

Demuxed, October '24

# PSSH; Primordial Soup of Secure-ish Headers

## Agenda

- Tear apart a few PSSH boxes in real time, bit by bit
- Identify a few design decisions inherent to the scheme specific structures
- Talk through the semantics of those designs

## Protection System Specific Header

- Contains the data needed by a content protection system to play back your media.
- Not required, regardless if the content is protected
- Zero or more, if content is playable under multiple schemes
- Primarily used in conjunction with EME and license requests
- Outside any security boundary

```
aligned(8) class PSSH extends FullBox('pssh', version, flags=0)
{
    unsigned int(8) [16] SystemID;
    if (version > 0)
    {
        unsigned int(32) KID_COUNT;
        {
            Unsigned int(8)[16] KID;
        } [KID_count];
    }
    unsigned int(32) DataSize;
    unsigned int(8) [DataSize] Data;
}
```

```
aligned(8) class PSSH extends FullBox('pssh', version, flags=0)
{
    unsigned int(8) [16]      SystemID;
    unsigned int(32)         DataSize;
    unsigned int(8) [DataSize] Data;
}
```

# Widevine

```
#EXT-X-KEY:METHOD=SAMPLE-AES,URI="data:text/plain;base64,AAAAkn  
Bzc2gAAAAA7e+LqXnWSs6jyCfc1R0h7QAAAHISEMtCZvRtSxeihjNfmx+ZfGQiW  
GV5SmhjM05sZEVsa0Lqb2LPVFUyTLRjMU56RXpNRGt6TORjM056WTNJaXdpZG1G  
eWFXRnVkrWxrSWpvaU9UVTJOVGM0TLRreU1qRXdNakL6TVRFeELuMD1I88aJmwY  
=",KEYID=0xcb4266f46d4b17a286335f9b1f997c64,KEYFORMAT="urn:uuid  
:edef8ba9-79d6-4ace-a3c8-27dcd51d21ed",KEYFORMATVERSION="1"
```

```
mp4dump -v3 widevine.bin
```

```
[pssh] size=12+134
```

```
  system_id = [ed ef 8b a9 79 d6 4a ce a3 c8 27 dc d5 1d 21 ed]
```

```
  data_size = 114
```

```
  data = [12 10 cb 42 66 f4 6d 4b 17 a2 86 33 5f 9b 1f 99 7c 64 22 58 65 79  
4a 68 63 33 4e 6c 64 45 6c 6b 49 6a 6f 69 4f 54 55 32 4e 54 63 31 4e 7a 45  
7a 4d 44 6b 7a 4f 44 63 33 4e 7a 59 33 49 69 77 69 64 6d 46 79 61 57 46 75  
64 45 6c 6b 49 6a 6f 69 4f 54 55 32 4e 54 63 34 4e 54 6b 79 4d 6a 45 77 4d  
6a 49 7a 4d 54 45 78 49 6e 30 3d 48 f3 c6 89 9b 06]
```



```
xxd -g1 widevine.bin
```

```
00000000: 00 00 00 92 70 73 73 68 00 00 00 00 ed ef 8b a9  ....pssh.....
00000010: 79 d6 4a ce a3 c8 27 dc d5 1d 21 ed 00 00 00 72  y.J... ' ...!....r
00000020: 12 10 cb 42 66 f4 6d 4b 17 a2 86 33 5f 9b 1f 99  ...Bf.mK...3_...
00000030: 7c 64 22 58 65 79 4a 68 63 33 4e 6c 64 45 6c 6b  |d"XeyJhc3NldElk
00000040: 49 6a 6f 69 4f 54 55 32 4e 54 63 31 4e 7a 45 7a  Ijoi0TU2NTc1NzEz
00000050: 4d 44 6b 7a 4f 44 63 33 4e 7a 59 33 49 69 77 69  MDkz0Dc3NzY3Iiwi
00000060: 64 6d 46 79 61 57 46 75 64 45 6c 6b 49 6a 6f 69  dmFyaWFudElkIjoi
00000070: 4f 54 55 32 4e 54 63 34 4e 54 6b 79 4d 6a 45 77  0TU2NTc4NTkyMjEw
00000080: 4d 6a 49 7a 4d 54 45 78 49 6e 30 3d 48 f3 c6 89  MjIzMTEwIn0=H...
00000090: 9b 06
```

```
xxd -g1 -l28 widevine.bin
```


```
00000000: 00 00 00 92 70 73 73 68 00 00 00 00 ed ef 8b a9 .....pssh.....  
00000010: 79 d6 4a ce a3 c8 27 dc d5 1d 21 ed y.J... '...!.
```

146 bytes!

It is indeed a PSSH

```
xxd -g1 -l28 widevine.bin
```

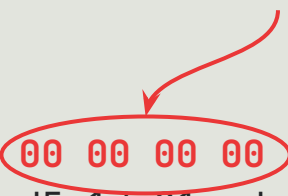
```
00000000: 00 00 00 92 70 73 73 68 00 00 00 00 ed ef 8b a9  ....pssh.....  
00000010: 79 d6 4a ce a3 c8 27 dc d5 1d 21 ed  y.J... '...!.
```



## It's version 0

```
xxd -g1 -l28 widevine.bin
```

```
00000000: 00 00 00 92 70 73 73 68 00 00 00 00 ed ef 8b a9 ....pssh.....  
00000010: 79 d6 4a ce a3 c8 27 dc d5 1d 21 ed y.J... '...!.
```



```
xxd -g1 -l28 widevine.bin
```

```
00000000: 00 00 00 92 70 73 73 68 00 00 00 00 ed ef 8b a9 ....pssh.....  
00000010: 79 d6 4a ce a3 c8 27 dc d5 1d 21 ed y.J...'...!.
```

It's specific to Widevine

```
xxd -g1 -s28 -l4 widevine.bin
```

```
0000001c: 00 00 00 72 ...r
```

114 bytes left

```
xxd -g1 -s32 -l114 widevine.bin
```

```
00000020: 12 10 cb 42 66 f4 6d 4b 17 a2 86 33 5f 9b 1f 99  ...Bf.mK...3_...
00000030: 7c 64 22 58 65 79 4a 68 63 33 4e 6c 64 45 6c 6b  |d"XeyJhc3NldElk
00000040: 49 6a 6f 69 4f 54 55 32 4e 54 63 31 4e 7a 45 7a  Ijoi0TU2NTc1NzEz
00000050: 4d 44 6b 7a 4f 44 63 33 4e 7a 59 33 49 69 77 69  MDkz0Dc3NzY3Iiwi
00000060: 64 6d 46 79 61 57 46 75 64 45 6c 6b 49 6a 6f 69  dmFyaWFudElkIjoi
00000070: 4f 54 55 32 4e 54 63 34 4e 54 6b 79 4d 6a 45 77  0TU2NTc4NTkyMjEw
00000080: 4d 6a 49 7a 4d 54 45 78 49 6e 30 3d 48 f3 c6 89  MjIzMTEwIn0=H...
00000090: 9b 06
```

## Protocol buffers

- Mechanism to serialize structured data into a tightly packed, non-canonical, wire format.
- Discards field names entirely (and therefore semantics)

```
message Foobar {  
    int32 a = 1;  → 1: 150 → 08 96 01  
}
```



12 10 → 00010010 00010000 → 2:LEN, 16 bytes

00000020:	12 10	cb 42 66 f4 6d 4b 17 a2 86 33 5f 9b 1f 99	...Bf.mK...3_...
00000030:	7c 64	22 58 65 79 4a 68 63 33 4e 6c 64 45 6c 6b	d"XeyJhc3NldElk
00000040:		49 6a 6f 69 4f 54 55 32 4e 54 63 31 4e 7a 45 7a	Ijoi0TU2NTc1NzEz
00000050:		4d 44 6b 7a 4f 44 63 33 4e 7a 59 33 49 69 77 69	MDkz0Dc3NzY3Iiwi
00000060:		64 6d 46 79 61 57 46 75 64 45 6c 6b 49 6a 6f 69	dmFyaWFudElkIjoi
00000070:		4f 54 55 32 4e 54 63 34 4e 54 6b 79 4d 6a 45 77	0TU2NTc4NTkyMjEw
00000080:		4d 6a 49 7a 4d 54 45 78 49 6e 30 3d 48 f3 c6 89	MjIzMTEuIn0=H...
00000090:		9b 06	

```
dd status=none skip=32 bs=1 if=widevine.bin | protoscope
```

```
2: {`cb4266f46d4b17a286335f9b1f997c64`}
```

```
4: {
```

```
"eyJhc3NldElkIjoi0TU2NTc1NzEzMDkzODc3NzY3IiwidmFyaWFudElkIjoi0TU2NTc4NTkyMjEwMjIzMTExIn0="
```

```
}
```

```
9: 1667392371
```

```
// (no comment, but key_id tells us everything we need)
```

```
repeated bytes key_id = 2;
```

```
2: {`cb4266f46d4b17a286335f9b1f997c64`}
```

```
// Protection scheme identifying the encryption algorithm.  
// Represented as one of the following 4CC values: 'cenc' (AES-CTR),  
// 'cbc1' (AES-CBC), 'cens' (AES-CTR subsample), 'cbcs'  
// (AES-CBC subsample).  
optional uint32 protection_scheme = 9;
```

9: 1667392371 → [0x63, 0x62, 0x63, 0x73] → cbcs

```
// A content identifier, specified by content provider.  
optional bytes content_id = 4;  
  
4: {  
    "eyJhc3NldElkIjoiOTU2NTc1NzEzMDkzODc3NzY3IiwidmFyaWFudE  
    lkIjoiOTU2NTc4NTkyMjEwMjIzMTE4In0="
```

```
dd status=none skip=52 count=88 bs=1 if=widevine.bin | base64 -d | jq  
  
{  
  "assetId": "956575713093877767",  
  "variantId": "956578592210223111"  
}
```



Always has been

Wait, it's **boxes**  
all the way down?

# PlayReady



#EXT-X-KEY:METHOD=SAMPLE-AES;URI="data:text/plain;char  
rset=UTF-16;base64,AAADYnBzc2gAAAAmgTweZhaQoarkuZb4I  
hfLQAAA0JCAwAAAQABADgDPABXAFIATQBIAEUAQQBEAEUAUgAgAHg  
AbQBsAG4AcwA9ACIAaAB0AHQAcAA6AC8ALwBzAGMAaABLAG0AYQBz  
AC4AbQBpAGMAcgvAvAHMAbwBmAHQALgBjAG8AbQAvAEQAUGBNAC8AM  
gAwADAANwAvADAAMwAvAFAAbABhAHkAUgBLAGEAZAB5AEgAZQBhAG  
QAZQByACIAIAB2AGUAcgvBzAGkAbwBuAD0AIgA0AC4AMwAuADAALgA  
wACIAPgA8AEQAQQBUAEEAPgA8AFAAUgBPFAFQARQBDAFQASQBOAEYA  
TwA+ADwASwBJAEQAUwA+ADwASwBJAEQAIABBAEWARwBJAEQAPQAiA  
EEARQBTAEMAQgBDACIAIABWAEETABVAEUAPQAiAGkAZwBYAEIAdg  
BhADEAZQBVAGcATgBCADQANQB0AEsAUQByAEQAeAA1AHcAPQA9ACI  
APgA8AC8ASwBJAEQAPgA8AC8ASwBJAEQAUwA+ADwALwBQAFIATwBU  
AEUAQwBUAEkATgBGAE8APgA8AEwAQQBfAFUAUgBMAD4AaAB0AHQAc  
ABzADoALwAvAGwAaQBjAC4AZABYAG0AdABvAGQAYQB5AC4AYwBvAG  
0ALwBsAGkAYwBLAG4AcwBLAC0AcABYAG8AeAB5AC0AaABLAGEAZAB  
LAHIAYQB1AHQAaAAvAGQAcgvBtAHQAbwBkAGEAeQAvAFIAaQBnAGgA  
dABzAE0AYQBuAGEAZwBLAHIALgBhAHMAbQB4ADwALwBMAEEAXwBVA  
FIATAA+ADwATABVAEkAXwBVAFIATAA+AGgAdAB0AHAAcwA6AC8ALw  
BwAGwAYQB5AHIAZQBhAGQAeQAtAHUAaQAuAGUAeABhAG0AcABsAGU  
ALgBjAG8AbQA8AC8ATABVAEkAXwBVAFIATAA+ADwARABFAEMAUGBZ  
AFAAVABPAFIAUwBFQAFQAVQBQAD4ATwB0AEQARQBNAEEATgBEADwAL  
wBEAEUAQwBSAFkAUABUAE8AUgBTAEUAVABVAFAPgA8AC8ARABBAF  
QAQQA+ADwALwBXAFIATQBIAEUAQQBEAEUAUgA+AA=" ,KEYFORMAT  
="com.microsoft.playready",KEYFORMATVERSION="1"

```
#EXT-X-KEY:METHOD=SAMPLE-AES,URI="data:text/plain;char  
rset=UTF-16;base64,AAADYnBzc2gAAAAmgTweZhaQoarkuZb4I  
hfLQAAA0JCAwAAAQABADgDPABXAFIATQBIAEUAQQBEAEUAUgAgAHg  
AbQBsAG4AcwA9ACIAaAB0AHQAcAA6AC8ALwBzAGMAaABLAG0AYQBz  
AC4AbQBpAGMAcgBvAHMAbwBmAHQALgBjAG8AbQAvAEQAUGBNAC8AM
```



**I don't even see the code anymore**

```
ALgBjAG8AbQA8AC8ATABVAEKAXwBVAFIATAA+ADwARABFAEMAUGBZ  
AFAAVABPAFIAUwBFQAFQAVQBQAD4ATwBOAEQARQBNAEEATgBEADwAL  
wBEAEUAQwBSAFkAUABUAE8AUgBTAEUAVABVAFAPgA8AC8ARABBAF  
QAQQA+ADwALwBXAFIATQBIAEUAQQBEAEUAUgA+AA=",KEYFORMAT  
="com.microsoft.playready",KEYFORMATVERSION="1"
```

## PlayReady Object

- Length
- PlayReady Object Record Count
- PlayReady Object Records
  - Record Type (PlayReady Header)
  - Record Length
  - Record Value

Intel 8008, UCS-2, SGML walk into a bar...

0000002a: 3c	57	52	4d	48	45	41	44	<.W.R.M.H.E.A.D.
0000003a: 45	52	20	78	6d	6c	6e	73	E.R. .x.m.l.n.s.
0000004a: 3d	22	68	74	74	70	3a	2f	=."h.t.t.p.:./.
0000005a: 2f	73	63	68	65	6d	61	73	/.s.c.h.e.m.a.s.
0000006a: 2e	6d	69	63	72	6f	73	6f	..m.i.c.r.o.s.o.
0000007a: 66	74	2e	63	6f	6d	2f	44	f.t...c.o.m./D.
0000008a: 52	4d	2f	32	30	30	37	2f	R.M./2.0.0.7./.
0000009a: 30	33	2f	50	6c	61	79	52	0.3./P.L.a.y.R.
000000aa: 65	61	64	79	48	65	61	64	e.a.d.y.H.e.a.d.
000000ba: 65	72	22	20	76	65	72	73	e.r.". .v.e.r.s.
000000ca: 69	6f	6e	3d	22	34	2e	33	i.o.n*="4...3.
000000da: 2e	30	2e	30	22	3e	3c	44	..0...0."><.D.
000000ea: 41	54	41	3e	3c	50	52	4f	A.T.A.><.P.R.O.
000000fa: 54	45	43	54	49	4e	46	4f	T.E.C.T.I.N.F.O.
00000100: 7	7	4	60	66	57	7	7	...K.T.P.O.

# UTF-16LE XML

0000018a: 44	3e	3c	2f	4b	49	44	53	D.><./R.I.D.S.
0000019a: 3e	3c	2f	50	52	4f	54	45	><./P.R.O.T.E.
000001aa: 43	54	49	4e	46	4f	3e	3c	C.T.I.N.F.O.><.
000001ba: 4c	41	5f	55	52	4c	3e	68	L.A._.U.R.L.>.h.
000001ca: 74	74	70	73	3a	2f	2f	6c	t.t.p.s.:././l.
000001da: 69	63	2e	73	74	61	67	69	i.c...s.t.a.g.i.
000001ea: 6e	67	2e	64	72	6d	74	6f	n.g...d.r.m.t.o.
000001fa: 64	61	79	2e	63	6f	6d	2f	d.a.y...c.o.m./.
0000020a: 6c	69	63	65	6e	73	65	2d	l.i.c.e.n.s.e.-.
0000021a: 70	72	6f	78	79	2d	68	65	p.r.o.x.y.-.h.e.
0000022a: 61	64	65	72	61	75	74	68	a.d.e.r.a.u.t.h.
0000023a: 2f	64	72	6d	74	6f	64	61	/d.r.m.t.o.d.a.
0000024a: 79	2f	52	69	67	68	74	73	y./R.i.g.h.t.s.
0000025a: 4d	61	6e	61	67	65	72	2e	M.a.n.a.g.e.r...
0000026a: 61	73	6d	78	3c	2f	4c	41	a.s.m.x.<./L.A.

```
xxd -g1 -s32 -l10 playready.bin
```

```
00000020: 42 03 00 00 01 00 01 00 38 03 00 00
```

B.....8.



834 bytes left

```
xxd -g1 -s32 -l10 playready.bin
```

```
00000020: 42 03 00 00 01 00 01 00 38 03 00 00
```

B.....8.

There's one record, and it's type 1

```
xxd -g1 -s32 -l10 playready.bin
```

```
00000020: 42 03 00 00 01 00 01 00 38 03 00 00
```

B.....8.

Almost there





```
dd status=none skip=42 bs=1 if=playready.bin | iconv -f UTF-16LE -t UTF-8 | xq
```

```
<WRMHEADER xmlns="http://schemas.microsoft.com/DRM/2007/03/PlayReadyHeader"  
version="4.3.0.0">
```

```
  <DATA>
```

```
    <PROTECTINFO>
```

```
      <KIDS>
```

```
        <KID ALGID="AESCBC" VALUE="igXBva1eUgNB45tKQrDx5w=" />
```

```
      </KIDS>
```

```
    </PROTECTINFO>
```

```
  </DATA>
```

```
</WRMHEADER>
```

# Fairplay

skd: // demuxed?keyId=bdc1058a5ead035241e39b4a42b0f1e7



```
if (
    initDataType ≡≡≡ 'sinf' &&
    this.config.drmSystems[KeySystems.FAIRPLAY]
) {
    const sinf = base64Decode(JSON.parse(json).sinf);
    const tenc = parseSinf(new Uint8Array(sinf));
} else {
    const psshInfo = parsePssh(initData);
}
```

```
aligned(8) class TENC extends FullBox('tenc', version, flags=0)
{
    if (version≠0) {
        unsigned int(4) default_crypt_byte_block;
        unsigned int(4) default_skip_byte_block;
    }

    unsigned int(8)      default_isProtected;
    unsigned int(8)      default_Per_Sample_IV_Size;
    unsigned int(8)[16] default_KID;

    if (default_isProtected == 1 && default_Per_Sample_IV_Size == 0) {
        unsigned int(8) default_constant_IV_size;
        unsigned int(8)[default_constant_IV_size] default_constant_IV;
    }
}
```

## HTTP Live Streaming (HLS) authoring specification for Apple devices

- (13.11) Encryption with SAMPLE-AES-CTR SHALL NOT be used on Apple devices.
- (13.4) The IV attribute SHOULD NOT be used with FPS unless necessary for interoperability.
- (13.7) Video encrypted with Common Encryption MUST use an encrypt:skip pattern of 1:9

Server Playback Contexts (SPCs) and Content Key Context (CKC) are mapped to a single key

```
aligned(8) class TENC extends FullBox('tenc', version, flags=0)
{
    unsigned int(8)    default_isProtected;
    unsigned int(8)[16] default_KID;
}
```

## Summary

- PSSH are behaviorally equivalent but semantically unique
- Fragmented definition of what is being protected
- Deeply steeped in company idioms and legacy





**Derek Buitenhuis**

@daemon404

[17:05] <wm4> multimedia is basically neverending pain

9:06 AM · May 17, 2015