



COLLABORA

Secure Video Path Done the Right Way

@ndufresne

Nicolas Dufresne

nicolas@collabora.com

Open First





COLLABORA

Who am I ?

Open Source Linux Developer

- Maintains **CODECs** drivers and API in **Linux Media**
- All around contributor to **GStreamer** (with a Linux focus)
- Helps with the GStreamer project **maintenance**
- Likes to help GStreamer users (discourse.gstreamer.org)
- Consultant at **Collabora** since **2009**



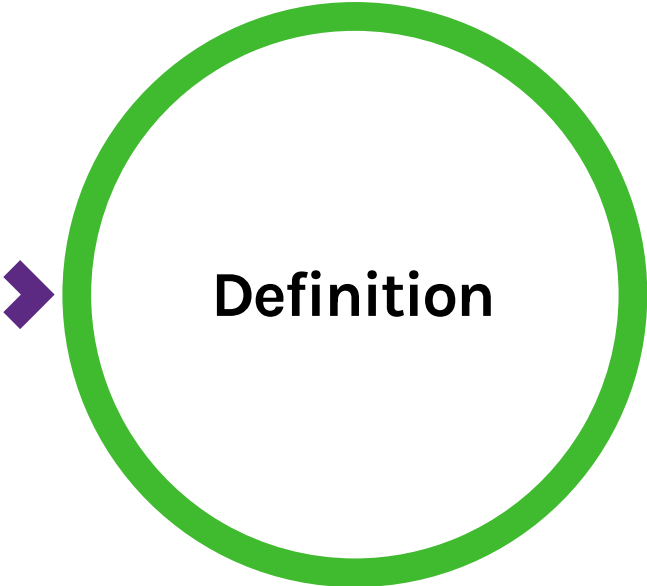
What does it mean “the right way” ?



- There are **multiple solutions** to most problems
- To be right, the solution must go beyond a single user or platform
- The solution must have been **discussed** and gained **acceptance**

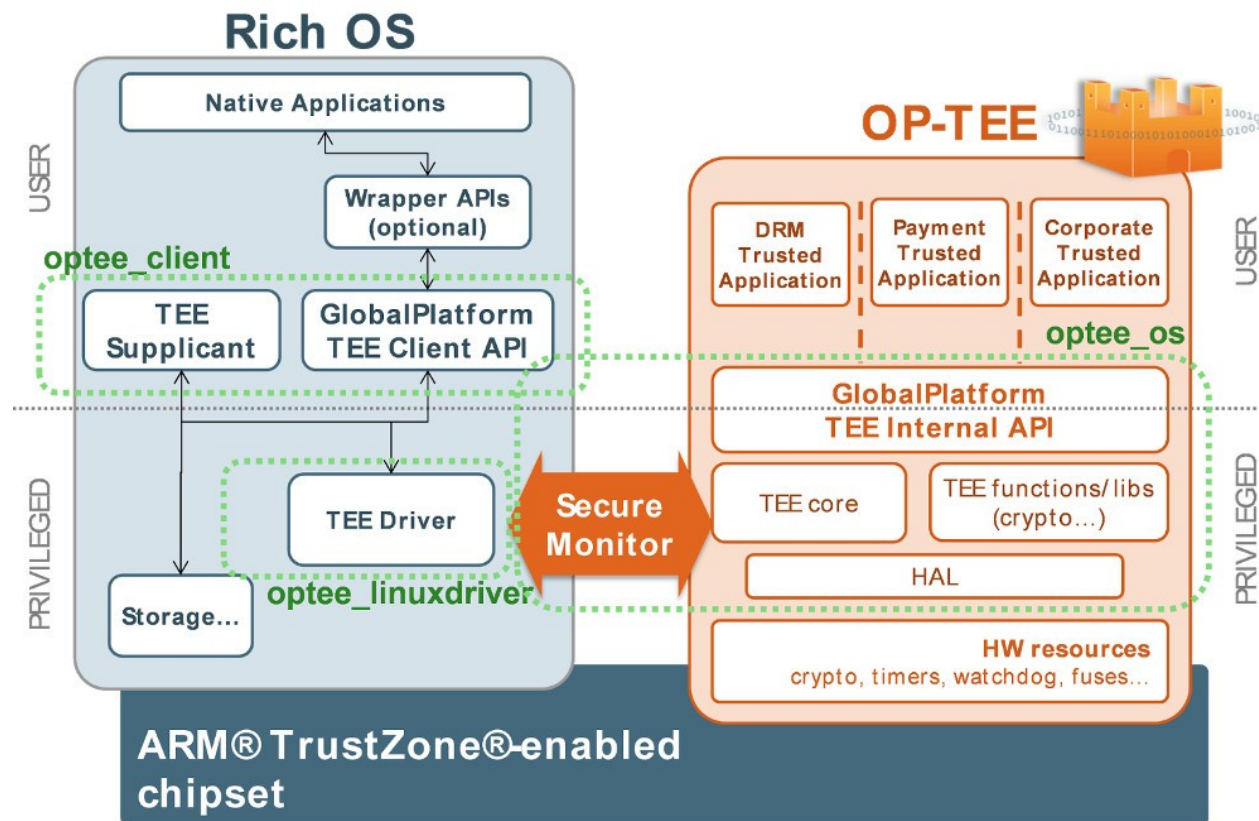
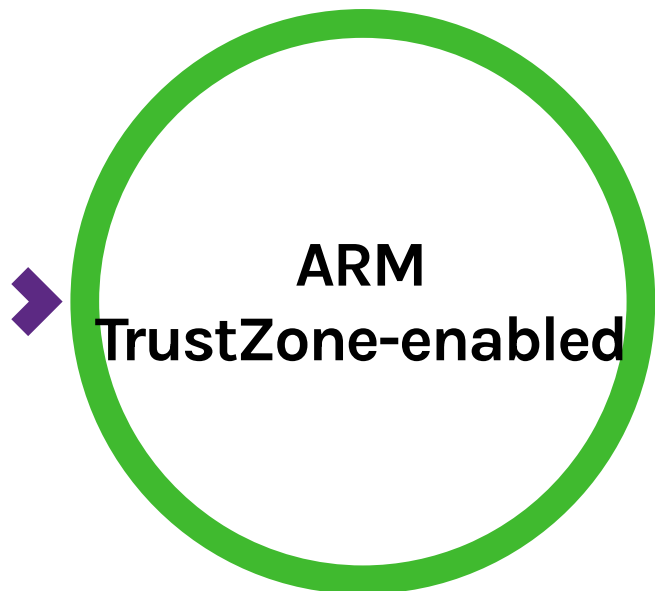


What is secure video path?



Definition

“The process of playing encrypted video content while hiding the video data from the CPU so that no digital copy can easily be made”

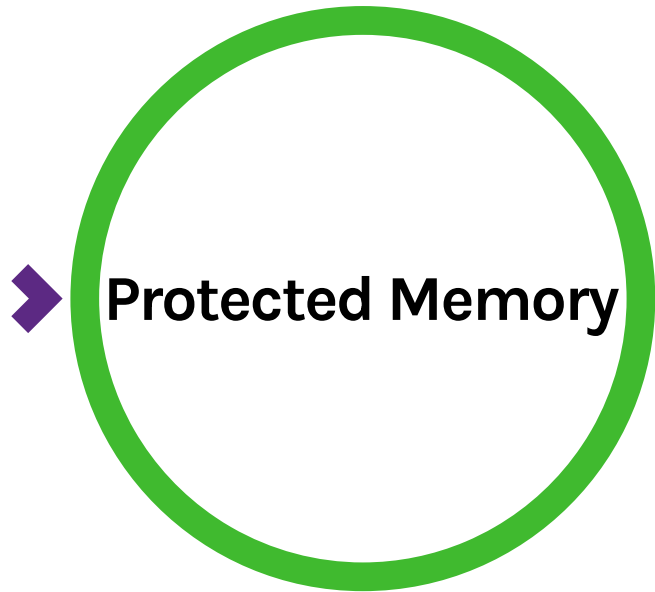


From Linaro, downloaded from:
https://linuxgizmos.com/files/linaro_optee_arch.jpg



COLLABORA

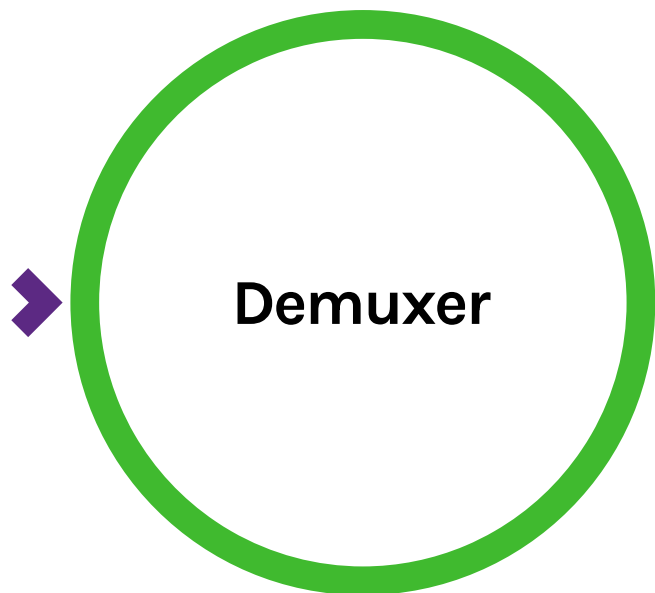
Open First



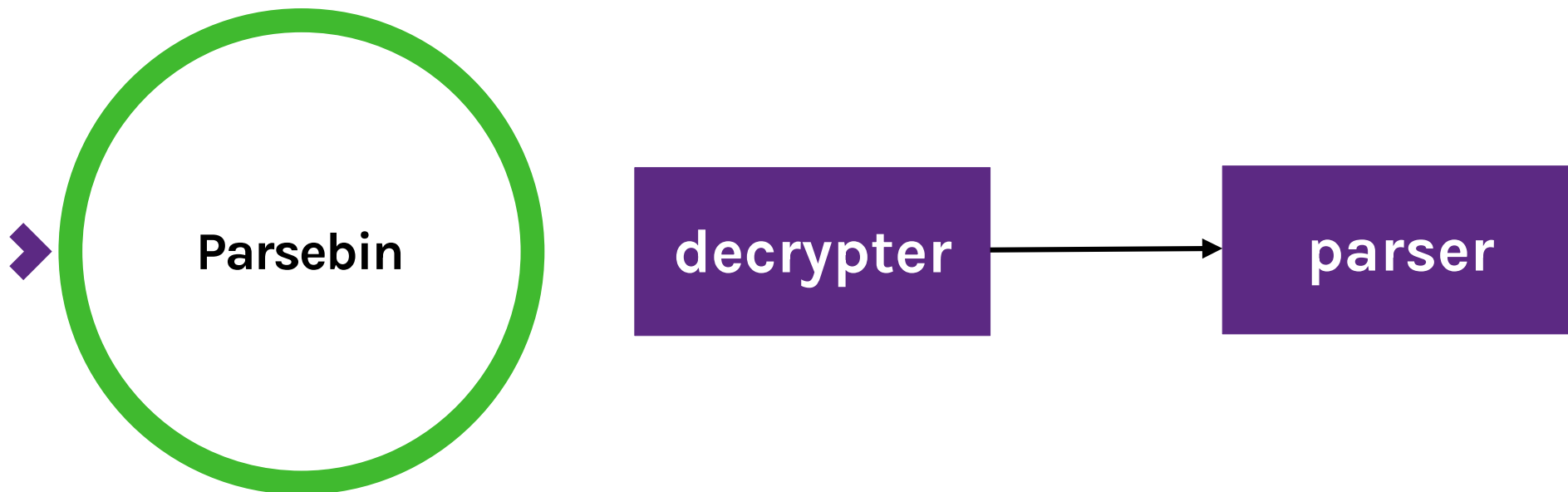
- Decrypted & decoded data is **write-only**
- Either defined at boot as **zones**, or **per-page**, or using virtualization hardware
- Only the TEE can “unprotect” pages (when the HW allows it)

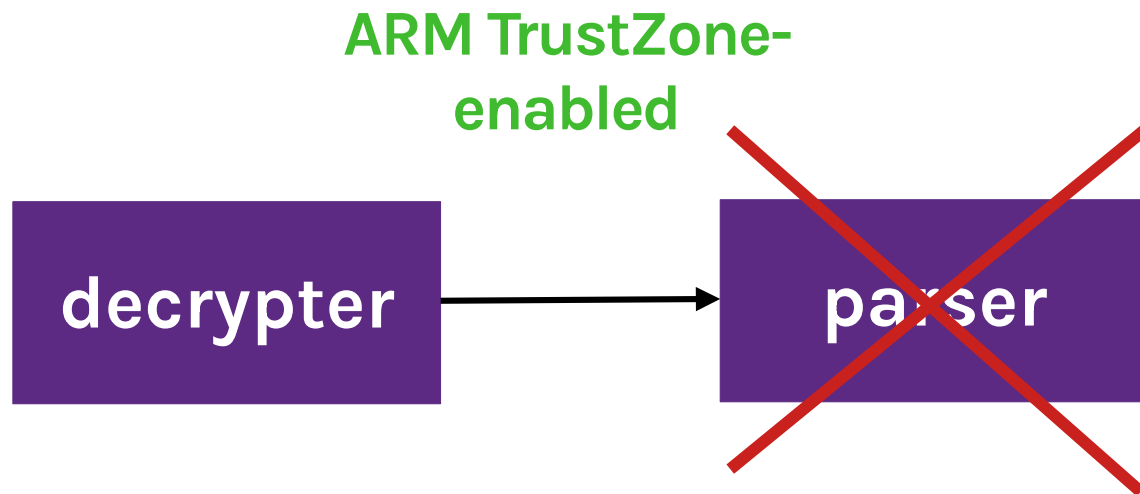
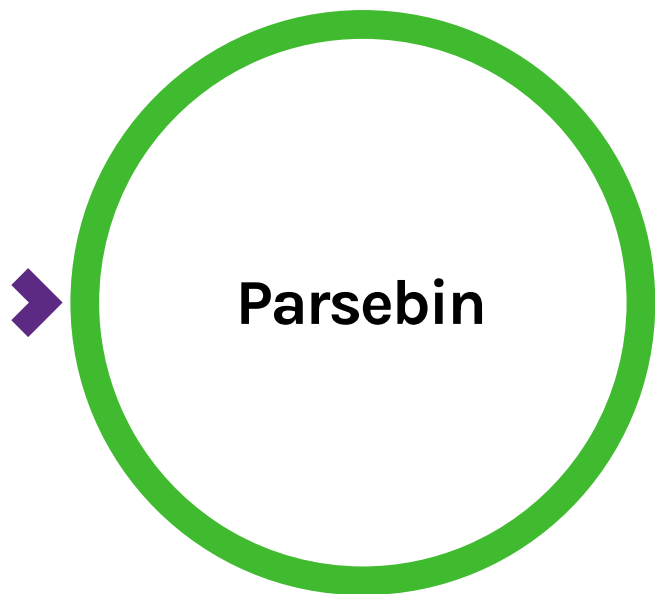


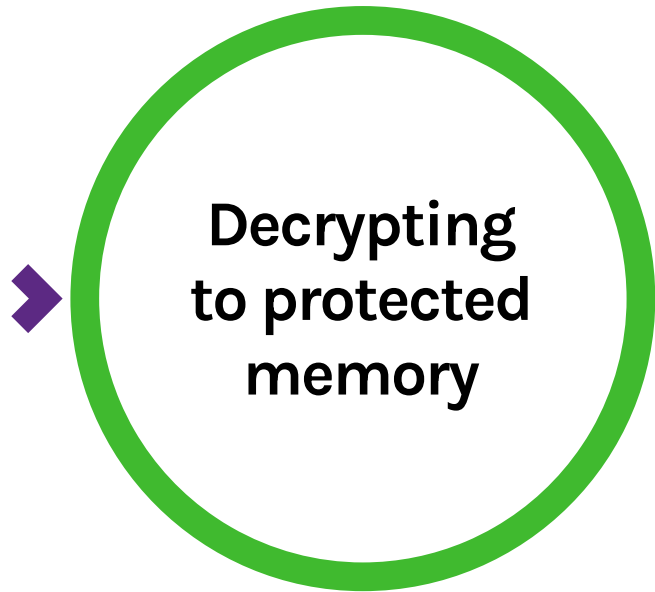
What does it mean for GStreamer?



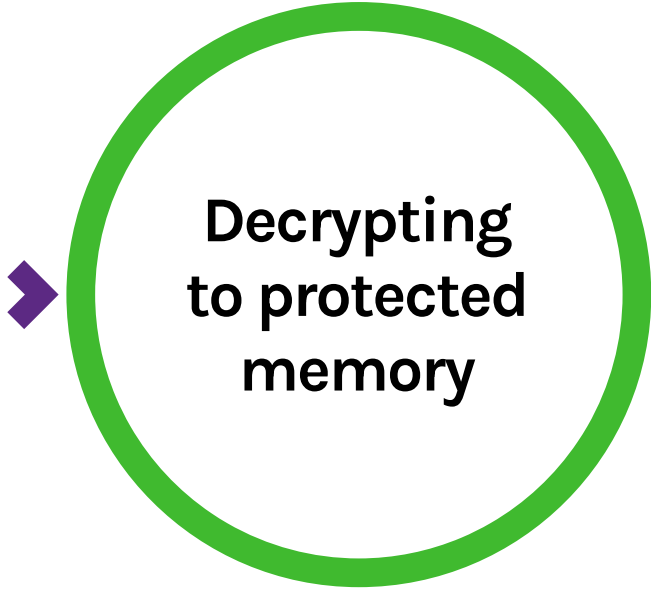
- Select the protection system
- Fill GstProtectionMeta
- Push data as “application/x-cenc”





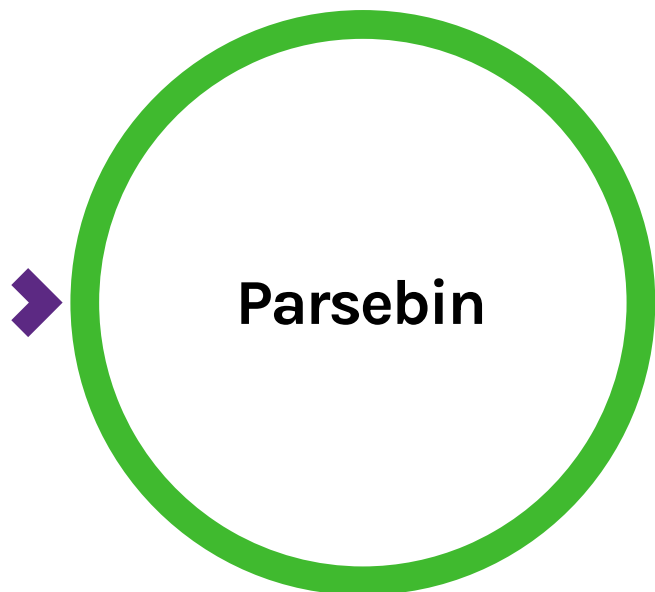


- 1) Output protected, but keep the encrypted buffer in the output buffer meta

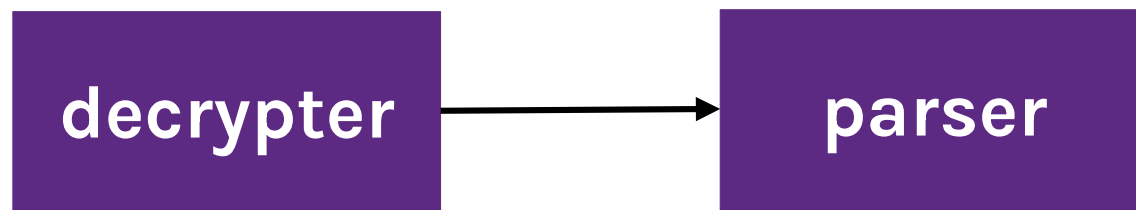


**Decrypting
to protected
memory**

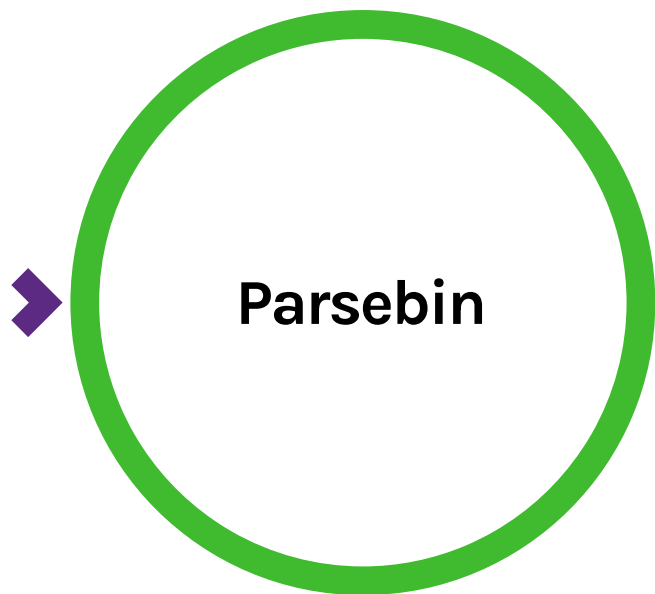
- 1) Output protected, but keep the encrypted buffer in the output buffer meta
- 2) Passthrough and store the protected handle in the existing GstProtectionMeta



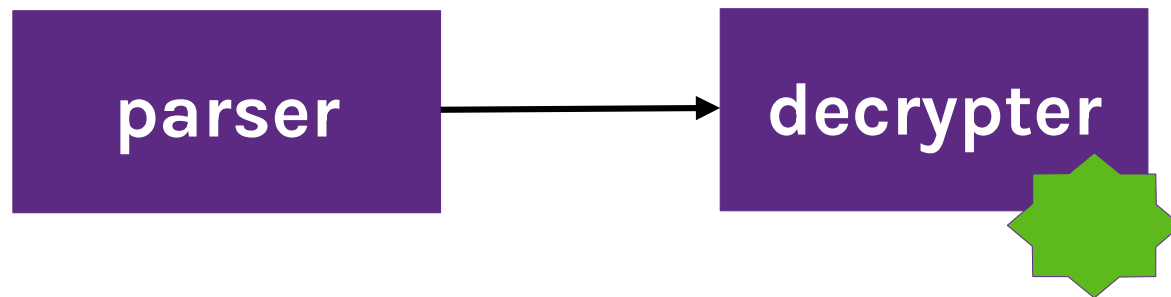
ARM TrustZone-
enabled



Works, but an alignment change will
break the samples description, and what
is decrypted won't match anymore



ARM TrustZone-
enabled

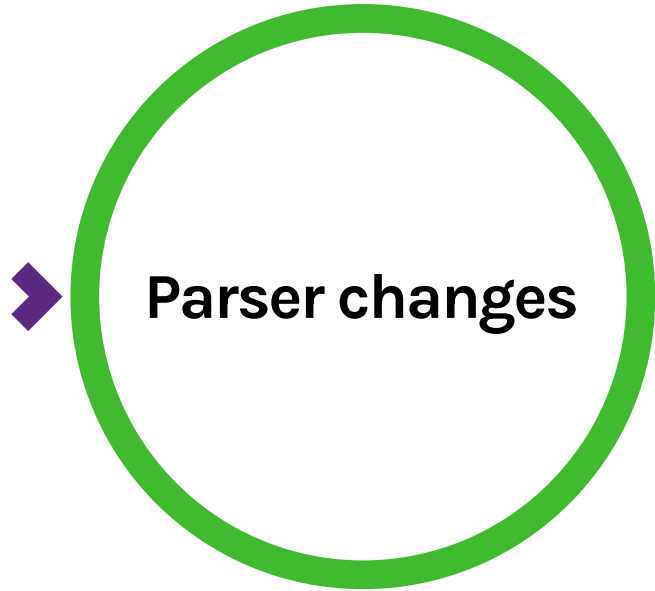


But ...

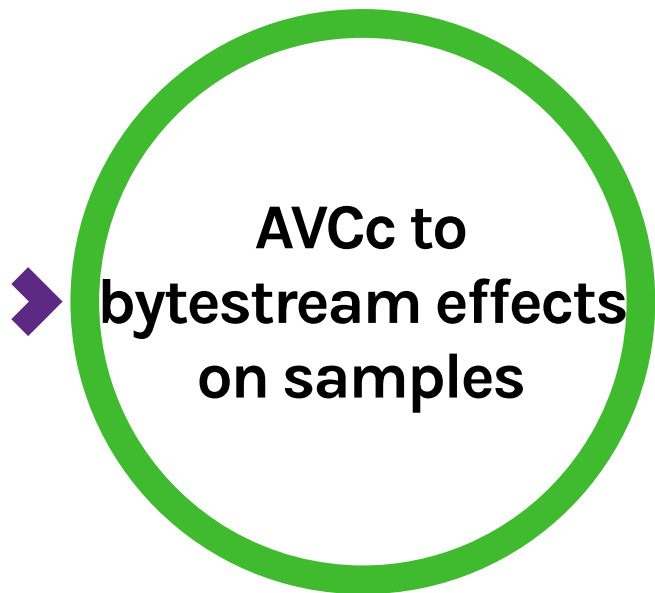


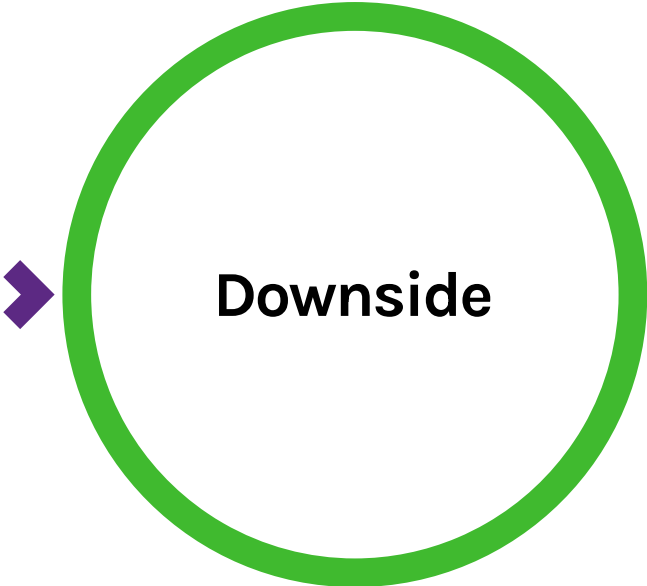
COLLABORA

Open First



- Need to accept **application/x-cenc**
- Stream format transformation impacts the GstProtectionMeta samples



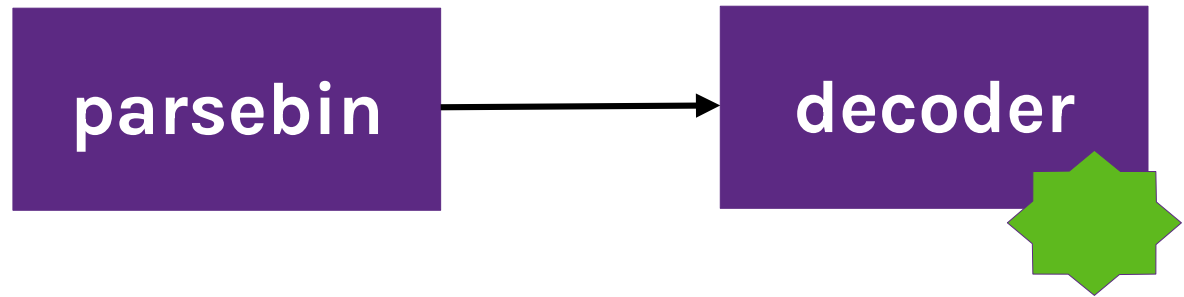
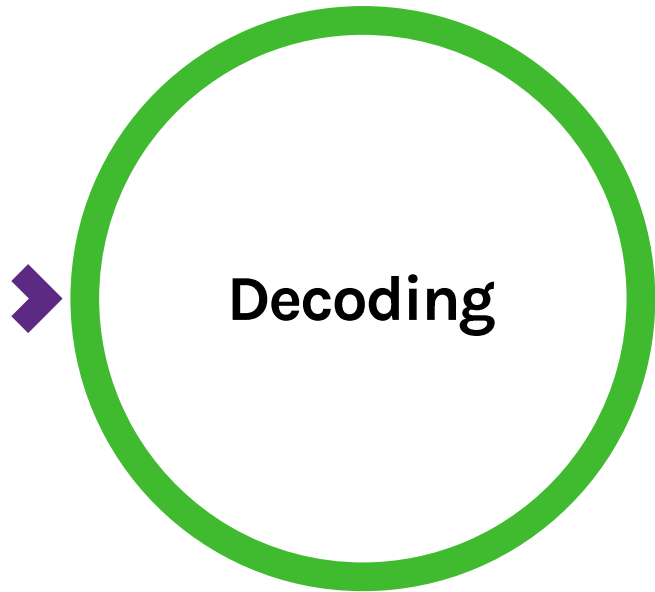


Downside

- The “decrypted” form is still encrypted, which allows various bogus pipelines to link and run.
- Should we revert to option 1)? use a caps feature? Both?



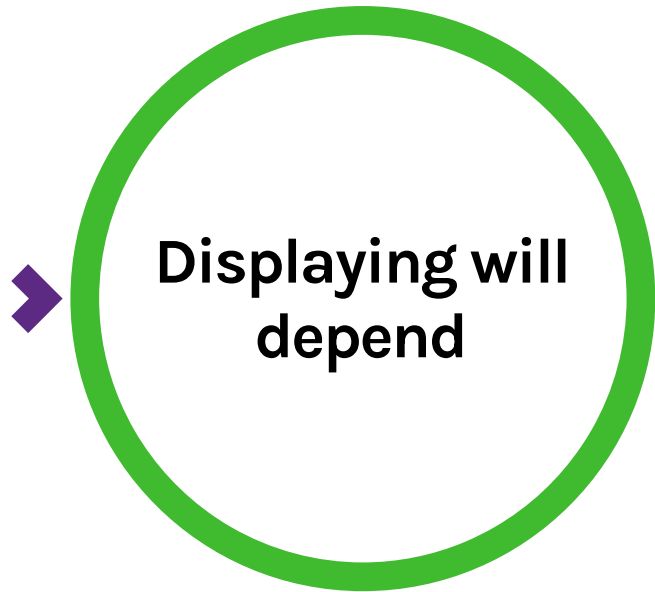
Can we decode now?



- The decode parses the encrypted stream to maintain the state
- Protected memory is passed to the accelerator for decoding



Can we display?



- Wayland has a simple frame-by-frame marking
- GL and Vulkan need a **protected context**
- A **caps feature** may solve the above issues
- Of course, it can always fail if you do not have an HDCP link, or a trusted panel

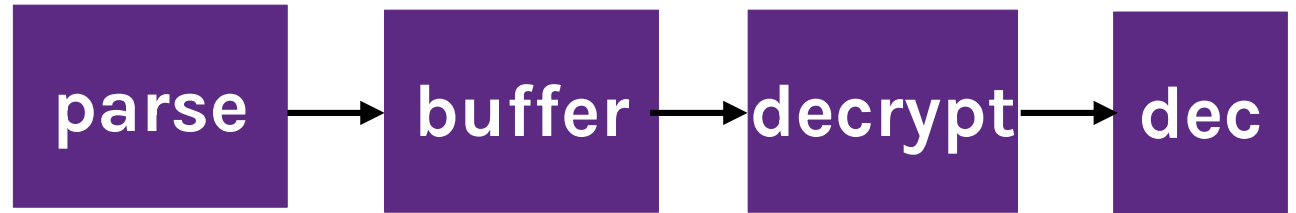
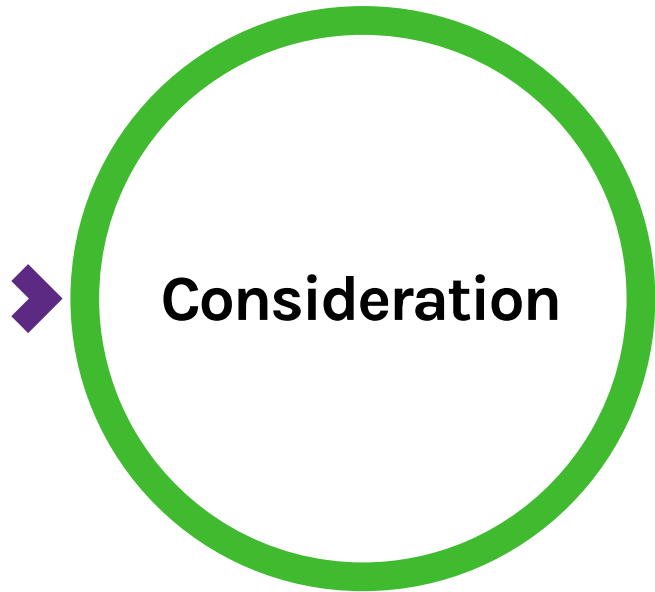


What other challenges do we have?



Challenges

- Limited amount of protected memory
- On disk buffering is broken, can't store and restore protected memory
- Perhaps we could try and move decryption next to the decoders?



- What changes need to be made?



Question?



COLLABORA

Open First



Thank you!



COLLABORA

Open First