# TZMP-1 Software Reference Implementation

Ken Liu

2018-Mar-12

# Content

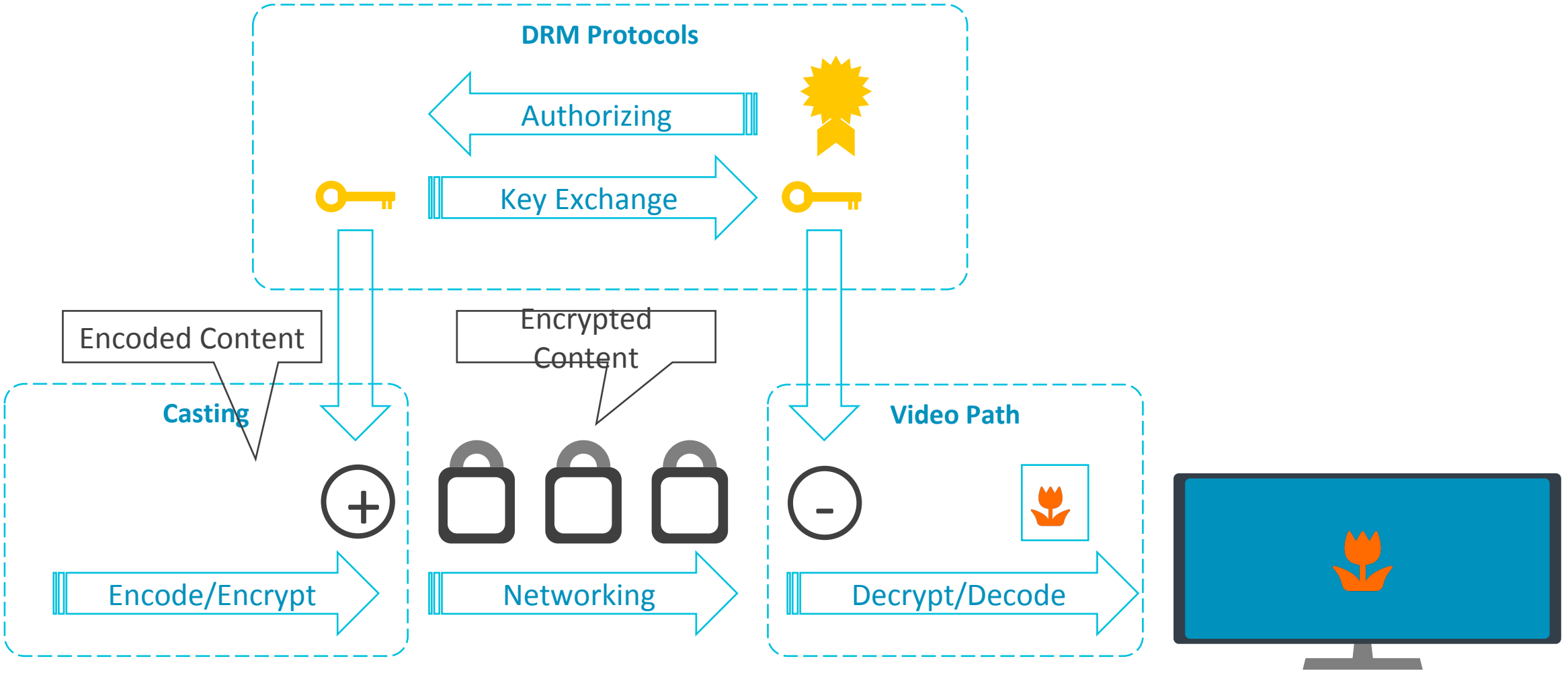
- **DRM Applications and Secure Video Path**

- Regular Secure Video Path Design with Trustzone
- TZMP1 Design Concepts
- Reference Implementation Details



arm

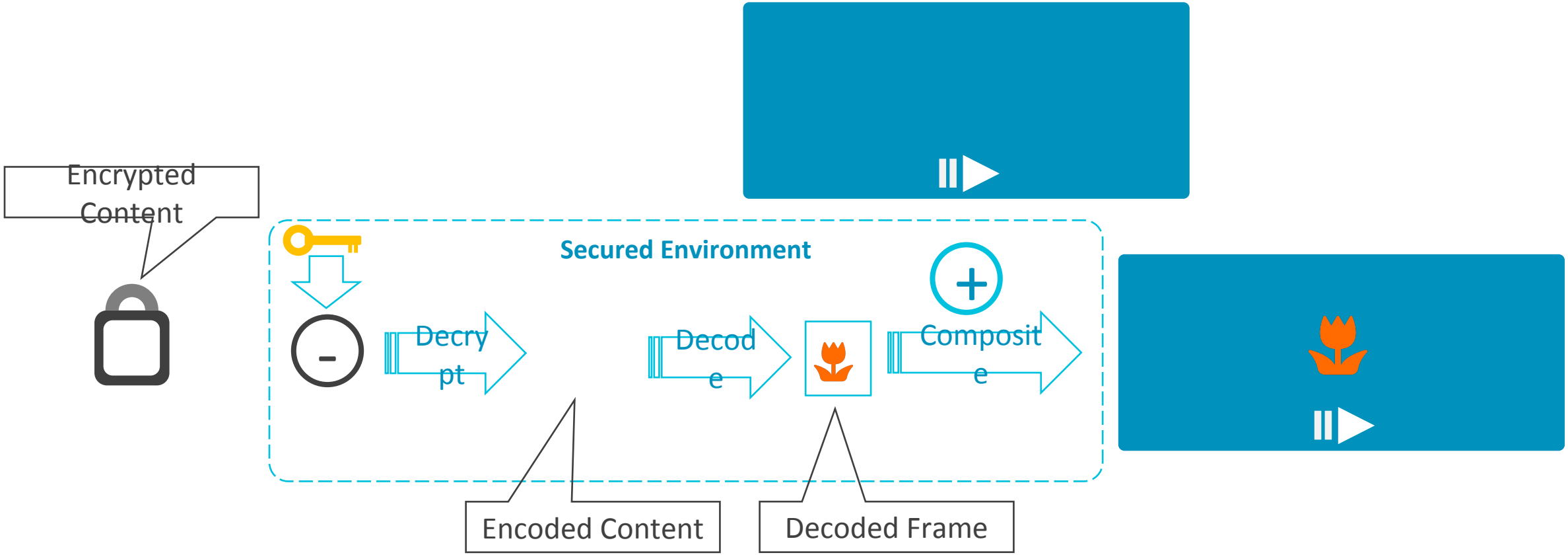
# General Process of DRM






arm

# Ideal Model of Secure Video Path






arm

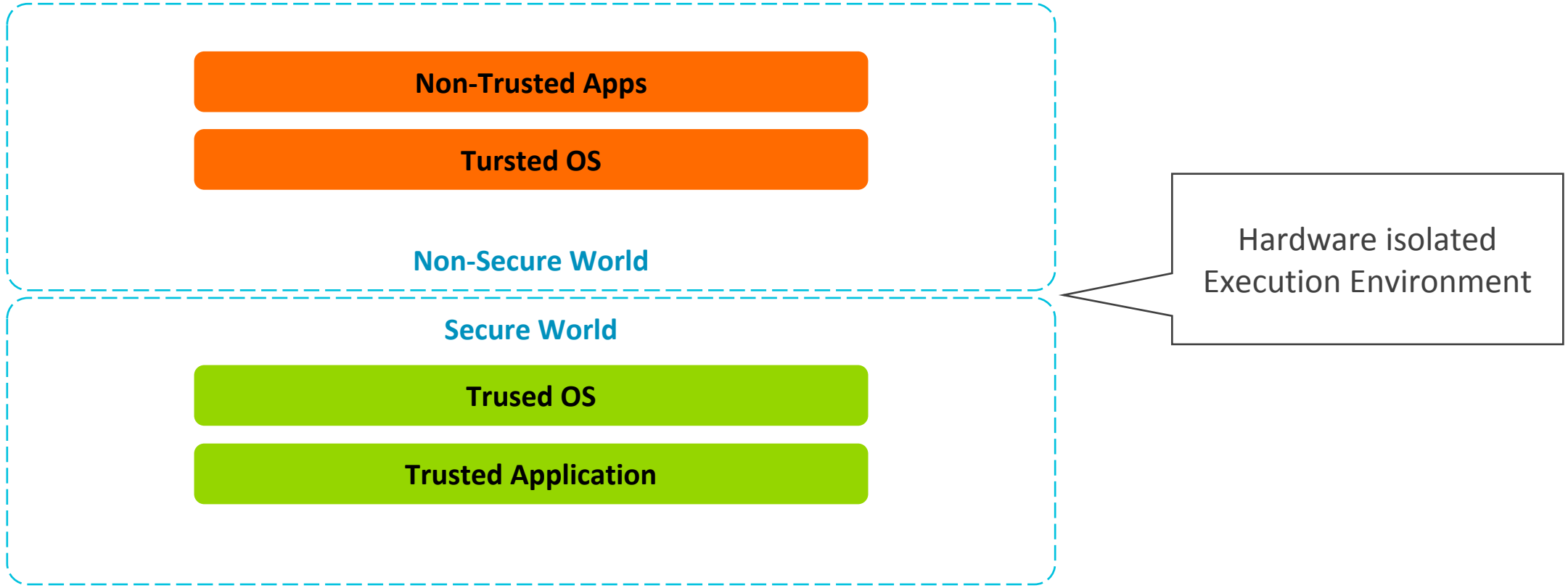
# Content

- DRM Applications and Secure Video Path
- **Regular Secure Video Path Design with Trustzone**
- TZMP1 Design Concepts
- Reference Implementation Details



arm

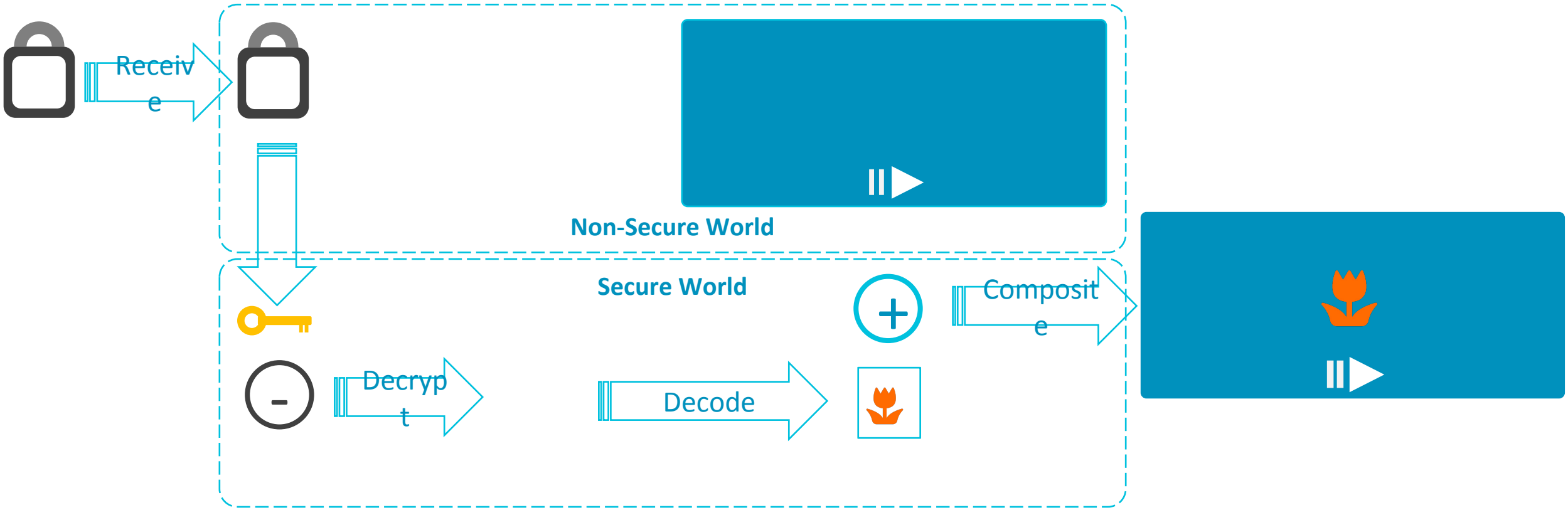
# Arm Trustzone






arm

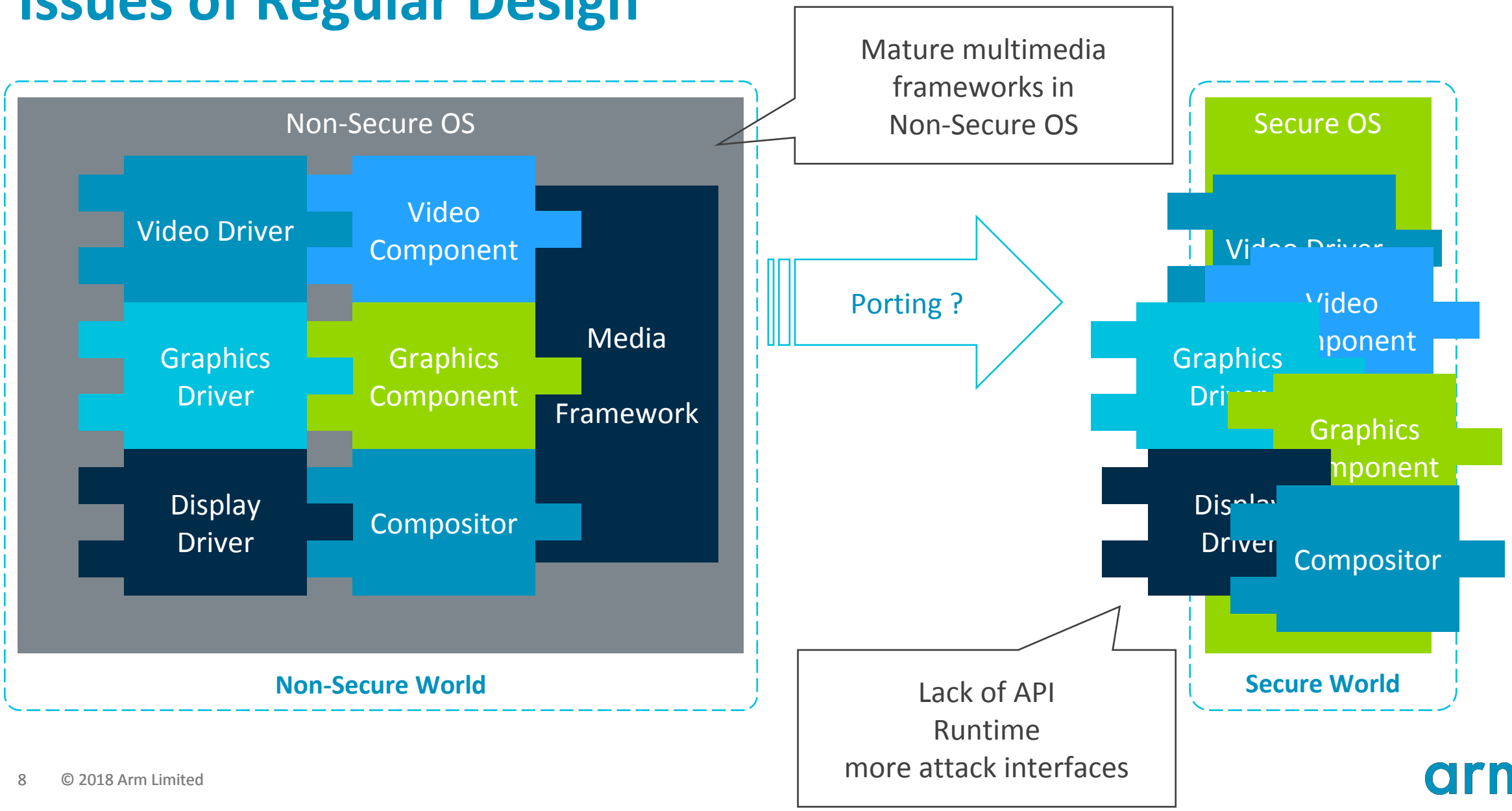
# Regular Design with TrustZone



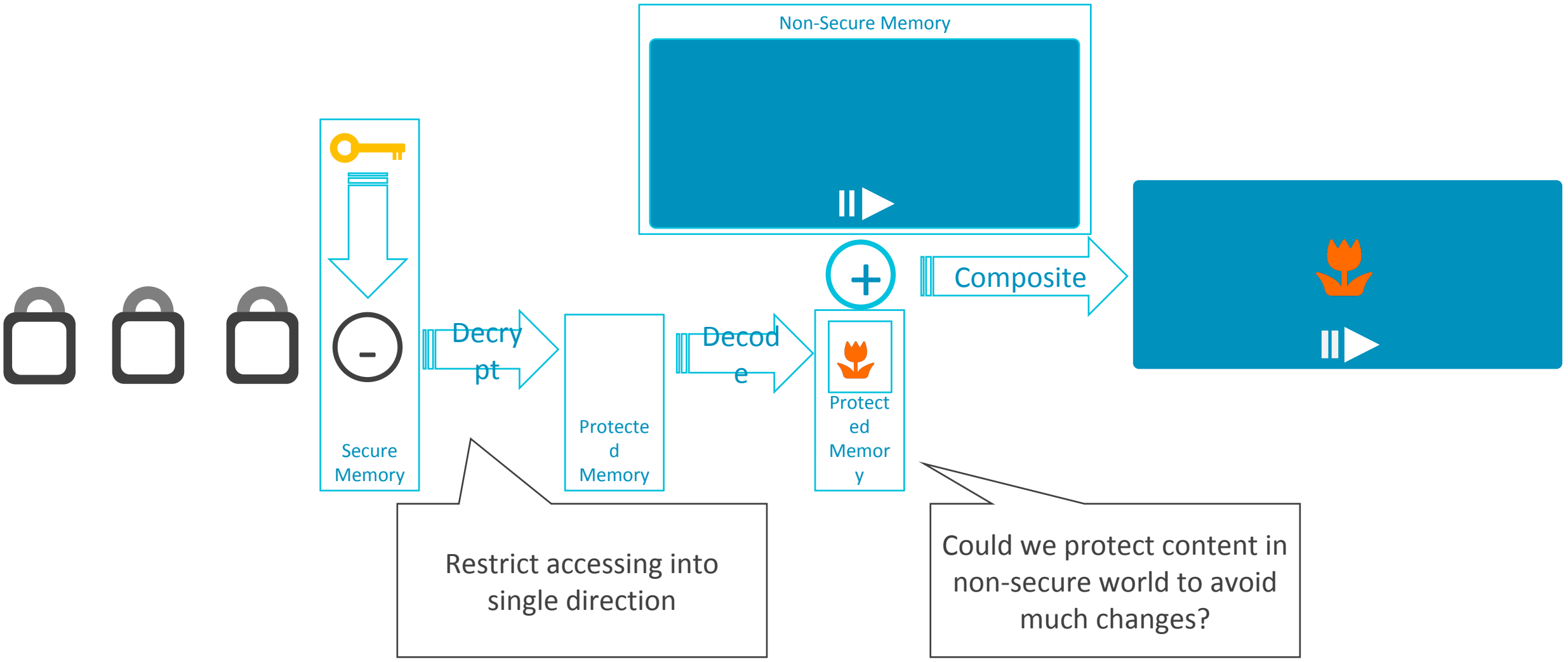



arm

# Issues of Regular Design



# Protect Content in Non-Secure World






arm

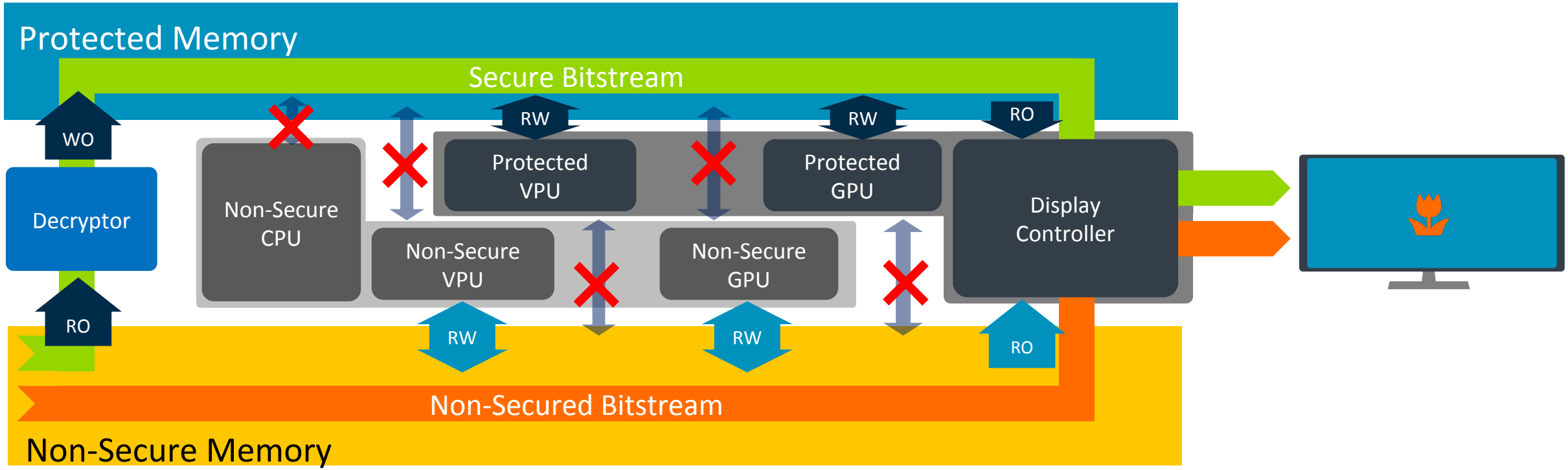
# Content

- DRM Applications and Secure Video Path
- Regular Secure Video Path Design with Trustzone
- **TZMP1 Design Concepts**
- Reference Implementation Details



arm

# Protected Memory and Secured Playback

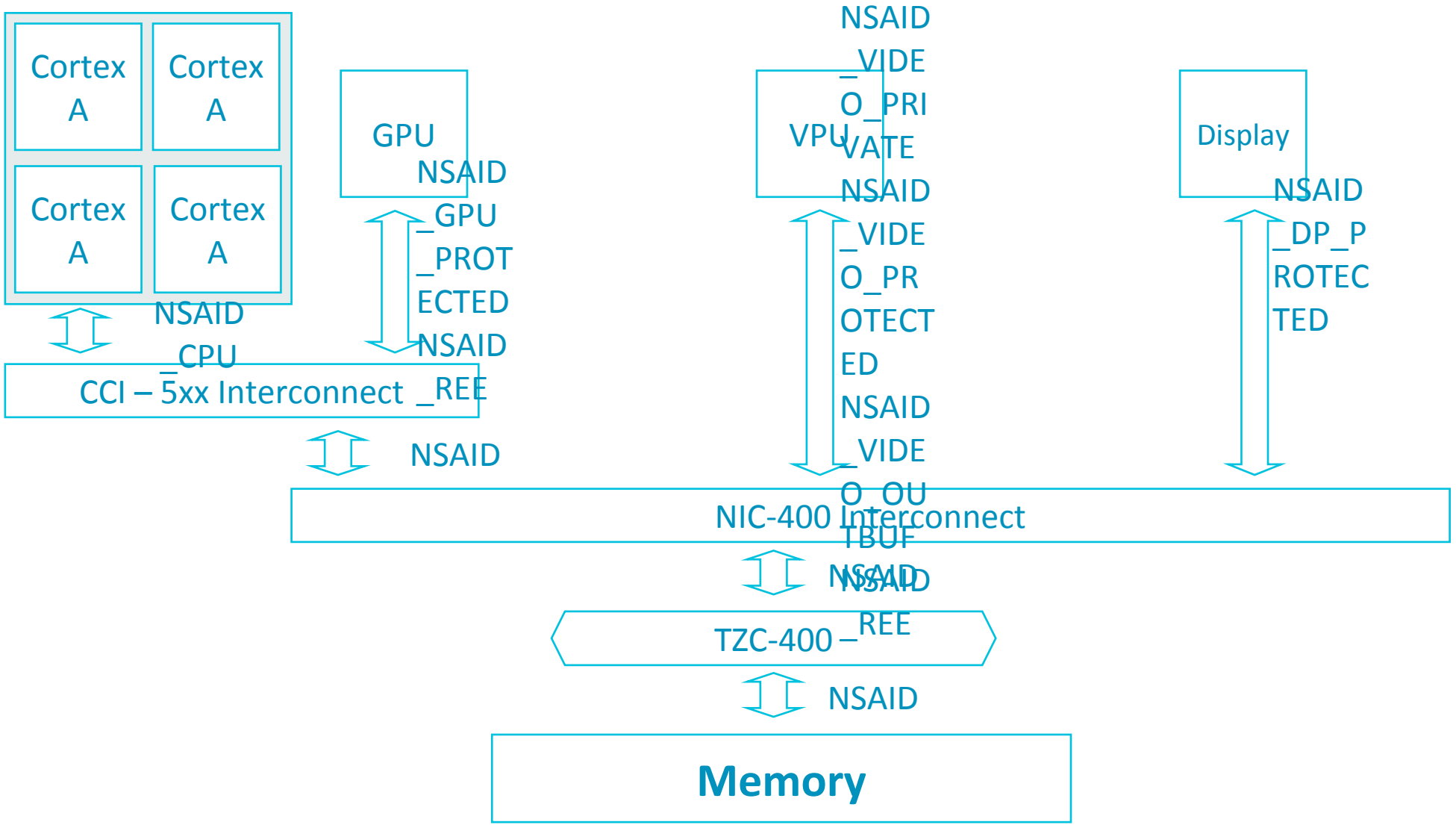



- Non-Secure Bitstream could **only** be accessed by Non-Secure hardware components
- Secure Bitstream could **only** be accessed by 'Protected' hardware components
- Display controller could read both types of bitstreams
- Mention the word 'Protected' – leads to Protected Memory and Protected Mode of HW



arm

# Hardware Architecture of TZMP1

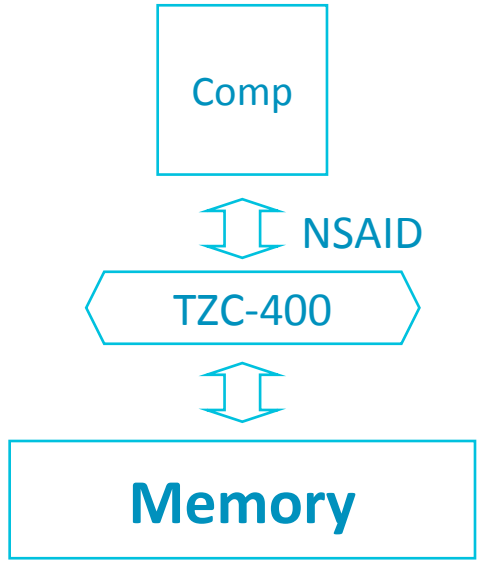





arm

# Firewall of Accessing - Arm Trustzone Controller 400

| Region | Ranges | NSAID 1 | NSAID 2 | … | NSAID 16 | Secure Access |
|---|---|---|---|---|---|---|
| 0 | All Memory | RW Configurable | RW Configurable | | RW Configurable | RW Configurable |
| 1 | Configurable | RW Configurable | RW Configurable | | RW Configurable | RW Configurable |
| 2 | Configurable | RW Configurable | RW Configurable | | RW Configurable | RW Configurable |
| 3 | Configurable | RW Configurable | RW Configurable | | RW Configurable | RW Configurable |
| 4 | Configurable | RW Configurable | RW Configurable | | RW Configurable | RW Configurable |
| 5 | Configurable | RW Configurable | RW Configurable | | RW Configurable | RW Configurable |
| 6 | Configurable | RW Configurable | RW Configurable | | RW Configurable | RW Configurable |
| 7 | Configurable | RW Configurable | RW Configurable | | RW Configurable | RW Configurable |




- Each non-secure memory accessing hardware is assigned with a Non-Secure Access ID (NSAID)
- TZC-400 checks NSAID and region permissions to decide access availability
- Total 8 regions and 16 NSAIDs are supported in TZC-400
- Secure accessing is also checked by TZC-400



arm

# Content

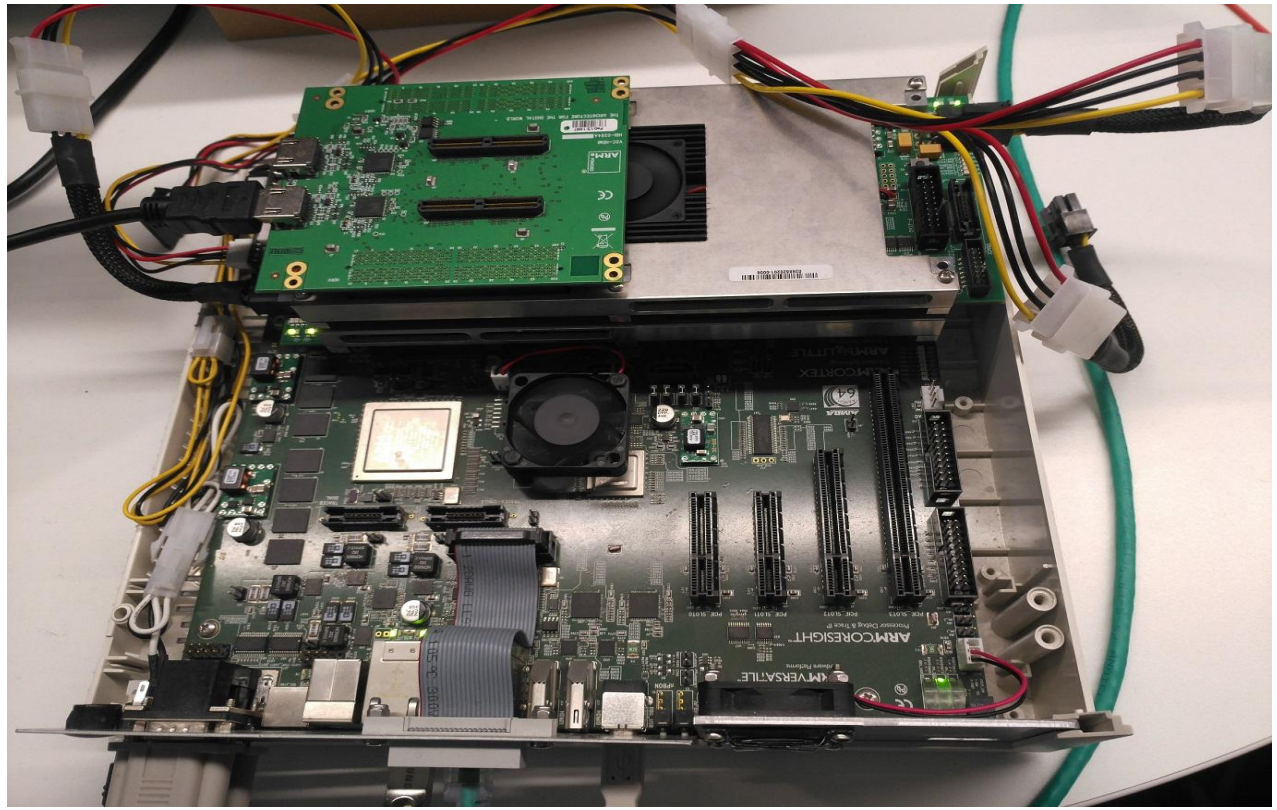
- DRM Applications and Secure Video Path
- Regular Secure Video Path Design with Trustzone
- TZMP1 Design Concepts

- **Reference Implementation Details**



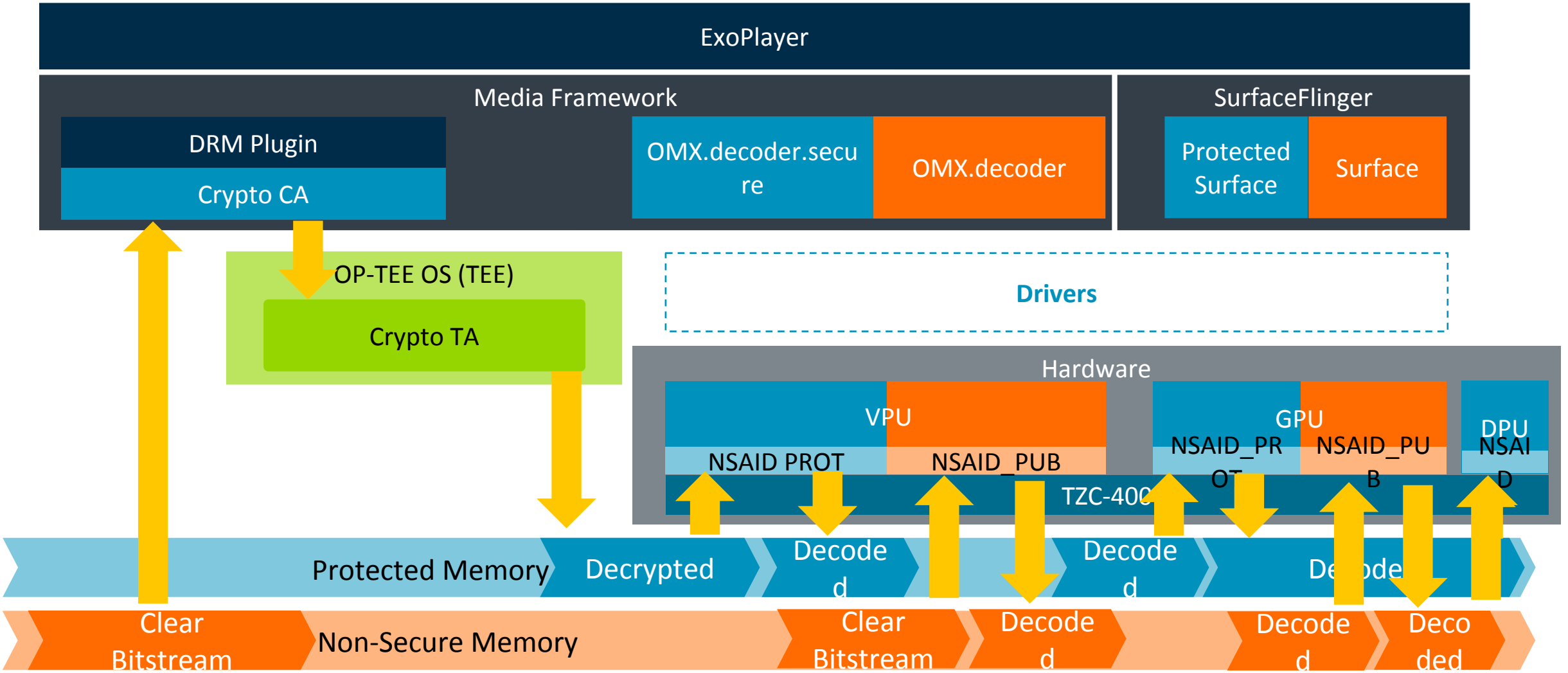
arm

# Platform and Software Components



| Component | Description |
|---|---|
| Board | Juno-r2 + 2 x Logictile |
| Non-Secure OS | Android<br>lsk-4.4-armlt Kernel |
| Secure OS | OPTEE OS |
| Boot | Arm-tf |
| Media IP | Arm Mali V550 G71 DP650 |
| DRM | Clearkey / Widevine |

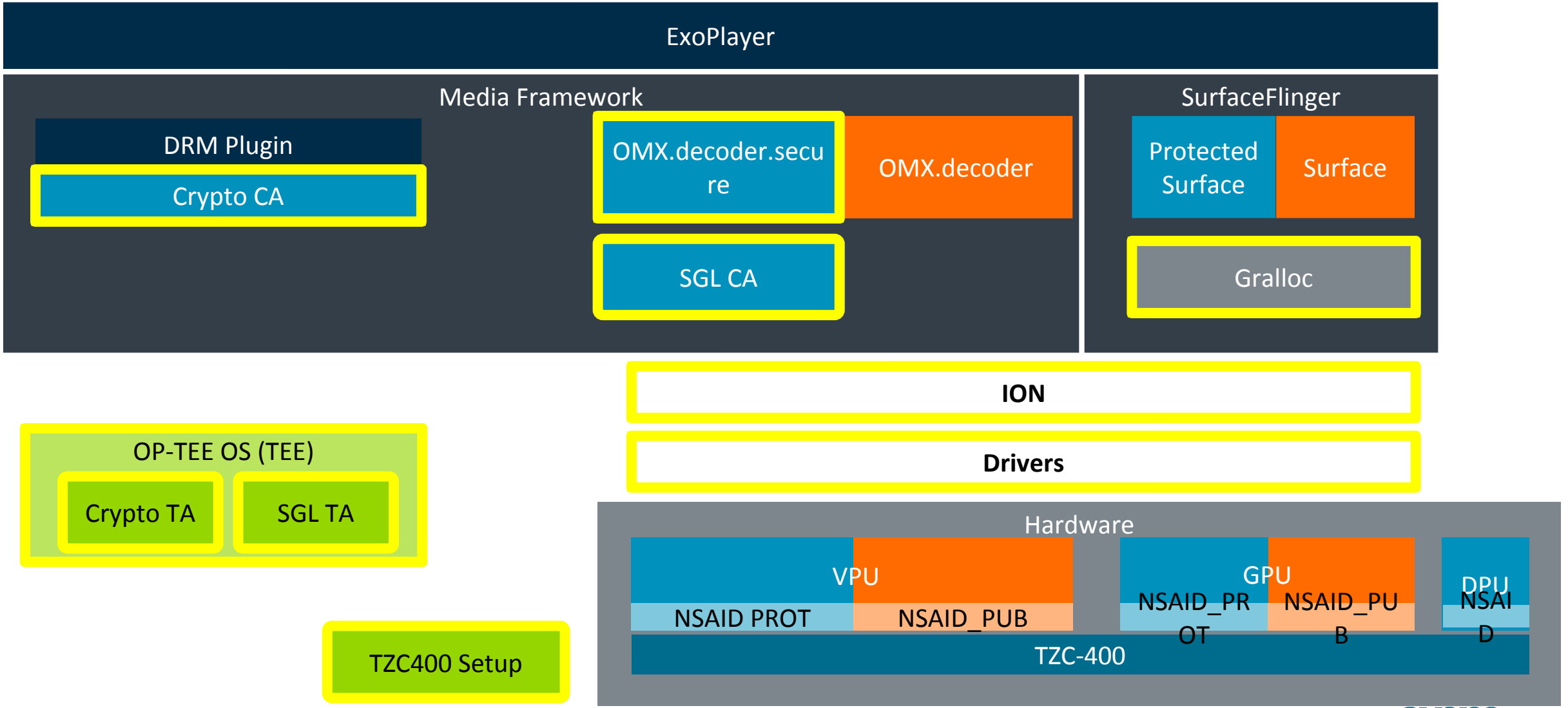
# Overall Reference Implementation






arm

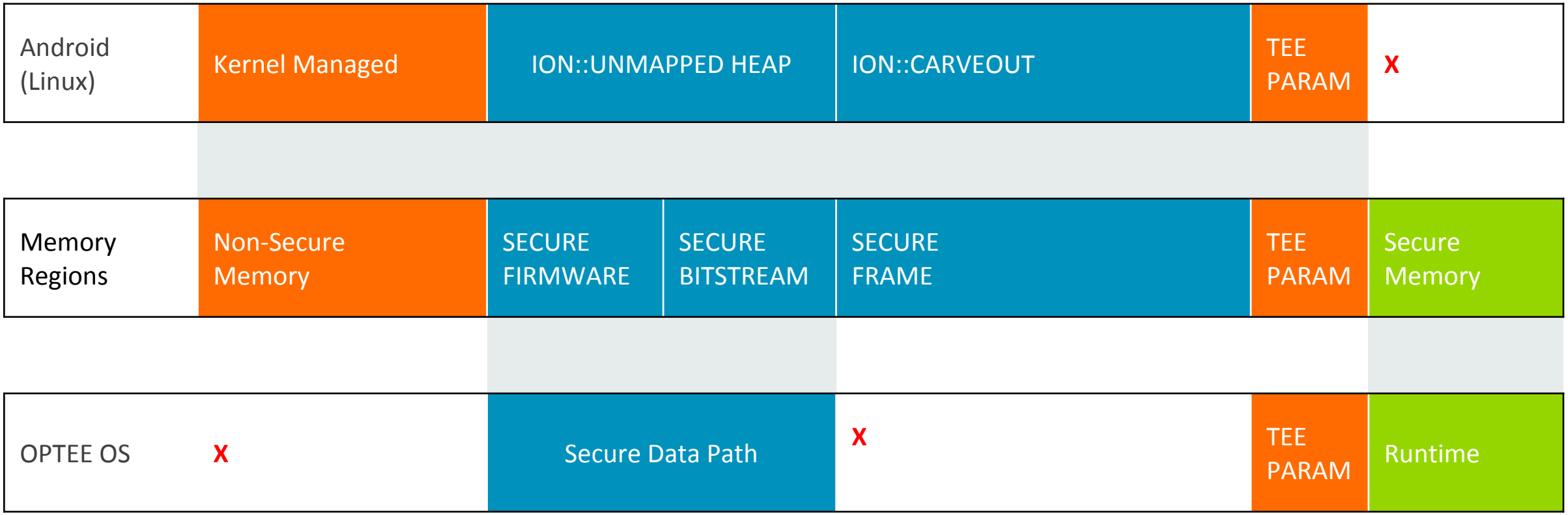
# Required Software Modifications






arm

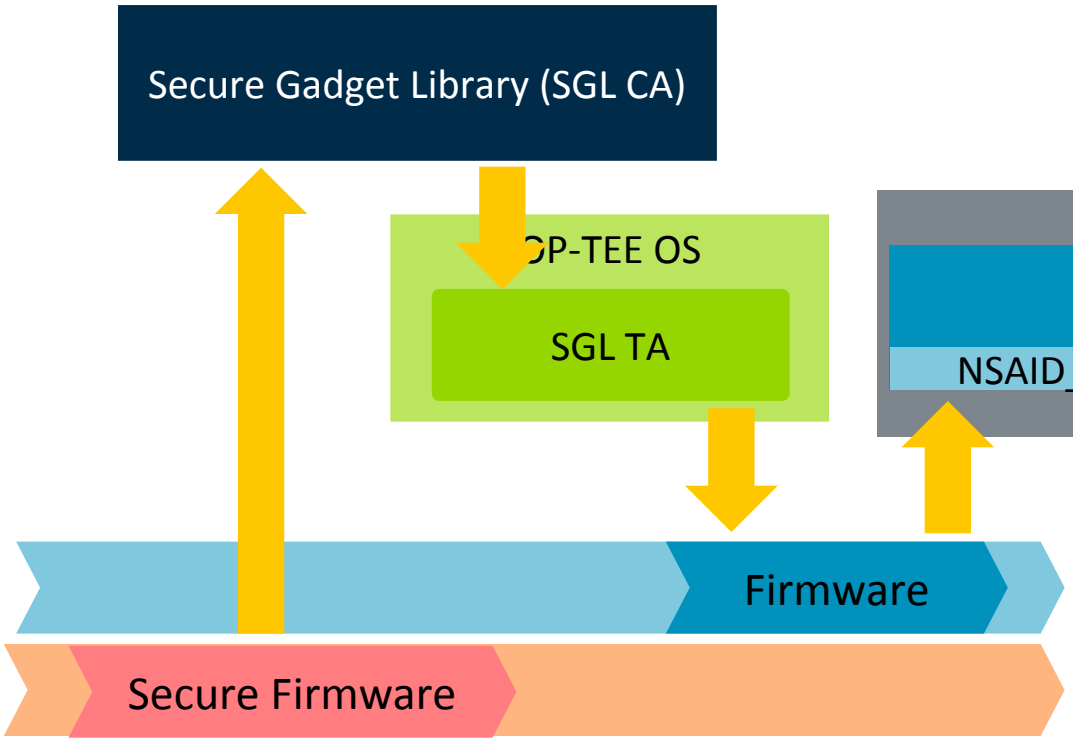
# Memory Regions

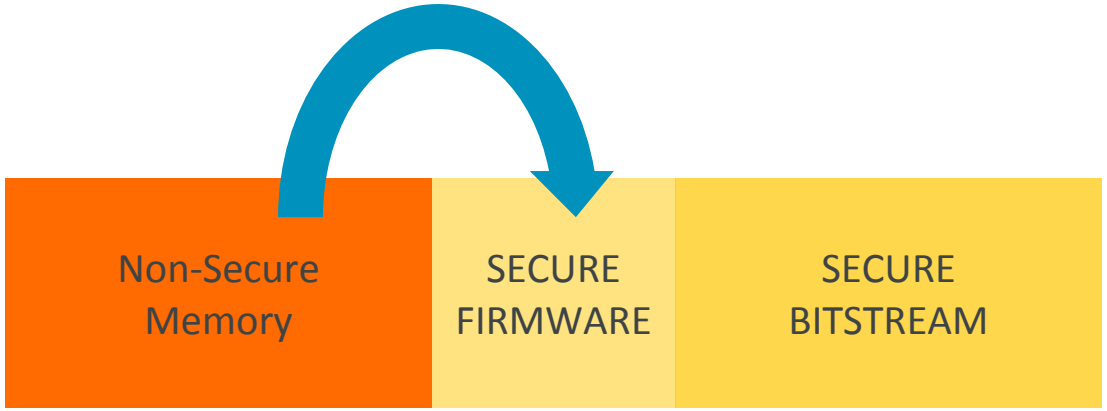





arm

# Secure VPU Firmware Loading



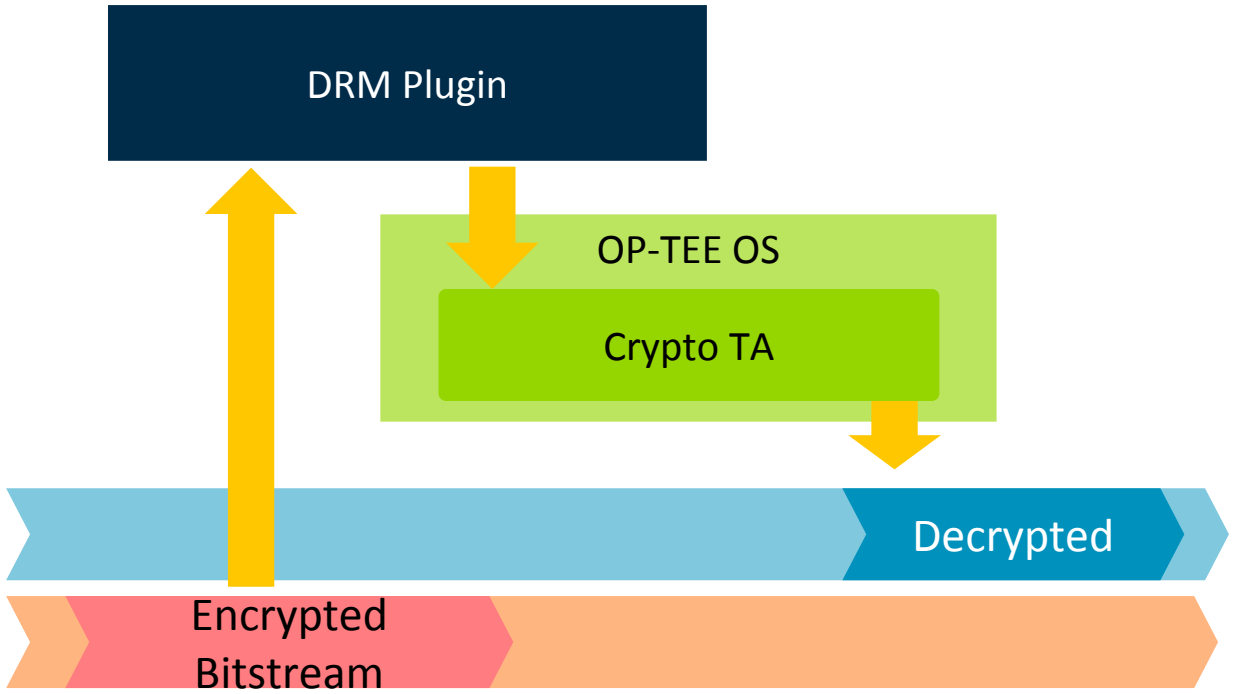



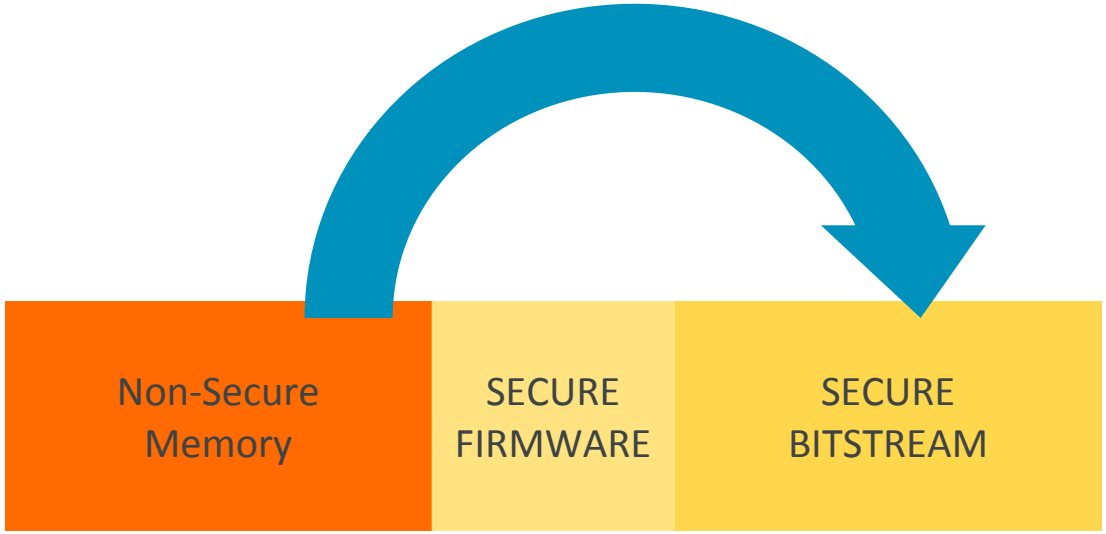

- Mandatory for firmware based decoder
- Unnecessary for non-firmware based decoder
- SDP Usage



arm

# Adopt DRM Crypto



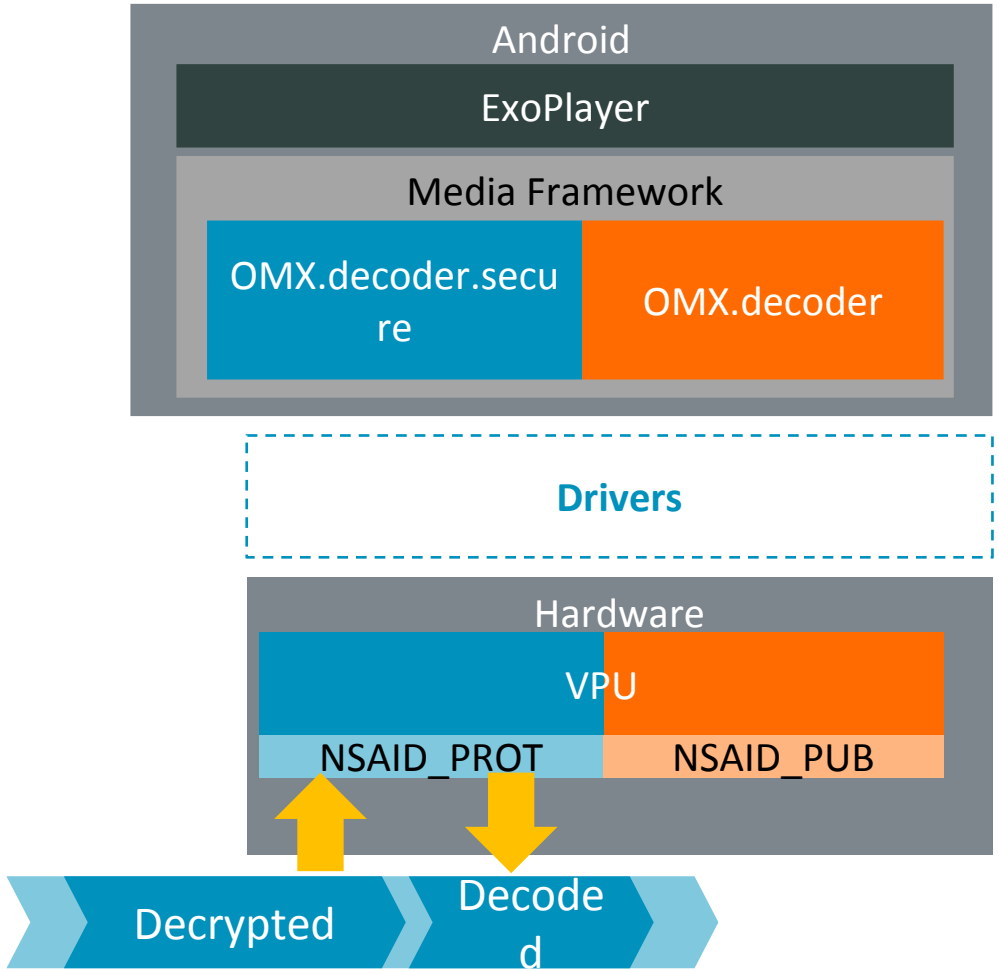




- Decrypt in OPTEE OS
- Put result into protected memory
- Take advantage SDP of OPTEE OS SDP



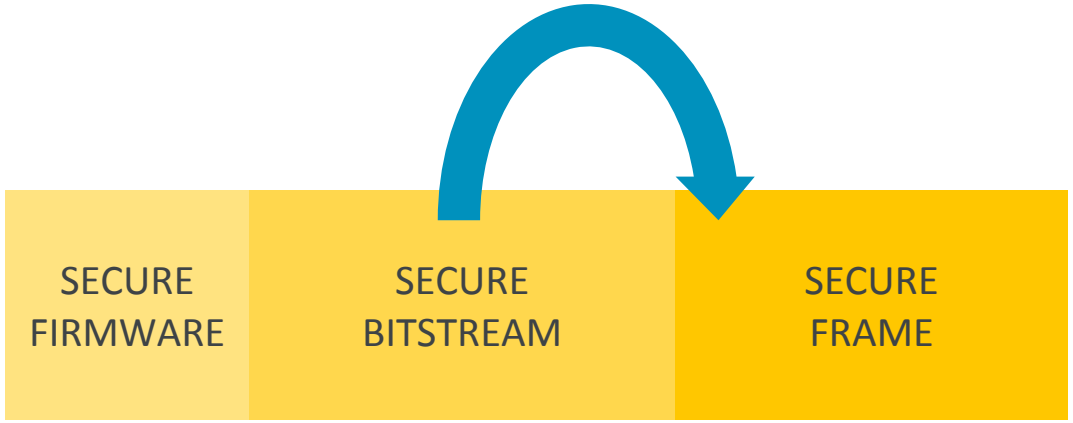
arm

# Adopt Secure Decoder




‘Secure Video Path’ in Android

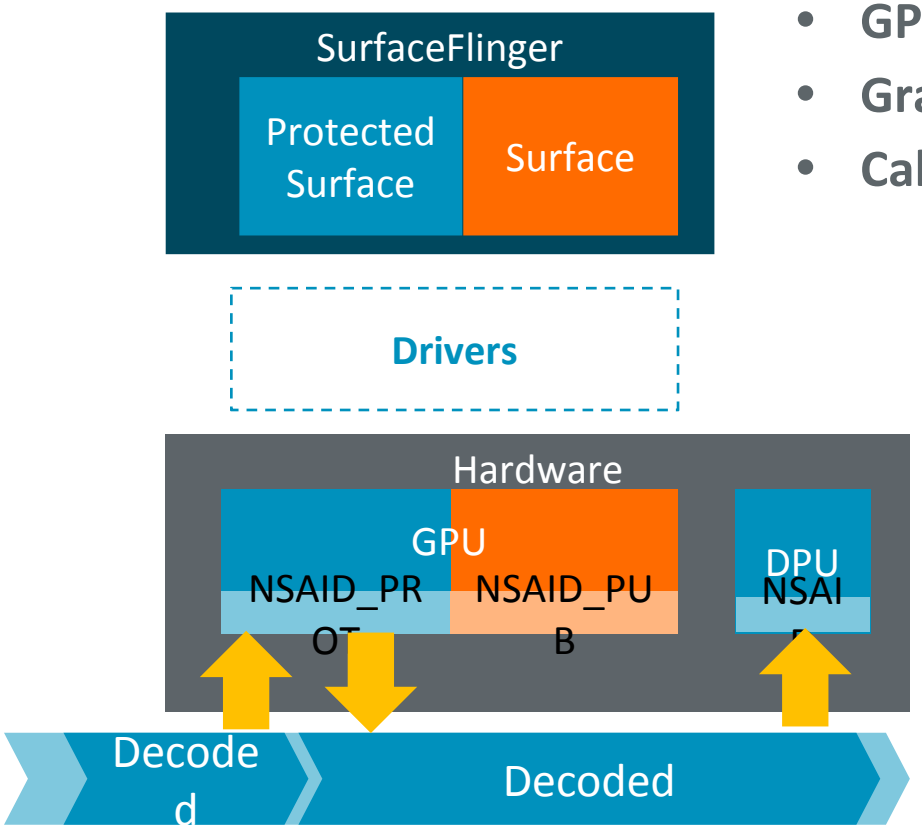
- Is DRM required ‘Secure Codec’ ?
  - Is ‘Secure Codec’ available ?
    - Setup Secure Video Path
      - Choose ‘Secure Codec’ component
      - Apply Protected Surface for output



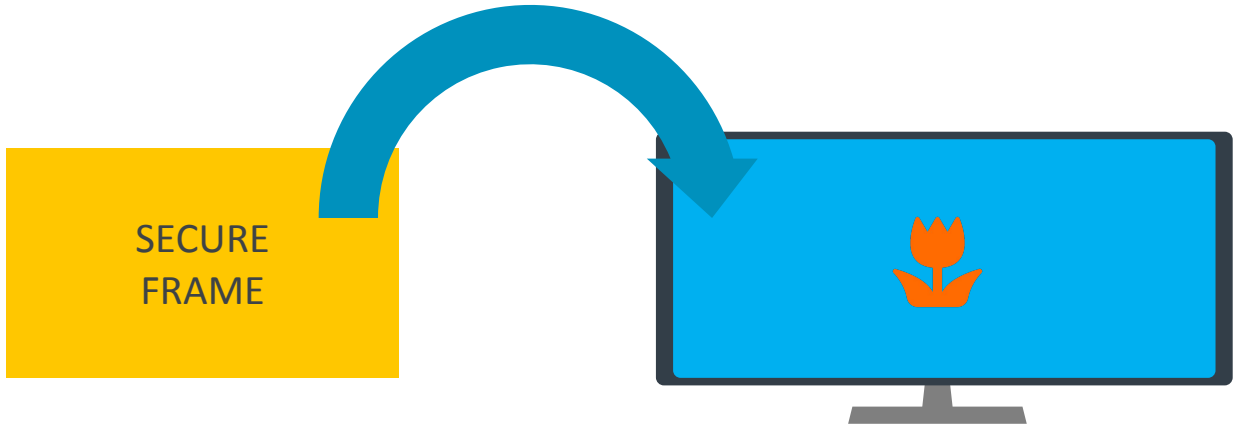



arm

# Graphics and Display




- GPU and Display calls gralloc for surface buffers
- Gralloc allocates memory from specified buffer due to flags
- Call ION APIs for protected buffer






arm

# References

| | Components | Repository |
|---|---|---|
| 1 | Workspace | To be upstreamed in April |
| 2 | Arm-tf | https://github.com/ARM-software/arm-trusted-firmware (Upstreaming) |
| 3 | OPTEE OS | https://github.com/OP-TEE/optee_os (Done) |
| 4 | Android manifest | To be upstreamed in April |
| 5 | Secure Gadget Library | Upstreaming in linaro private repository |
| 6 | Gralloc | https://developer.arm.com/products/software/mali-drivers/android-gralloc-module |
| 7 | Multimedia IP | Contact Arm support |
| 8 | Linux and DTS | https://git.linaro.org/landing-teams/working/arm/kernel-release.git (Upstreaming) |
| 9 | Arm Connected Community Page | Planed to be done by ~April |



arm

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
תודה

arm