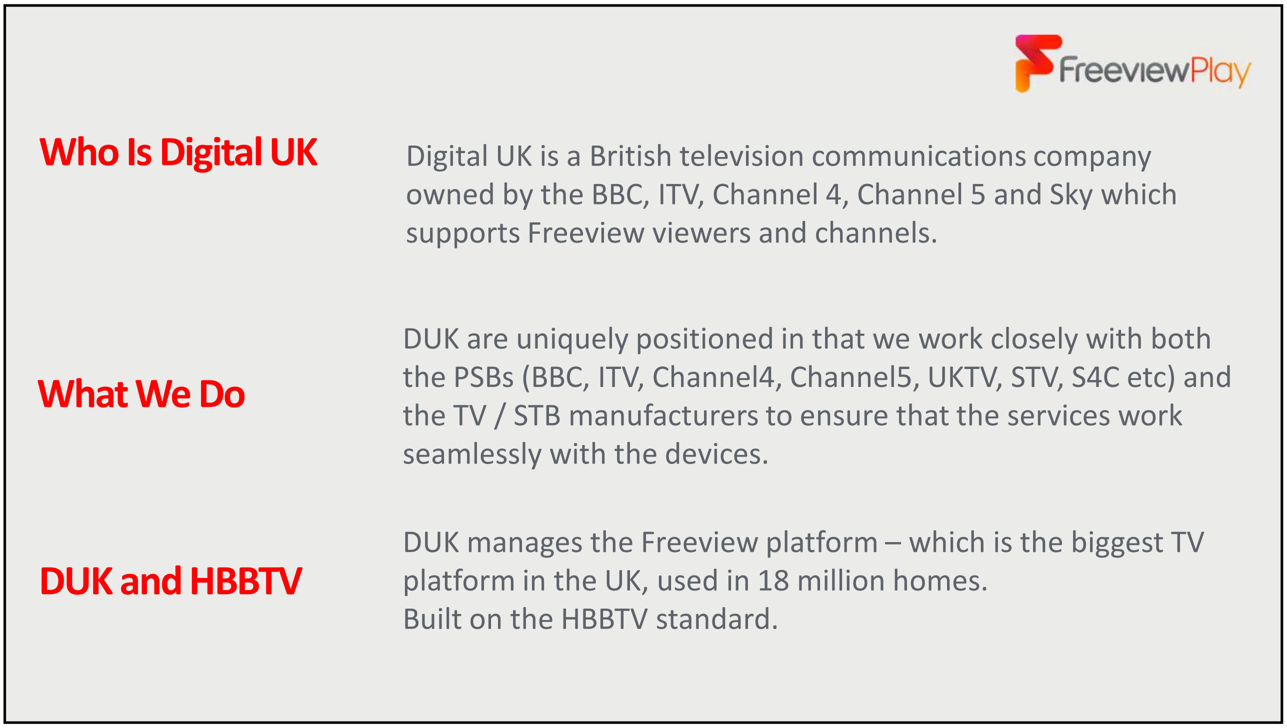
Significance of SL3000 and Experiences In Testing It

Mark Riley
June 22

FreeviewPlay

1



FreeviewPlay

Who Is Digital UK

Digital UK is a British television communications company owned by the BBC, ITV, Channel 4, Channel 5 and Sky which supports Freeview viewers and channels.

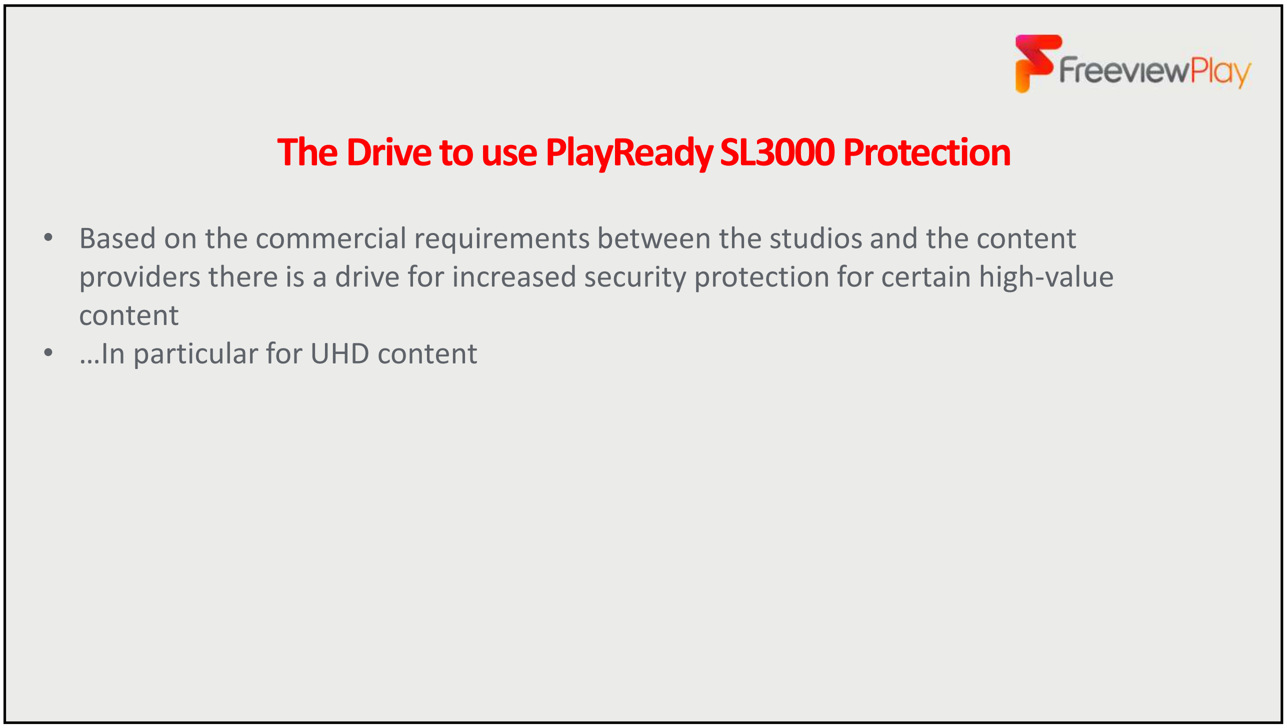
What We Do

DUK are uniquely positioned in that we work closely with both the PSBs (BBC, ITV, Channel4, Channel5, UKTV, STV, S4C etc) and the TV / STB manufacturers to ensure that the services work seamlessly with the devices.

DUK and HBBTV

DUK manages the Freeview platform – which is the biggest TV platform in the UK, used in 18 million homes.
Built on the HBBTV standard.

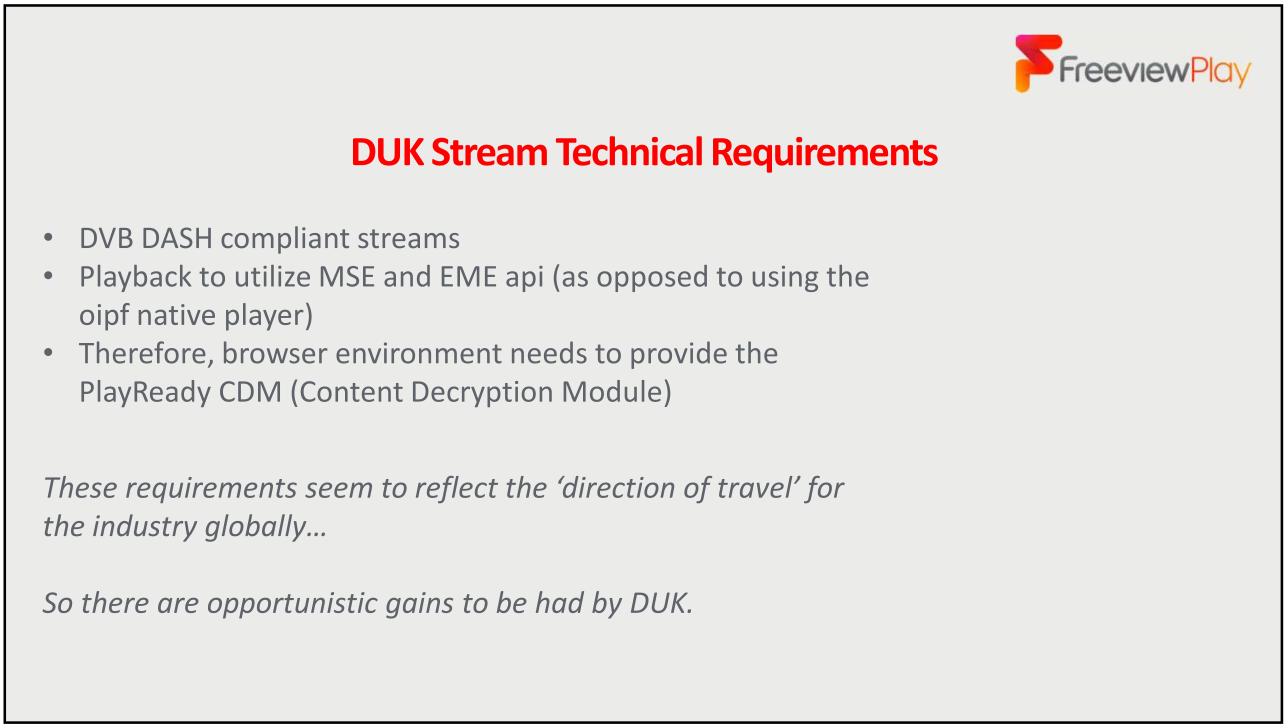
2



The Drive to use PlayReady SL3000 Protection

- Based on the commercial requirements between the studios and the content providers there is a drive for increased security protection for certain high-value content
- …In particular for UHD content

3



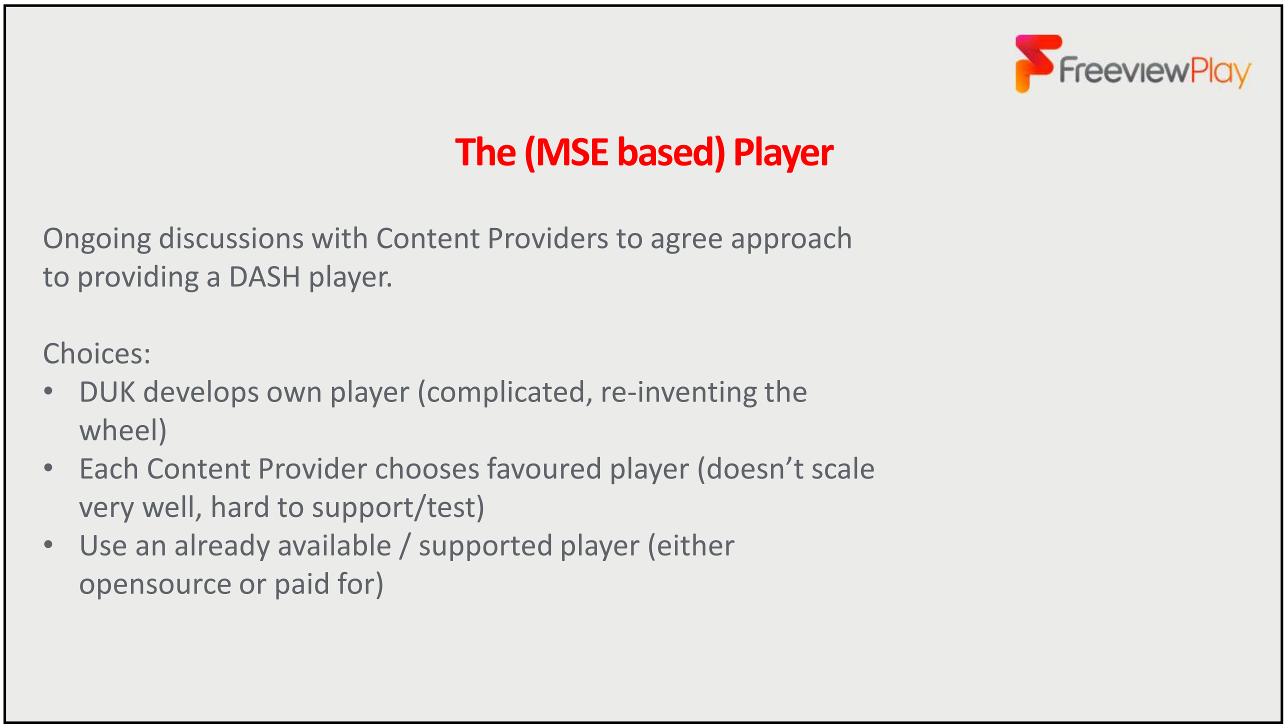
DUK Stream Technical Requirements

- DVB DASH compliant streams
- Playback to utilize MSE and EME api (as opposed to using the oipf native player)
- Therefore, browser environment needs to provide the PlayReady CDM (Content Decryption Module)

These requirements seem to reflect the 'direction of travel' for the industry globally…

So there are opportunistic gains to be had by DUK.

4



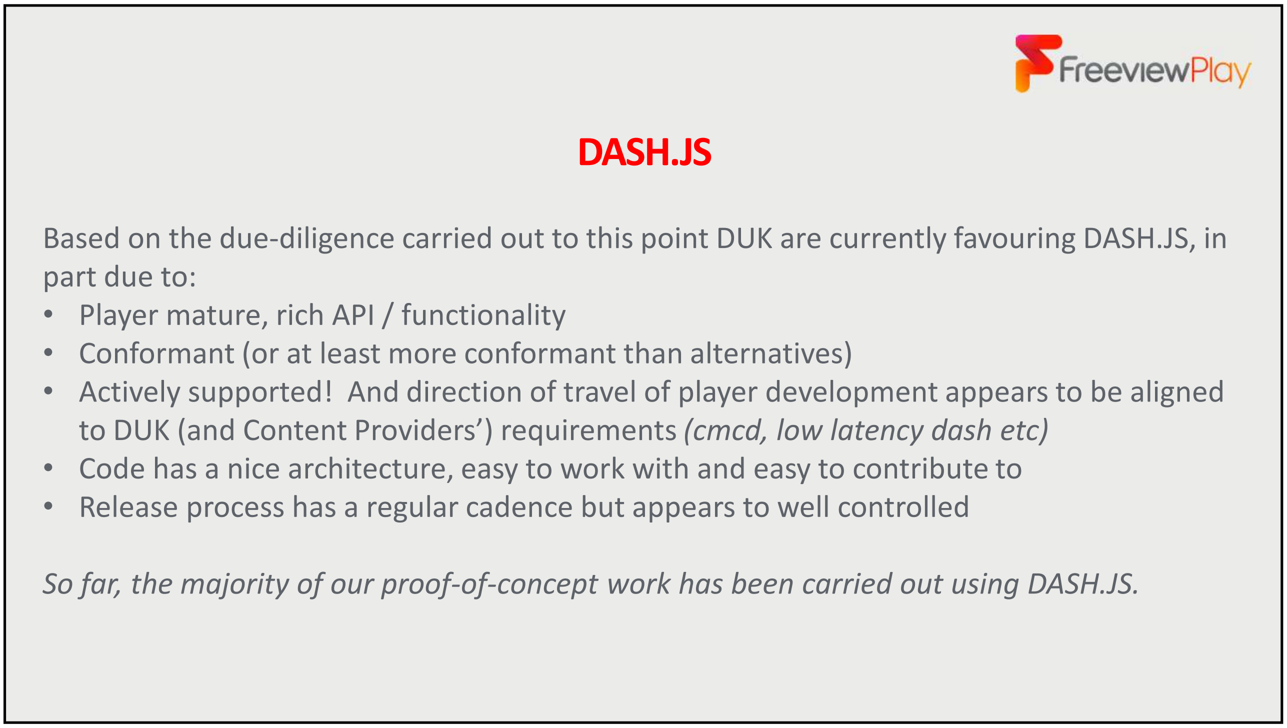
The (MSE based) Player

Ongoing discussions with Content Providers to agree approach to providing a DASH player.

Choices:

- DUK develops own player (complicated, re-inventing the wheel)
- Each Content Provider chooses favoured player (doesn't scale very well, hard to support/test)
- Use an already available / supported player (either opensource or paid for)

5



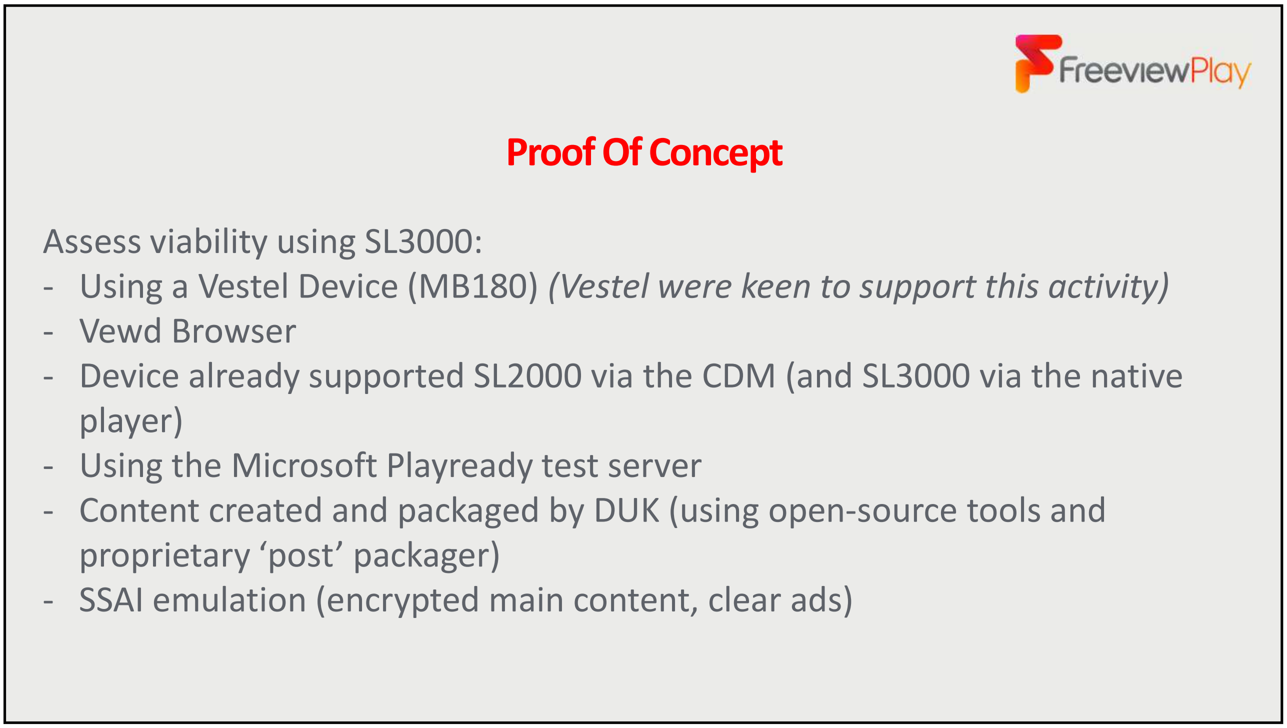
DASH.JS

Based on the due-diligence carried out to this point DUK are currently favouring DASH.JS, in part due to:

- Player mature, rich API / functionality
- Conformant (or at least more conformant than alternatives)
- Actively supported! And direction of travel of player development appears to be aligned to DUK (and Content Providers') requirements *(cmcd, low latency dash etc)*
- Code has a nice architecture, easy to work with and easy to contribute to
- Release process has a regular cadence but appears to well controlled

So far, the majority of our proof-of-concept work has been carried out using DASH.JS.

6

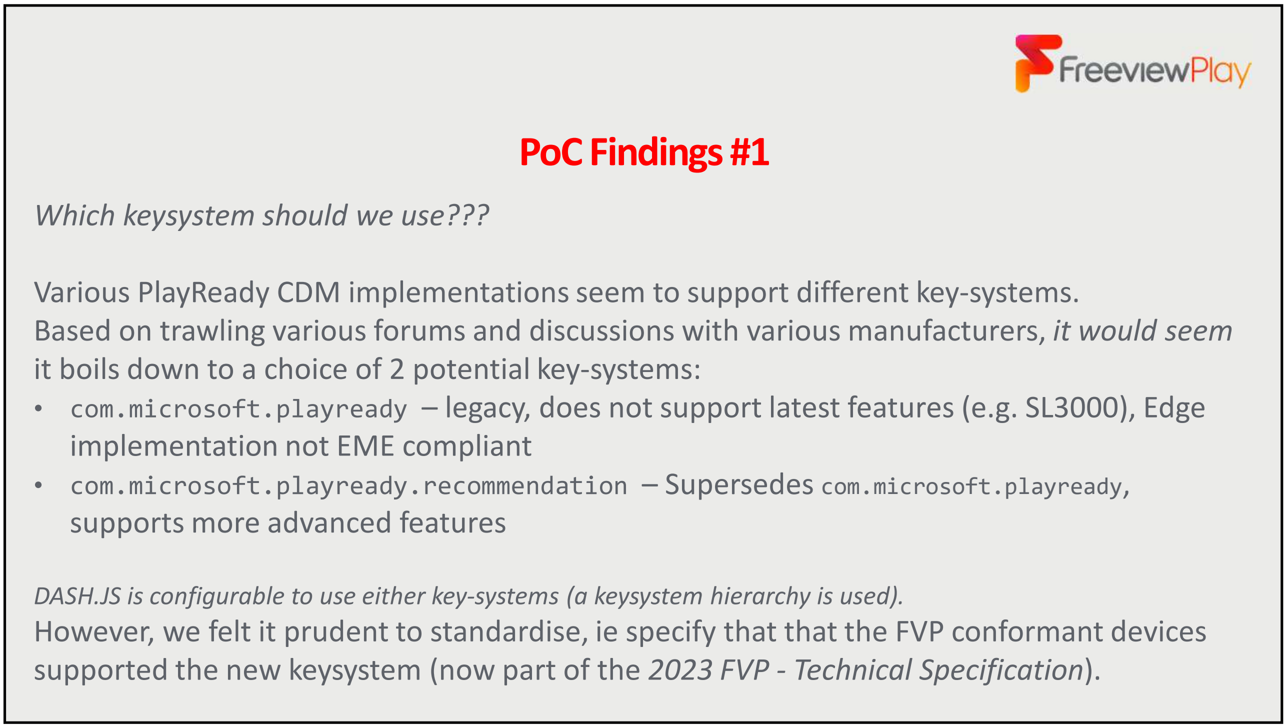


Proof Of Concept

Assess viability using SL3000:

- Using a Vestel Device (MB180) *(Vestel were keen to support this activity)*
- Vewd Browser
- Device already supported SL2000 via the CDM (and SL3000 via the native player)
- Using the Microsoft Playready test server
- Content created and packaged by DUK (using open-source tools and proprietary ‘post’ packager)
- SSAI emulation (encrypted main content, clear ads)

7



PoC Findings #1

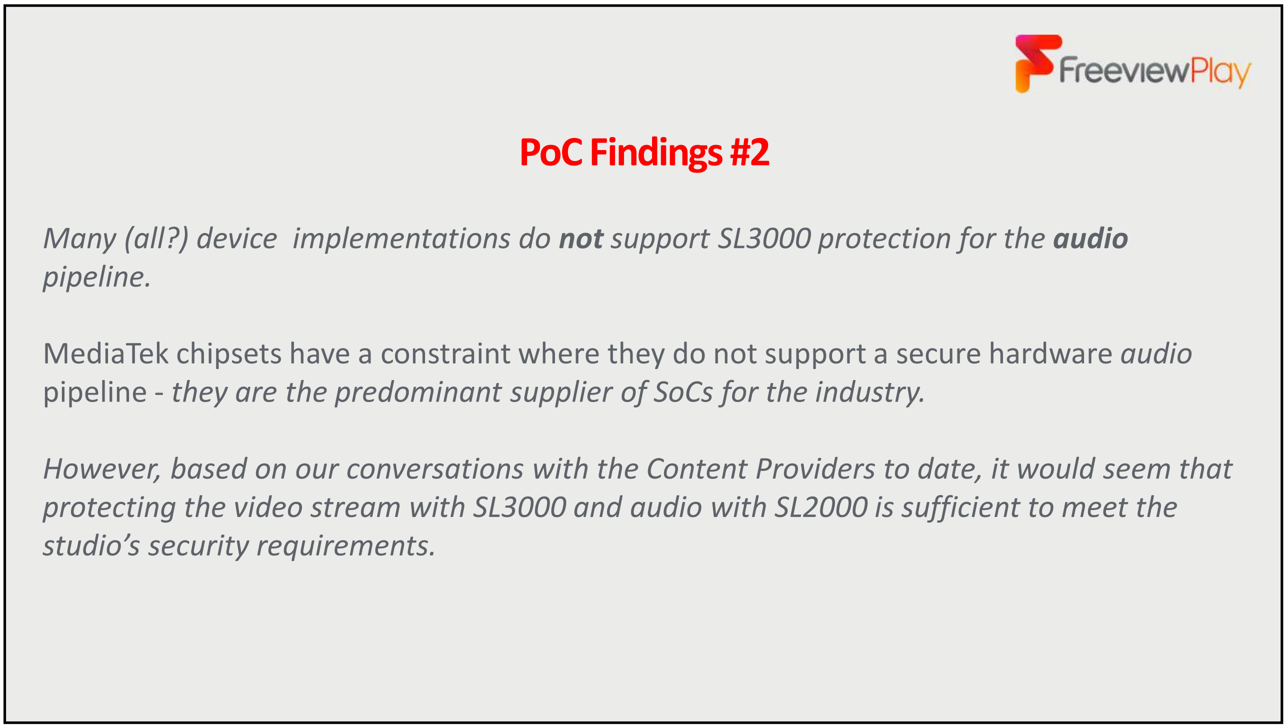
Which keysystem should we use???

Various PlayReady CDM implementations seem to support different key-systems.
Based on trawling various forums and discussions with various manufacturers, *it would seem* it boils down to a choice of 2 potential key-systems:

- `com.microsoft.playready` – legacy, does not support latest features (e.g. SL3000), Edge implementation not EME compliant
- `com.microsoft.playready.recommendation` – Supersedes `com.microsoft.playready`, supports more advanced features

DASH.JS is configurable to use either key-systems (a keysystem hierarchy is used).
However, we felt it prudent to standardise, ie specify that that the FVP conformant devices supported the new keysystem (now part of the *2023 FVP - Technical Specification*).

8



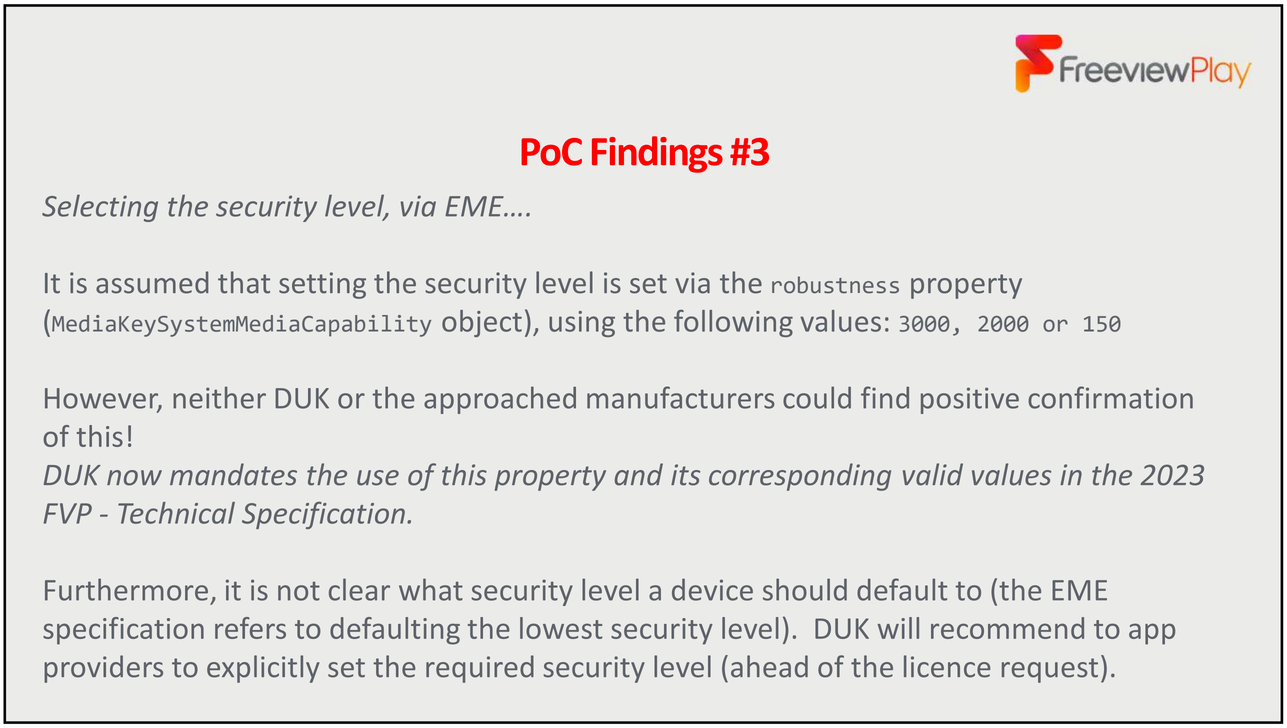
PoC Findings #2

Many (all?) device implementations do ***not*** *support SL3000 protection for the* ***audio*** *pipeline.*

MediaTek chipsets have a constraint where they do not support a secure hardware *audio* pipeline - *they are the predominant supplier of SoCs for the industry.*

However, based on our conversations with the Content Providers to date, it would seem that protecting the video stream with SL3000 and audio with SL2000 is sufficient to meet the studio's security requirements.

9



PoC Findings #3

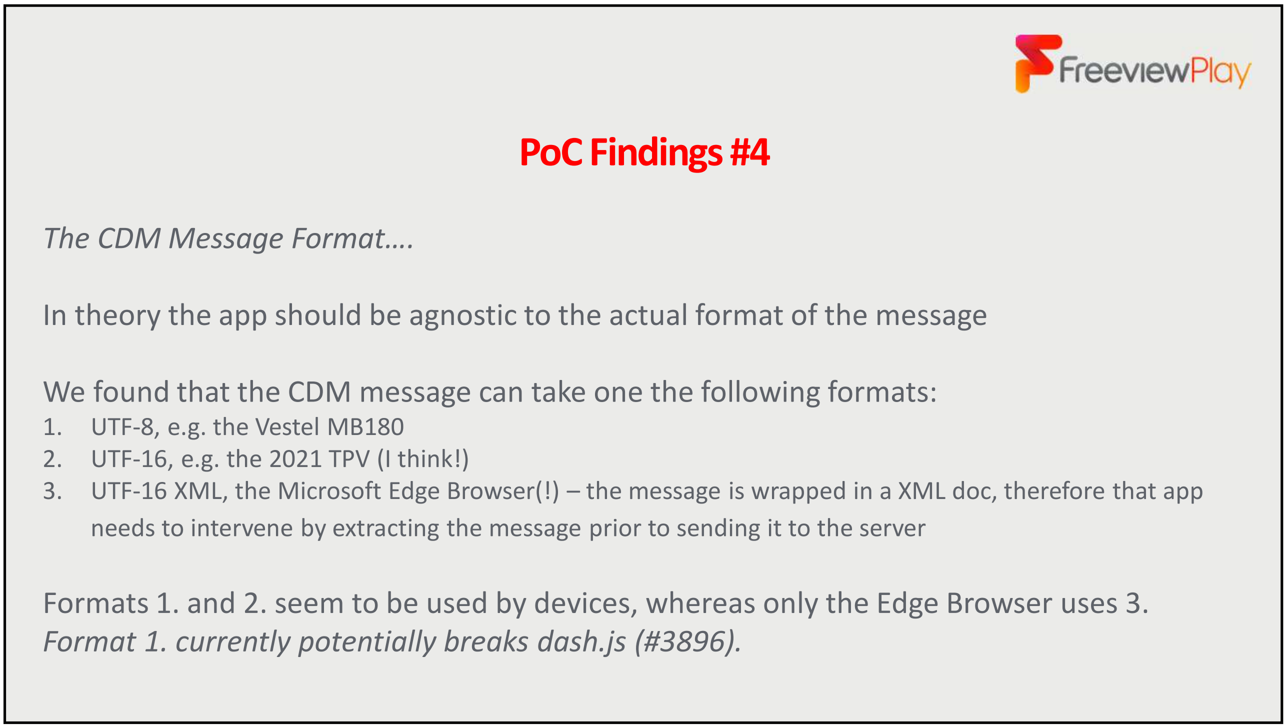
Selecting the security level, via EME….

It is assumed that setting the security level is set via the `robustness` property (`MediaKeySystemMediaCapability` object), using the following values: `3000, 2000 or 150`

However, neither DUK or the approached manufacturers could find positive confirmation of this!
DUK now mandates the use of this property and its corresponding valid values in the 2023 FVP - Technical Specification.

Furthermore, it is not clear what security level a device should default to (the EME specification refers to defaulting the lowest security level). DUK will recommend to app providers to explicitly set the required security level (ahead of the licence request).

10



PoC Findings #4

The CDM Message Format….

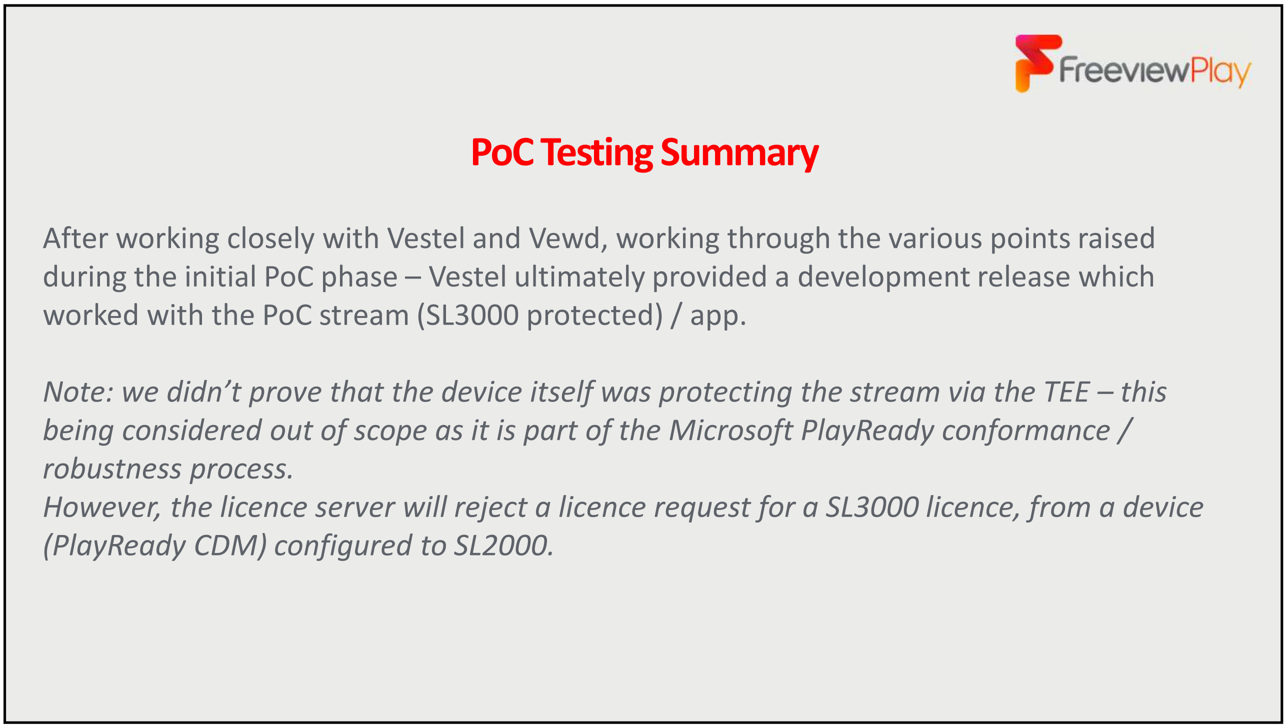
In theory the app should be agnostic to the actual format of the message

We found that the CDM message can take one the following formats:

1. UTF-8, e.g. the Vestel MB180
2. UTF-16, e.g. the 2021 TPV (I think!)
3. UTF-16 XML, the Microsoft Edge Browser(!) – the message is wrapped in a XML doc, therefore that app needs to intervene by extracting the message prior to sending it to the server

Formats 1. and 2. seem to be used by devices, whereas only the Edge Browser uses 3.
Format 1. currently potentially breaks dash.js (#3896).

11

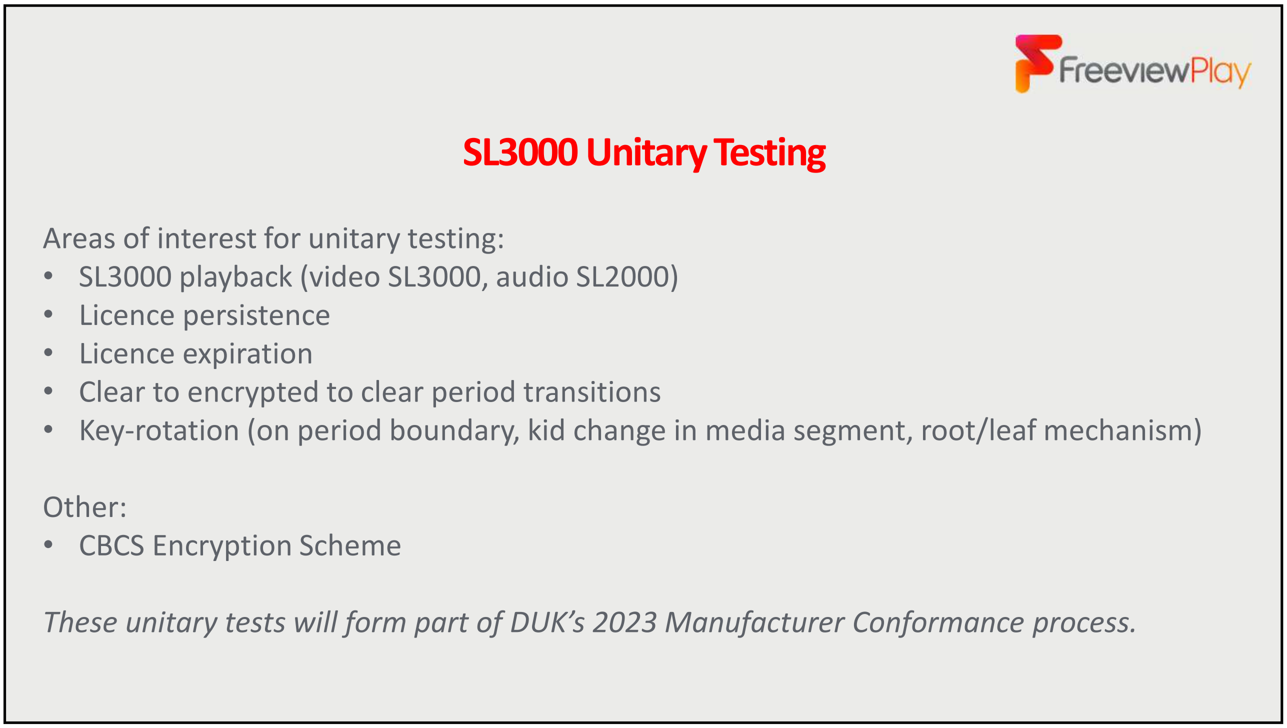


PoC Testing Summary

After working closely with Vestel and Vewd, working through the various points raised during the initial PoC phase – Vestel ultimately provided a development release which worked with the PoC stream (SL3000 protected) / app.

Note: we didn't prove that the device itself was protecting the stream via the TEE – this being considered out of scope as it is part of the Microsoft PlayReady conformance / robustness process.
However, the licence server will reject a licence request for a SL3000 licence, from a device (PlayReady CDM) configured to SL2000.

12



SL3000 Unitary Testing

Areas of interest for unitary testing:

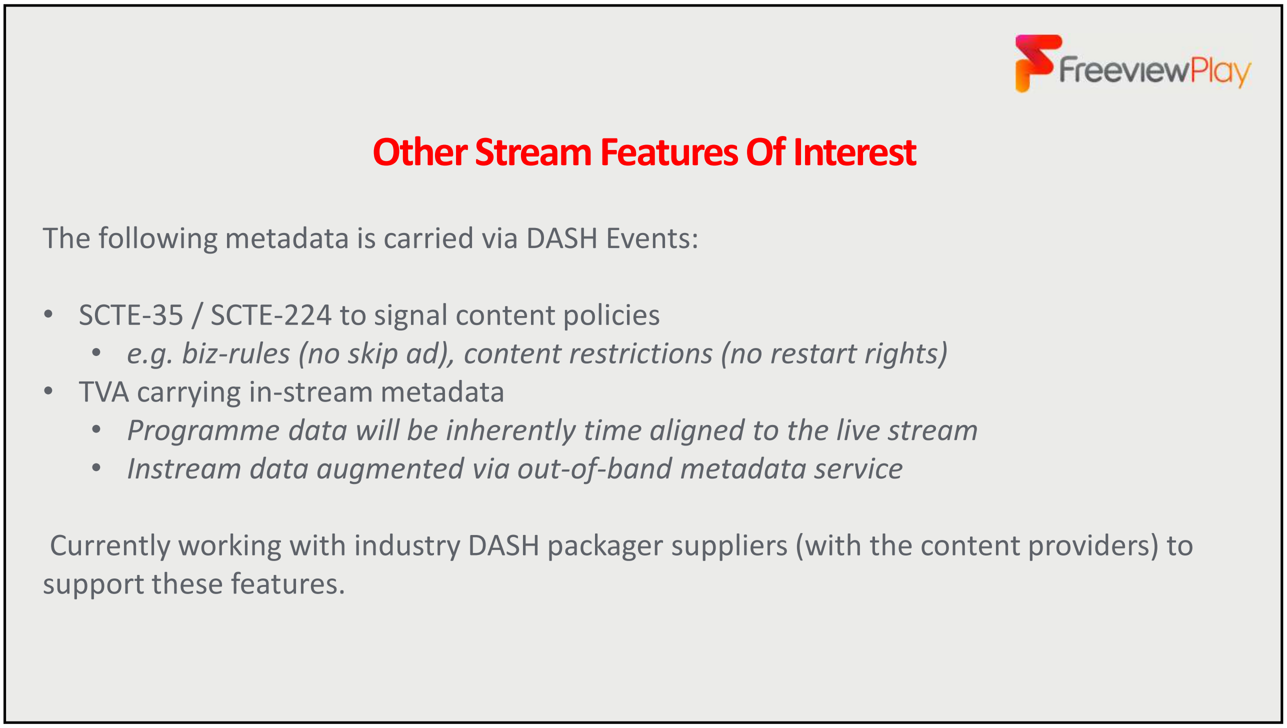
- SL3000 playback (video SL3000, audio SL2000)
- Licence persistence
- Licence expiration
- Clear to encrypted to clear period transitions
- Key-rotation (on period boundary, kid change in media segment, root/leaf mechanism)

Other:

- CBCS Encryption Scheme

These unitary tests will form part of DUK's 2023 Manufacturer Conformance process.

13



Other Stream Features Of Interest

The following metadata is carried via DASH Events:

- SCTE-35 / SCTE-224 to signal content policies
  - *e.g. biz-rules (no skip ad), content restrictions (no restart rights)*
- TVA carrying in-stream metadata
  - *Programme data will be inherently time aligned to the live stream*
  - *Instream data augmented via out-of-band metadata service*

Currently working with industry DASH packager suppliers (with the content providers) to support these features.

14