIN)

Un-tar file to a valid web-server directory. Load index.html in a web browser via HTTP url (not file://). Install plugin when prompted. Restart browser (or refresh). Select content and hit Start.

The configuration file is WidevineMediaTransformer.js

The Flash player has basic playback controls. The bitrate indicator will only display 6 bitrates (if the content has more than 6 bitrates, it will display the first 5 and the last highest bitrate). Clicking on a bitrate will force a manual adaptation to that bitrate. Clicking on the bitrate currently being played (once manual adaptation is toggled) will re-enable automatic bitrate adaptation.

4. SUPPORTED PLATFORMS

The Cypher for Digital Media solution for the PC and Macintosh provides the service provider with studio approved DRM as well as adaptive streaming, DVD like fast startup and trick play as well as chaptering.

4.1. SUPPORTED OPERATING SYSTEMS

Operating System	Version	Service Pack	User
Windows XP	Home	SP2 and SP3	Administrator and Guest
Windows XP	Professional	SP2 and SP3	Administrator and Guest
Windows Vista	Home	SP1 and SP2	Non-Administrator and Administrator
Windows Vista	Business	SP1 and SP2	Non-Administrator and Administrator
Windows 7	Ultimate	N/A	Standard and Standard
Macintosh OS X (Intel)	10.5	N/A	Administrator
Macintosh OS X (Intel)	10.6	N/A	Administrator

4.2. SUPPORTED BROWSERS

Browser	Version	Plugin
Internet Explorer	7 , 8, 9	activex / .exe
FireFox (Windows and Macintosh)	3.x, 4.x, 5.x	xpi
Safari (Macintosh)	5.x	dmg
Chrome (Windows and Macintosh)	10, 11, 12	exe / dmg

5. HOSTING THE PLUGIN

As noted above, the Widevine VSC for the PC and Macintosh are browser plugins. They integrate into a Flash player via the addition of a small amount of ActionScript in the .fla that will be used to delivery video on the e-portal.

The Widevine plugin accepts an RTMP connection from the Flash player as well as makes an HTTP connection to the content server to request the video. The content is sent to the flash player over the RTMP connection.

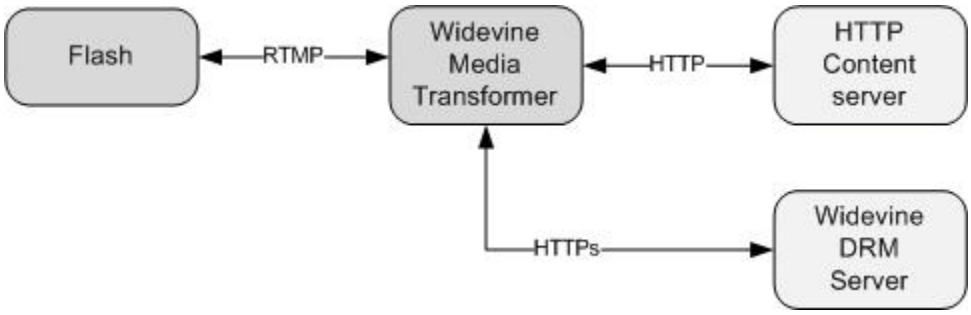

FIGURE 1 - CLIENT FLOW DIAGRAM

6. Flash Player (SWF) Integration

There are several classes, WvNetConnection and WvNetStream, that Widevine provides to streamline the integration. Use these classes instead of NetConnection and NetStream.

- WvNetConnection, which inherits from NetConnection
- WvNetStream, which inherits from NetStream

6.1. HTTP STREAMING

The program in the right column below shows an example of how to integrate the Widevine client into ActionScript to support HTTP streaming. The implementation resembles the model for RTMP, therefore the call to nc.connect() is passed the URL which is valid rather than NULL, as is typical in the case of HTTP.

	`Import com.widevine.*;`
`var nc:NetConnection = new NetConnection();`	`var nc:WvNetConnection = new WvNetConnection();`
`var theURL:String = new String();`	`var theURL:String = new String();`
`theURL = "http://10.150.1.20/flash/video.flv";`	`theURL = http://<cdn.url>/flash/`
`theMovie = "video.flv"`	`theMovie = "video.vob"`
`nc.connect(null);`	`nc.connect(theURL + theMovie);`
`var ns:NetStream = new NetStream(nc);`	`var ns:WvNetStream = new WvNetStream(nc);`
`theVideo.attachVideo(ns);`	`theVideo.attachVideo(ns);`
`ns.play(theURL + theMovie);`	`ns.play(theMovie);`

6.2. WvNetStream

The WvNetStream class inherits from flash.net.NetStream. The followings public methods are defined:

Method	Description
play	Calls super.play() and starts a local timer. The entire URL can be specified or only the movie name. **`public function play(… arguments):void`**
pause	Sets the play scale to 1 and calls super.pause() **`public function pause():void`**
resume	Sets the play scale to 1 and calls super.resume() **`public function resume():void`**
close	Stops the local timer and calls super.close() **`public function close():void`**
playForward	If the play scale is <= 1, sets the play scale to 4. Otherwise increases the play scale by a factor of 2 in the forwards direction. **`public function playForward():void`**
playRewind	If the play scale is >= 1, sets the play scale to -4. Otherwise increases the play scale by a factor of 2. In the reverse direction. **`public function playRewind():void`**
getCurrentMediaTime	Returns the correct media time (position of playhead) in seconds. If the play scale is not 1, this method must be used to get the correct time. **`public function getCurrentMediaTime():Number`**
getPlayScale	Returns the current play scale or speed (e.g. - a value of 1 indicates normal play; 4 indicates 4 times normal play). **`public function getPlayScale():int`**
getCurrentBitrate	Returns the current bitrate in bytes/second
getBitrates	Returns an array of supported bitrates for the current stream **`public function getBitrates():Array`**

getCurrentQualityLevel	Returns the current quality level as measured by current bitrate given min/max bitrates. **`public function getCurrentQualityLevel():int`**
getMaxQualityLevel	Returns the maximum quality level. **`public function getMaxQualityLevel():int`**
selectTrack	Sets the desired bitrate to use. The index into the list of bitrates is specified instead of the actual bitrate. Adaptation is disabled when this function is used to manually select a bitrate. To turn adaptation back on, call this function with the previous value or with a 0. **`public function selectTrack(trackIndex:int):void`**
getNumChapters	Returns the number of chapters in this asset. A value of -1 is returned if chapter data is not yet available. **`public function getNumChapters():int`**
getChapter	Returns a WvChapter object **`public function getChapter(chapterNumber:int):WvChapter`**
isChaptersReady	Returns true if chapter data is ready, otherwise false. Generally chapter data is ready within a few seconds of initial playback. **`public function isChaptersReady():Boolean`**

6.3. WvNetConnection

The WvNetConnection class inherits from flash.net.NetConnection. This class communicates with the Widevine plugin using RTMP protocol. The Widevine plugin creates an HTTP connection to the content server.

Method	Description
connect	This method will call a Widevine function WVGetURL() using *ExternalInterface.call()* to translate the passed in HTTP URL to an RTMP URL using the localhost. Exceptions throws: Error – if connect() fails, an exception is thrown containing an error string. Use WvNetConnection::getErrorText() for additional error message. **`public function connect(command:String, … arguments):void`**
getNewURL	Returns the translated URL. **`public function getNewURL():String`**
getErrorText	Returns additional error message in the event of connect() failure. **`public function getErrorText():String`**

6.4. WvChapter

The WvChapter class provides access to the chapter information contained in the movie.

Method	Description
getBitmap	Returns a bitmap object containing the chapter image **`public function getBitmap():Bitmap`**
getIndex	Returns the time index into the movie where the chapter starts **`Public function getIndex():Number`**
getName	Returns the name of this chapter **`Public function getName():String`**
hasBitmap	Returns true if this chapter contains a bitmap image, otherwise returns false. **`public function hasBitmap():Boolean`**

7. Hosting Widevine Cypher VSC Client

The Widevine Cypher VSC client is hosted and served to devices by the customer. To host the client, place it on an HTTP server in the directory that is configured in the Widevine Media Transformer JavaScript configuration file. It is a requirement that the compressed installation image be signed to guarantee authenticity and minimize tampering.

8. Hosting the Widevine Cypher Configuration Script

A server side configuration file, WidevineMediaTransformer.js, is used to configure devices to talk to the client download servers and to the license server. The configuration script is server-side JavaScript. When included in the body of the customer HTML page, the JavaScript will provide the URLs that the target device will use to download the Widevine Cypher VSC client, the URLs of where to obtain licenses, the URLs of where to log usage information, and the information to initiate client installation.

The next section describes the lines that will need to be edited in the JavaScript.

8.1. CONFIGURING THE WIDEVINEMEDIATRANSFORMER.JS FILE

To include the WidevineMediaTransformer.js into a web page, add this line into the body of the page:

```
<script type="text/javascript" language="javascript"
src="WidevineMediaTransformer.js"></script>
```

The variables that need to be configured in the JavaScript are:

```
//plugin download locations
var windows_activex_installer_exe    = "<Path>/WidevineMediaTransformer.exe";
var windows_activex_location_cab     = "<Path>/WidevineMediaTransformer.cab";
var windows_activex_location_xp_cab  =
"<Path>/WidevineMediaTransformer_xp.cab";
var windows_firefox_location         =
"<Path>/WidevineMediaTransformer_windows.xpi";
var macintosh_firefox_location       =
"<Path>/WidevineMediaTransformer_osx.xpi";
var safari_location                  = "<Path>/WidevineMediaTransformer.dmg";


//SignOn, License (EMM), and logging URLS
//Staging wstfcps005.shibboleth.tv, Production fcpstage.shibboleth.tv
var signon_url  = "https://<LicenseServerPath>/widevine/cypherpc/cgi-
bin/SignOn.cgi";
var log_url     = "https://<LicenseServerPath>/widevine/cypherpc/cgi-
bin/LogEncEvent.cgi";
var emm_url     =
"https://<LicenseServer_or_ProxyServerPath>/widevine/cypherpc/cgi-
bin/GetEMMs.cgi";

//Portal ID (Provider Identifier)
var portal = "IDM";
```

For further information, please contact your Widevine Program Manager.

Note: The idm_emm_url will be the proxy code on the Customer HTTP server when user-based DRM is being used.

The following sequence diagram shows the installation of the DRM client.

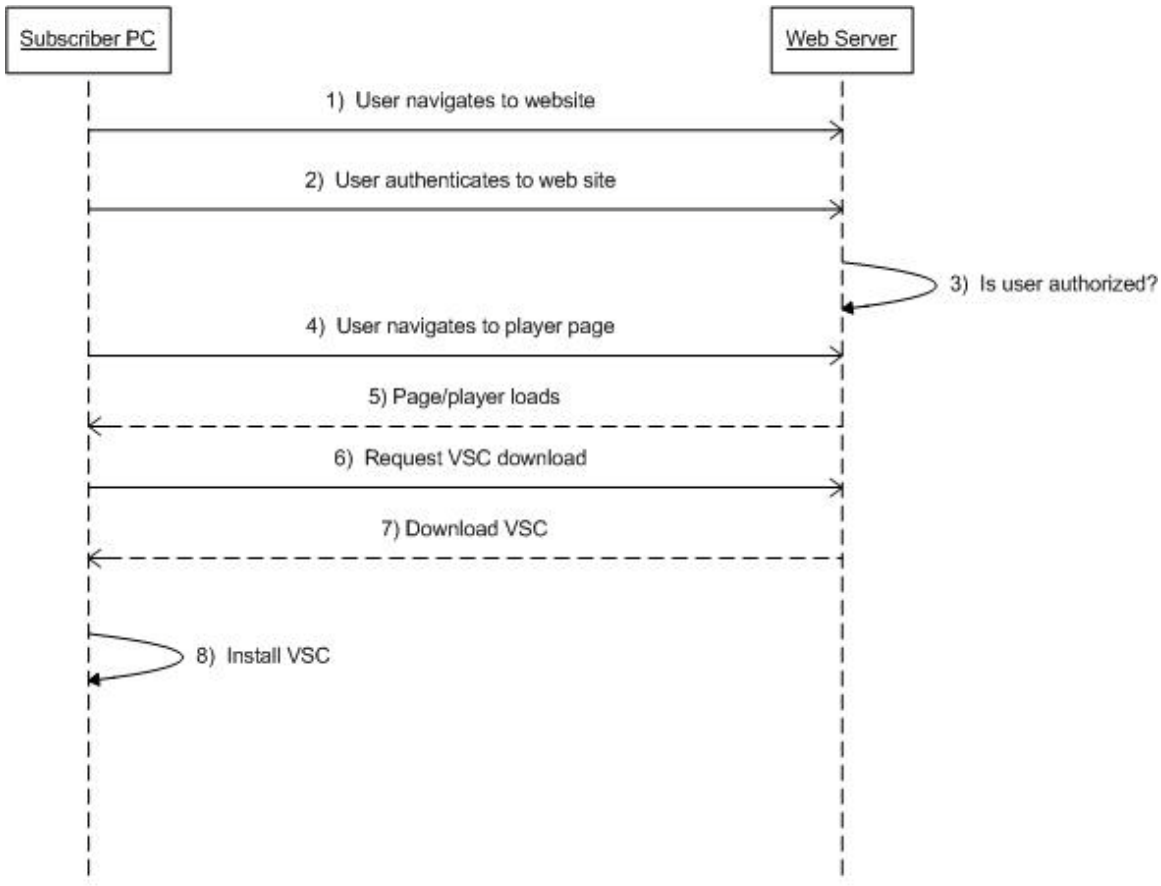

FIGURE 2 - VSC INSTALLATION

9. WIDEVINE CYPHER CLIENT EVENTS

The Widevine Cypher VSC client will send notification through the NetStream object.

The following events are published as "NetStatusEvent.NET_STATUS" and will show up if a handler is registered as follows:

```
myNetStream.addEventListener(NetStatusEvent.NET_STATUS,
netStatusHandler);
```

9.1. FLASH EVENTS

Code	Description
NetStream.Wv.EmmSuccess	EMM was successfully granted. *details*- returns the length of the license in seconds. *description*- contains the movie name
NetStream.Wv.EmmFailed	The user attempted to play an asset without authorization. *details*–contains the error code. *description*–contains the movie name
NetStream.Wv.EmmError	Widevine was not able to receive an EMM for the encrypted asset, possibly due to network errors. *details*–contains the error code. *description* - contains the movie name
NetStream.Wv.EmmExpired	The EMM has expired. This can occur if the EMM was valid when playback started but expired during playback. *details* – returns detail string.. *description* - contains the movie name
NetStream.Wv.SwitchUp	Widevine media switched to a higher bitrate. *default* -returns the current bitrates(separated by semicolons) in bytes/second and an index (following the colon) indicating the current bitrate. The format is as follows: <bitrate1>;<bitrate 2>;…;<bitrate n>:<index> *For* example: 187657;125142;250142;87638:3 The above example shows 4 bitrates in the order the file was encoded. The current bitrate is the 3rd listed which is 2.5 Mb/s. *description* - contains the movie name
NetStream.Wv.SwitchDown	Widevine media switched to a lower bitrate. *details* - returns current bitrates in bytes/second and an index. *description*– contains the movie name
NetStream.Wv.LogError	Widevine attempted to log a message and was not successful. *details* - returns numeric value representing the error code.
NetStream.Wv.DcpStop	Widevine detected an illegal attempt to copy protected

	content. Decryption will stop and the asset will stop playing. The NetStream and NetConnection objects should be closed at this time.
NetStream.Wv.DcpAlert	Widevine detected an illegal attempt to copy protected content. Decryption will continue and the asset will continue to play.

10. REGION-BASED DRM

Content can be encrypted with geofiltering in the policy which will allow a license for the content to only be issued if the device is in an allowed region. When geo-filtering is used there is no additional integration between the e-portal and Cypher. As a secondary check, the time zone for the allowed region is also confirmed for accuracy.

11. USER-BASED DRM

Please refer to Proxy Integration documentation.

12. ENHANCED SEEK

The enhanced seek support within the Cypher VSC provides the user random access within the video during a progressive download. This enables the user to move anywhere within the asset instantly and can be used as a foundation for bookmarks.

To use the enhanced seek functionality in the Cypher VSC, simply use the Flash Netstream.seek() command in the SWF's ActionScript. Several examples include:

```
// Seek to beginning
my_netsream.seek(0);

// Seek to 3600 (one hour) seconds into the movie
my_netsream.seek(3600);

// Seek backwards 30 minutes
my_netsream.seek(my_netsream.time - 1800);
```

13. INTERNET EXPLORER USER LEVEL PLUGIN

To use the user-level IE plugin installer, the browser must prompt to download and install the WidevineMediaTransformerUser.exe.

This allows the plugin installation on Windows systems without administrative privileges. The plugin installer cannot be launched / invoked from the browser or it will prompt for administrative privileges.

14. SIGNING THE WIDEVINE BROWSER PLUGINS

14.1. EXECUTABLE FILES (.EXE)

- Use the Microsoft signing tool.

```
signtool sign /f <Signing Certificate File> /v /t <URL of time stamp
server> WidevineMediaTransformer.exe

signtool sign /f <Signing Certificate File> /v /t <URL of time stamp
server> WidevineMediaTransformerChrome.exe
```

14.2. FIREFOX PLUGINS (.XPI)

- Requires unzipping the file, signing it (using a CertDB) and re-zipping it again.

```
mkdir tmpxpi
cd tmpxpi
unzip ../WidevineMediaTransformer_osx.xpi
cd ..
signtool --verbosity 4 -d <certDB> -p <certDBpwd> -k <certInDB> tmpxpi
cd tmpxpi
zip -rv WidevineMediaTransformer_osx.xpi META-INF/zigbert.rsa
zip -r -D WidevineMediaTransformer_osx.xpi * -x META-INF/zigbert.rsa

(The first file of the .xpi is to be the META-INF/zigbert.rsa file,
then package the rest back in)

Reference: https://developer.mozilla.org/en/Signing_a_XPI
```