Android Widevine on OP-TEE

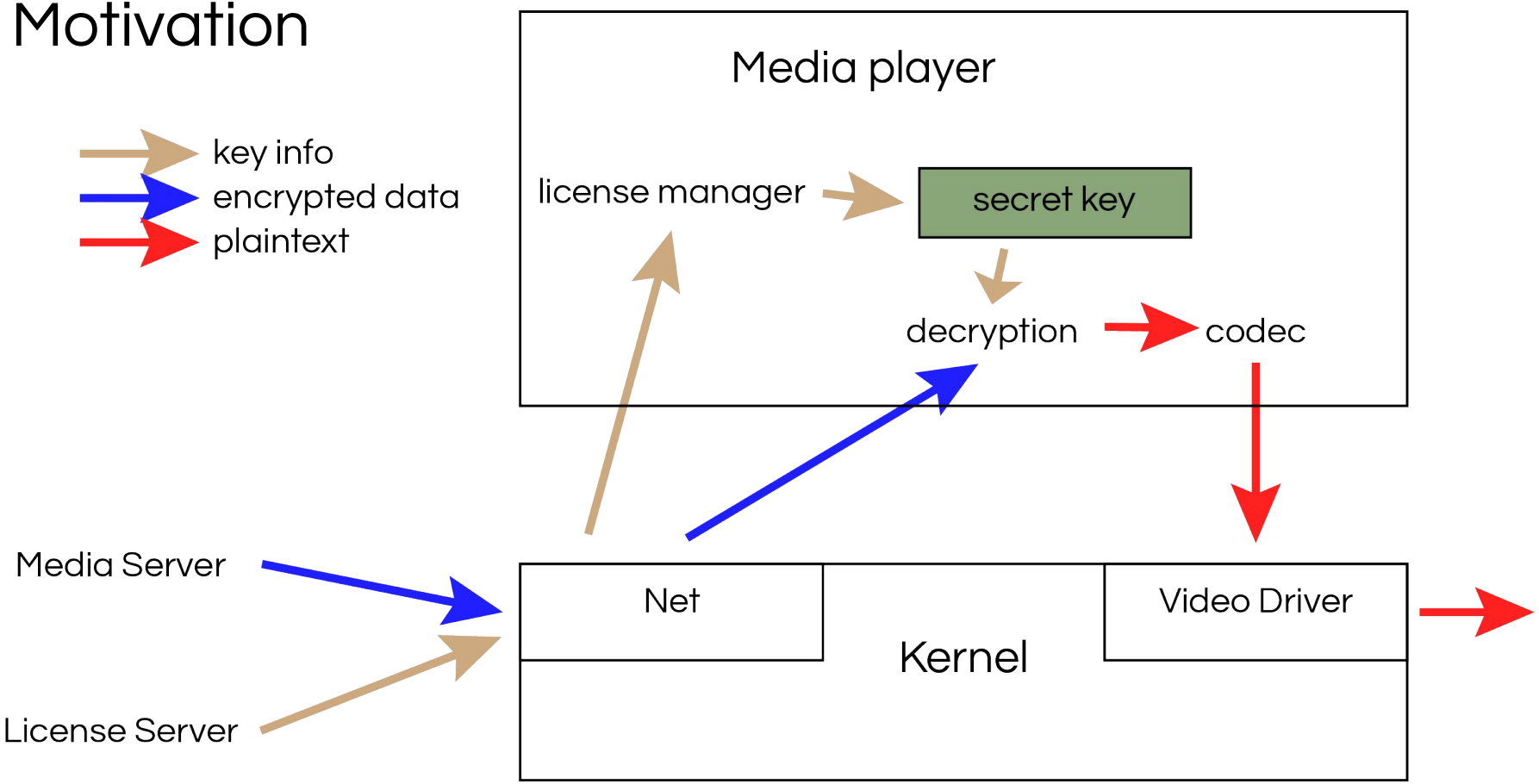
David Brown

ENGINEERS
AND DEVICES
WORKING
TOGETHER

Agenda

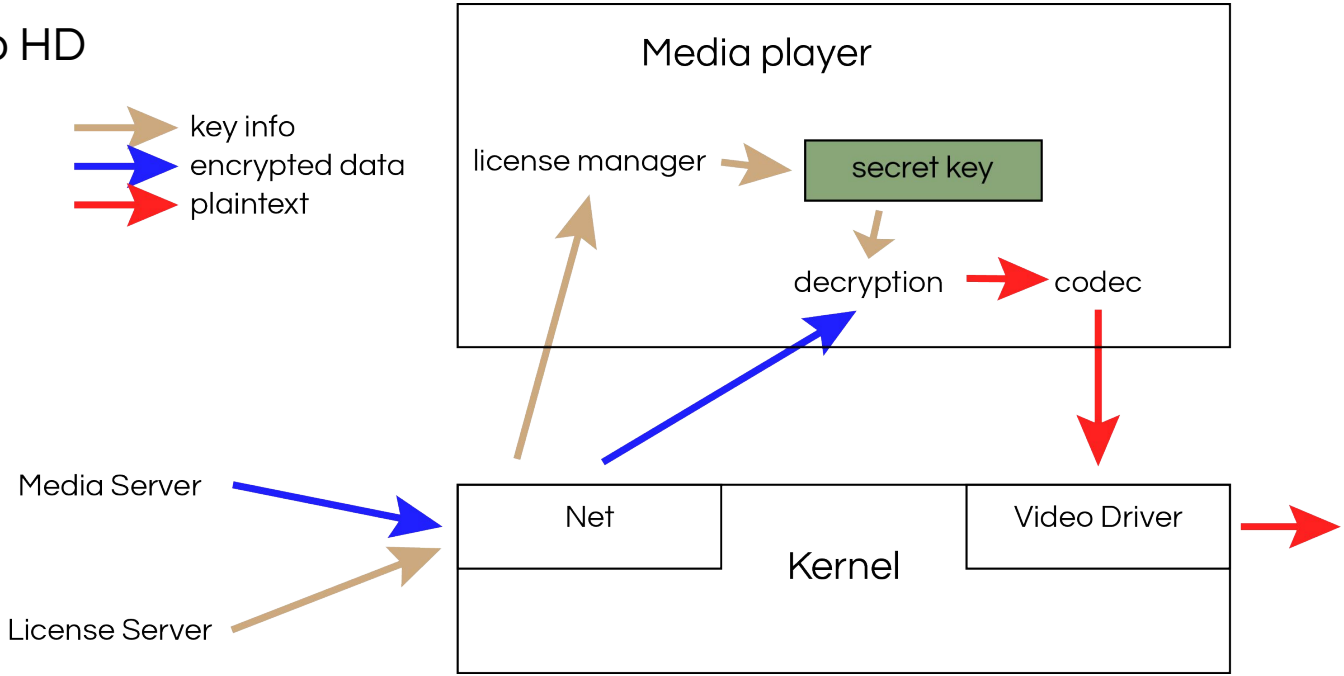
- **Motivations**
- How not to do it
- OP-TEE
- General solutions
- Overview of Widevine

Motivation


key info
encrypted data
plaintext
Media player
license manager
secret key
decryption
codec
Media Server
License Server
Net
Kernel
Video Driver

Motivation

- Software playback
- Red arrow, bad!
- Creators sad, no HD



ENGINEERS
AND DEVICES
WORKING
TOGETHER

Agenda

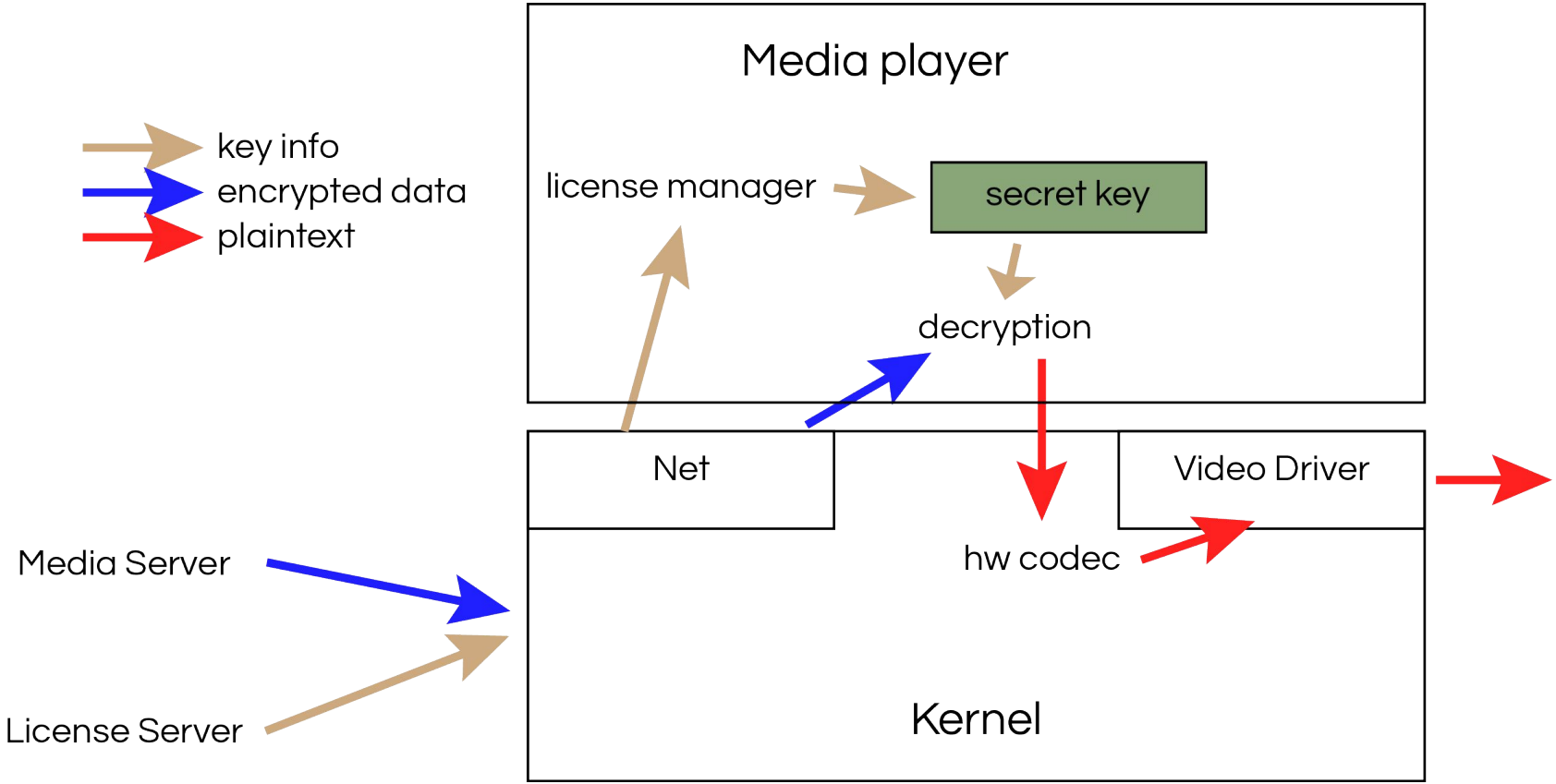
- Motivations
- **How not to do it**
- OP-TEE
- General solutions
- Overview of Widevine

How not to do it?

- Plaintext video passes through userspace
- Find exploit in player, or many other things
- Root makes it trivial to get

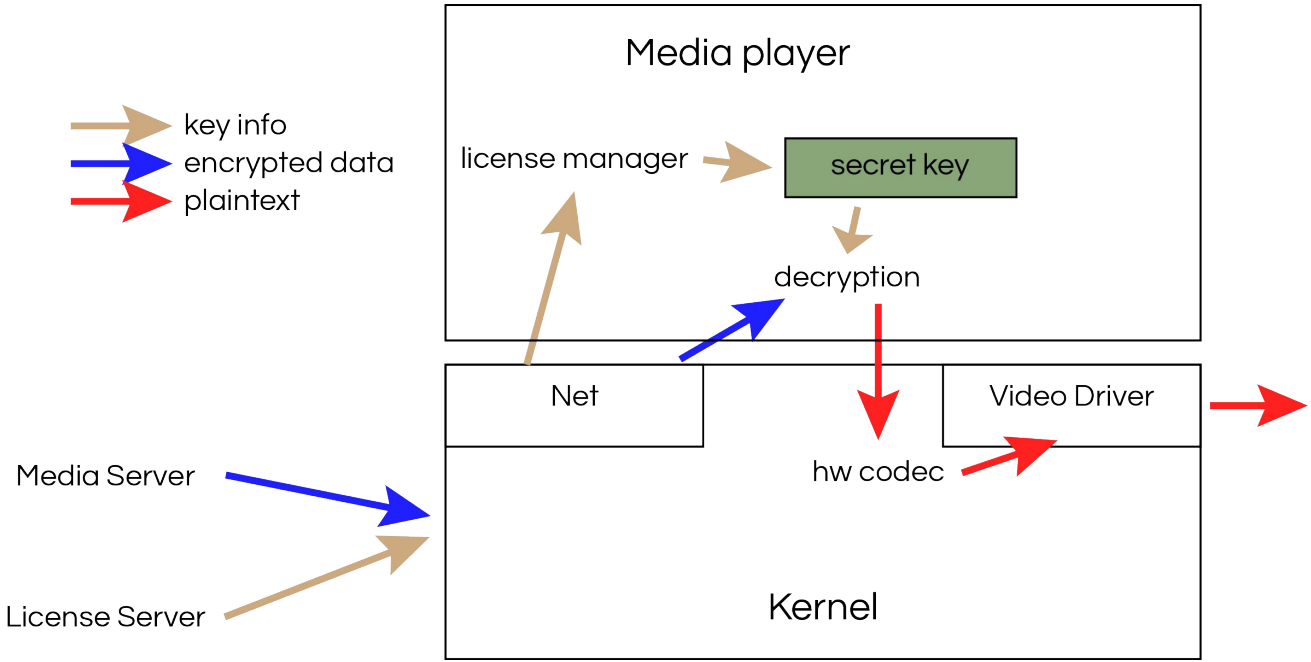
- Notice the key is also in userspace
- This is bad

Can we do better?

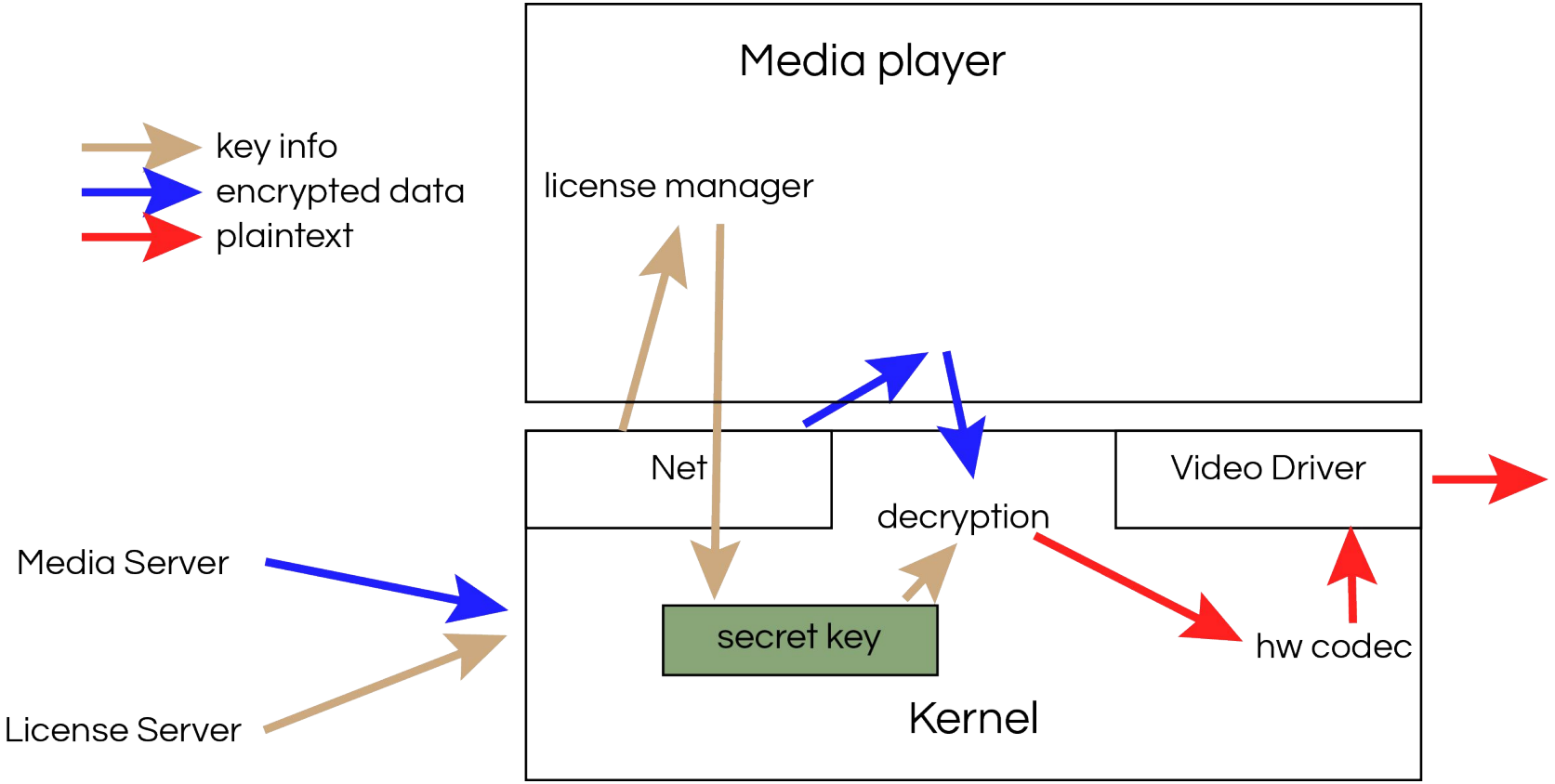


Can we do better?

- Less is accessible
- Plaintext still in userspace
- Creators still sad

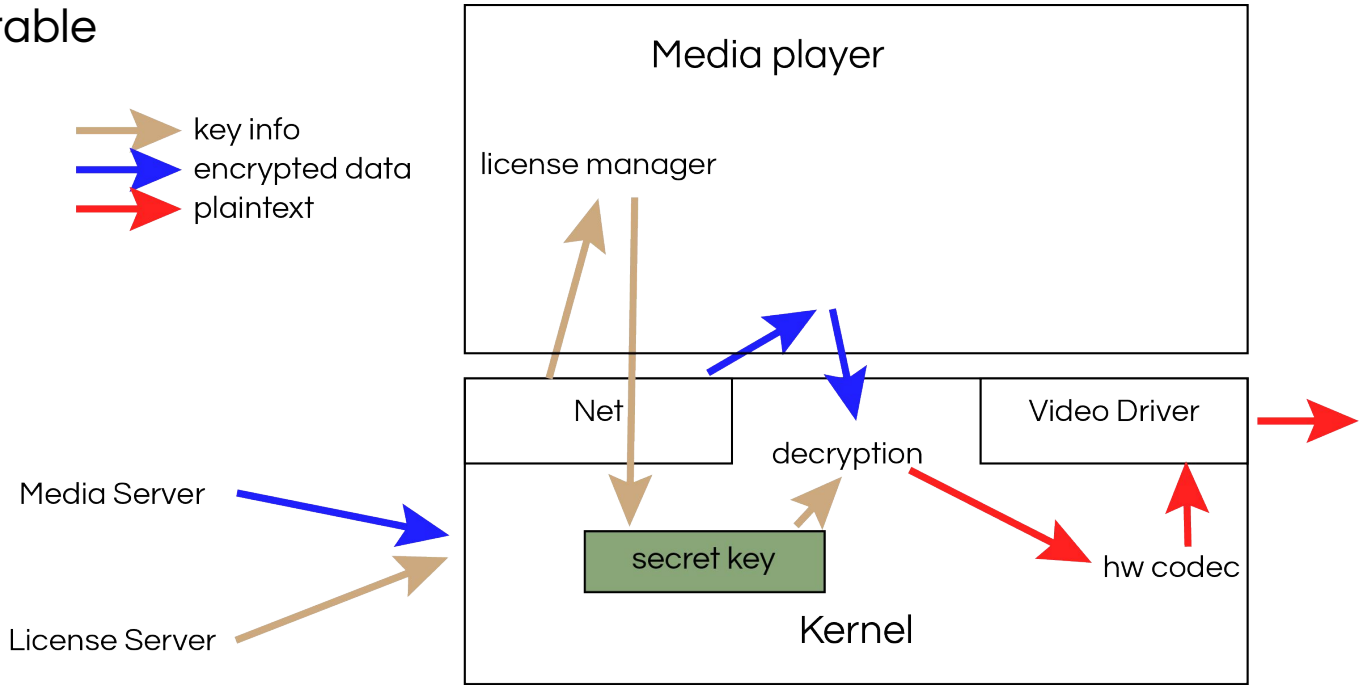


All plaintext in kernel?

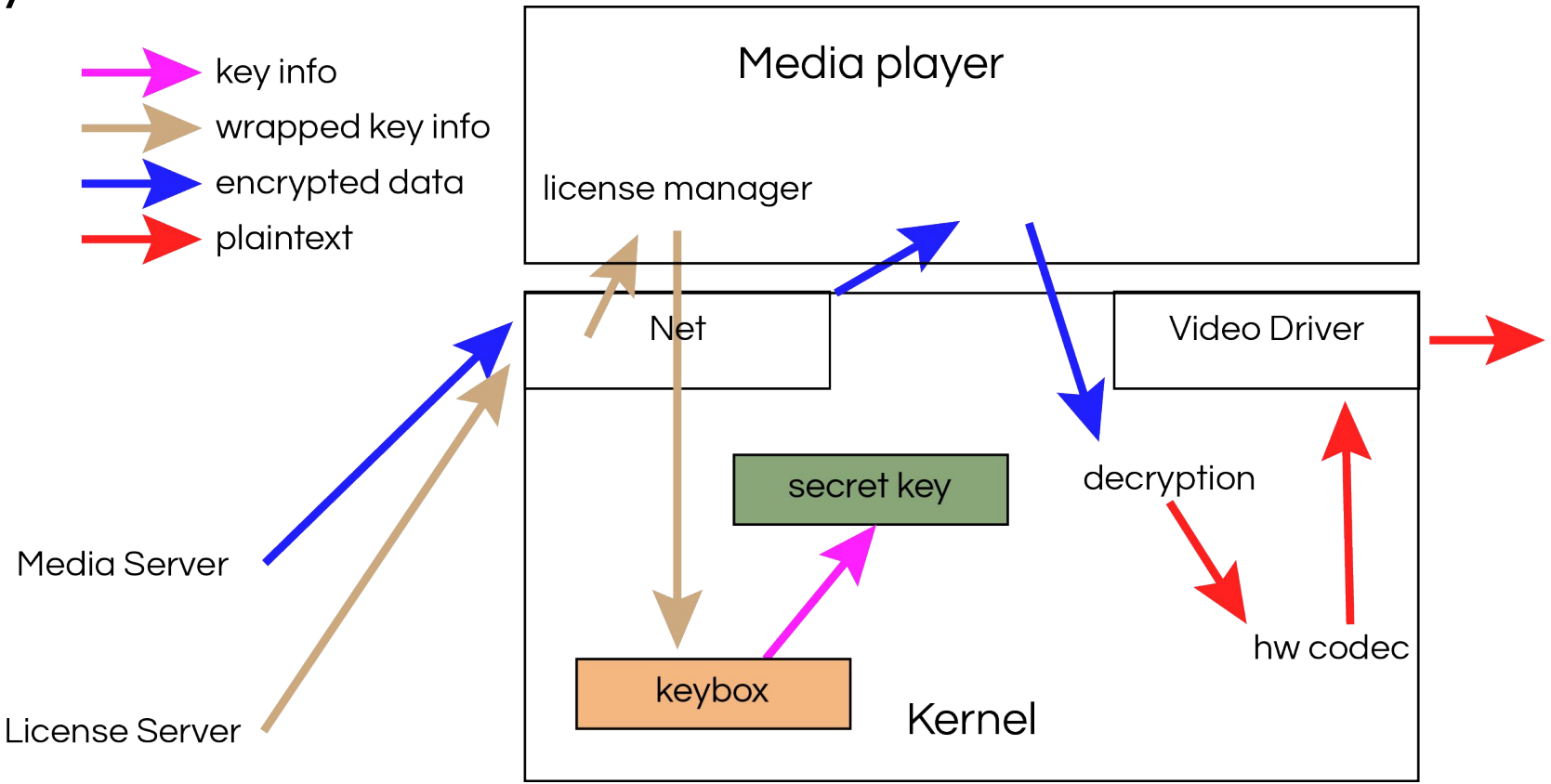


All plaintext in kernel?

- Better, no plaintext in userspace
- Key still there
- Kernel is vulnerable

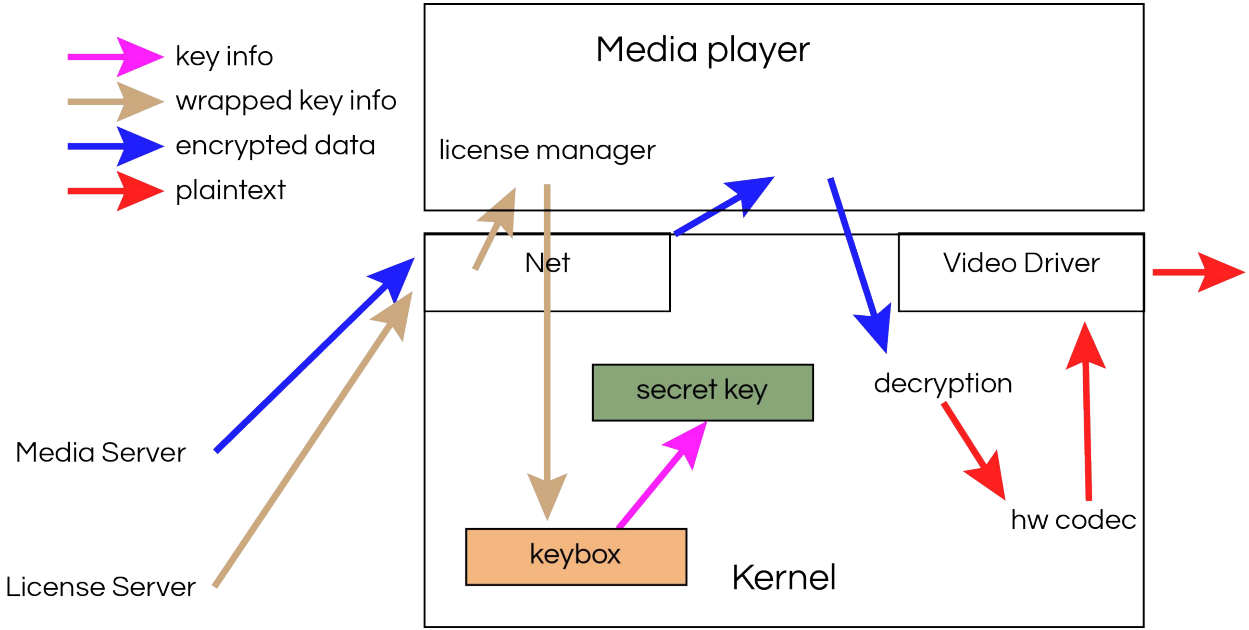


Key in kernel



Key in kernel

- All key/plaintext now in kernel
- Content protected from userspace
- Kernel exploits possible
- Creators still sad

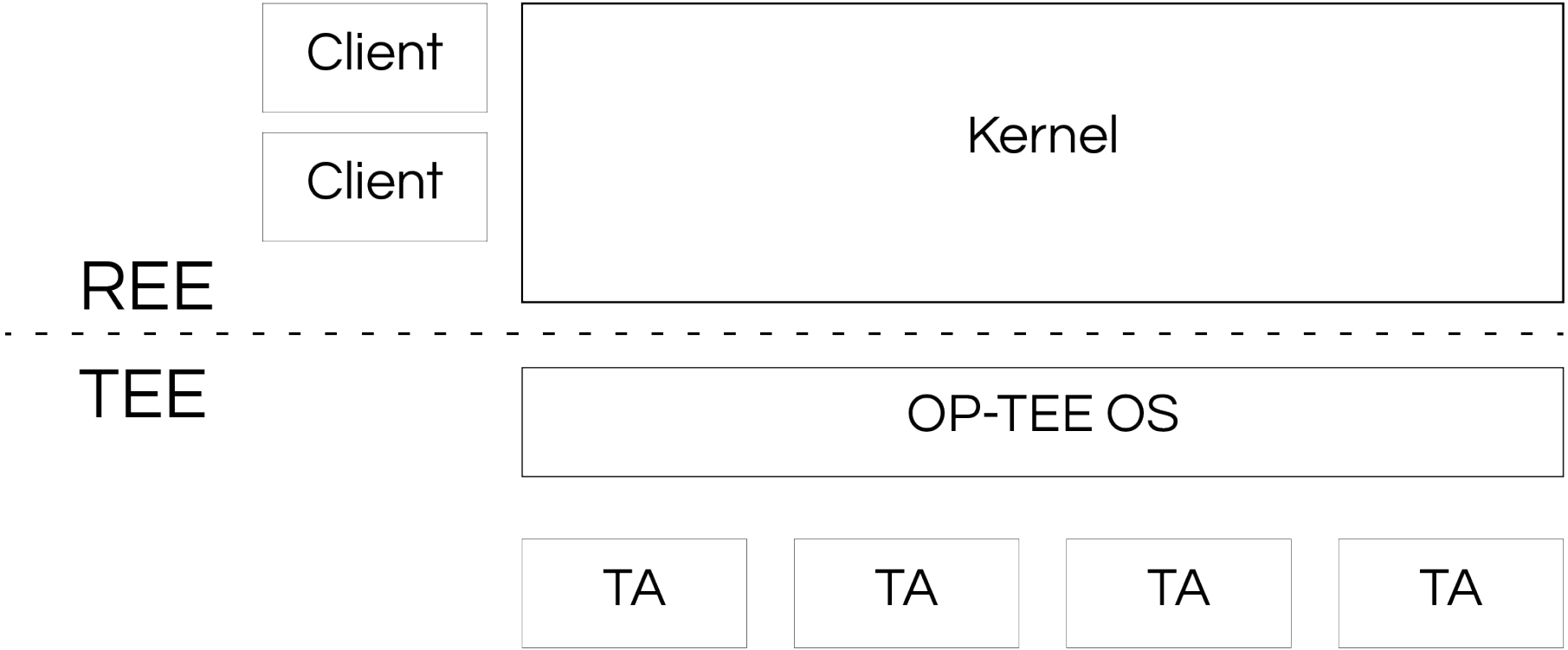


ENGINEERS
AND DEVICES
WORKING
TOGETHER

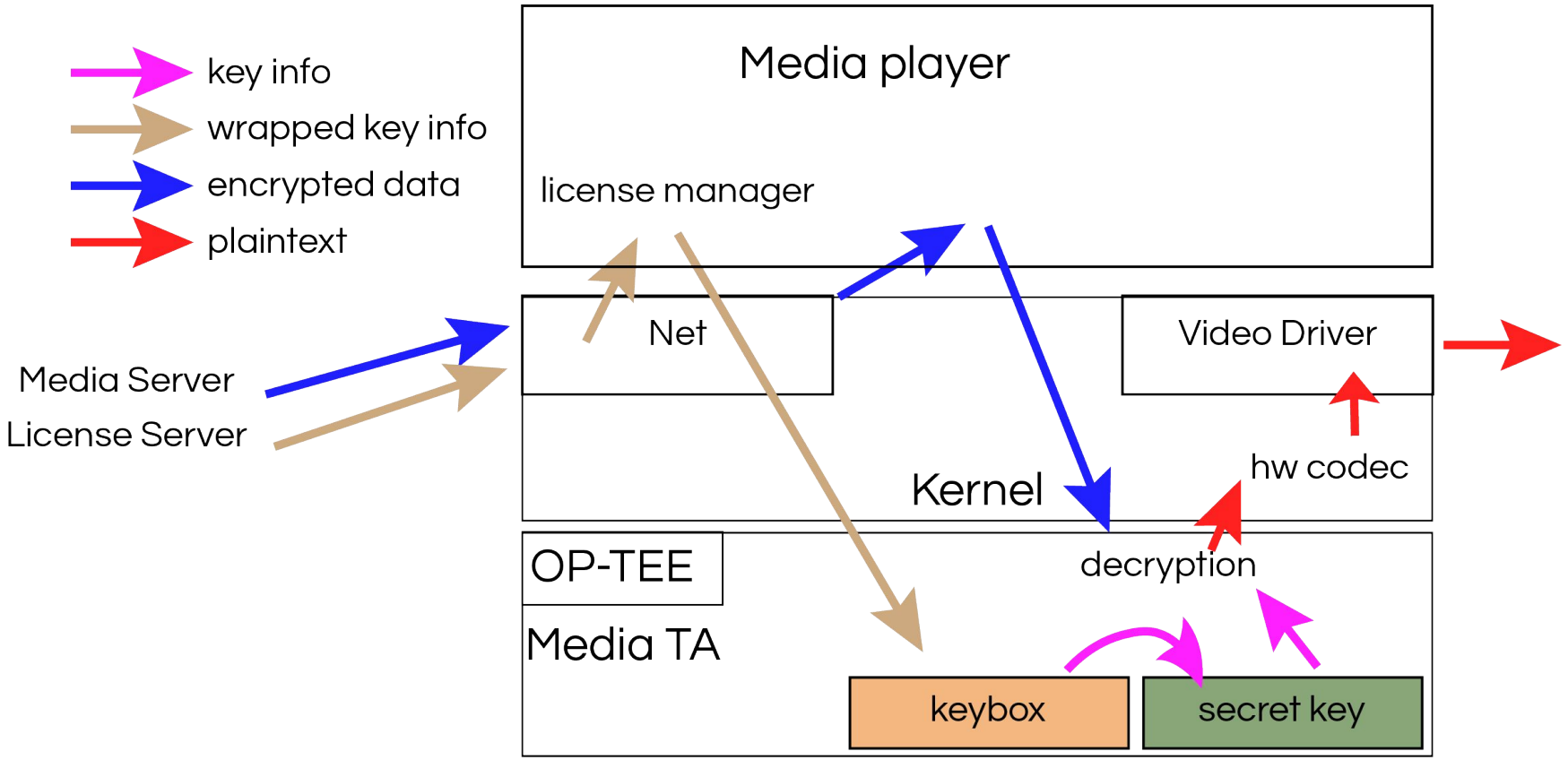
OP-TEE

- ARM® TrustZone®
  - Trustable through boot into secure OS
  - Runs alongside Kernel
- GlobalPlatform TEE Specification
  - OP-TEE is our implementation
  - Allows trusted apps, and clients

OP-TEE

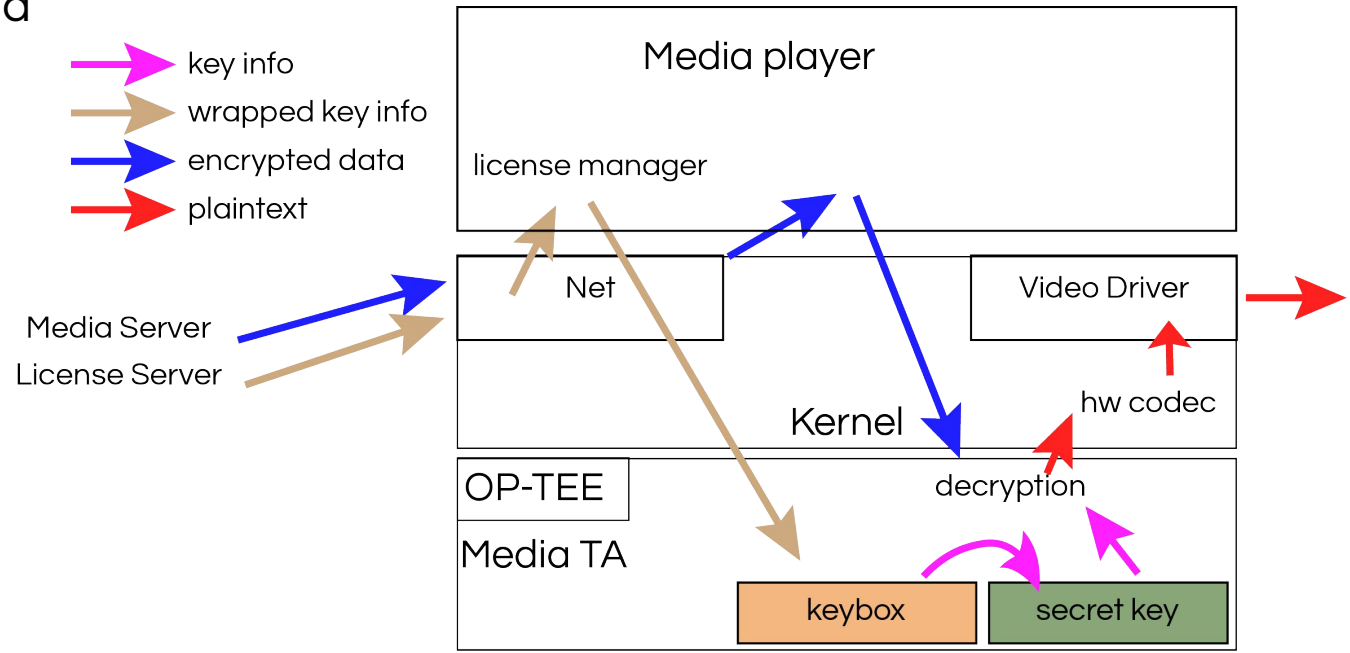


DRM in TEE


key info
wrapped key info
encrypted data
plaintext
Media player
license manager
Net
Video Driver
Media Server
License Server
hw codec
Kernel
OP-TEE
decryption
Media TA
keybox
secret key

DRM in TEE

- Almost there, key is in TEE
- Plaintext video still available at end
- Providers **still** sad



One more thing

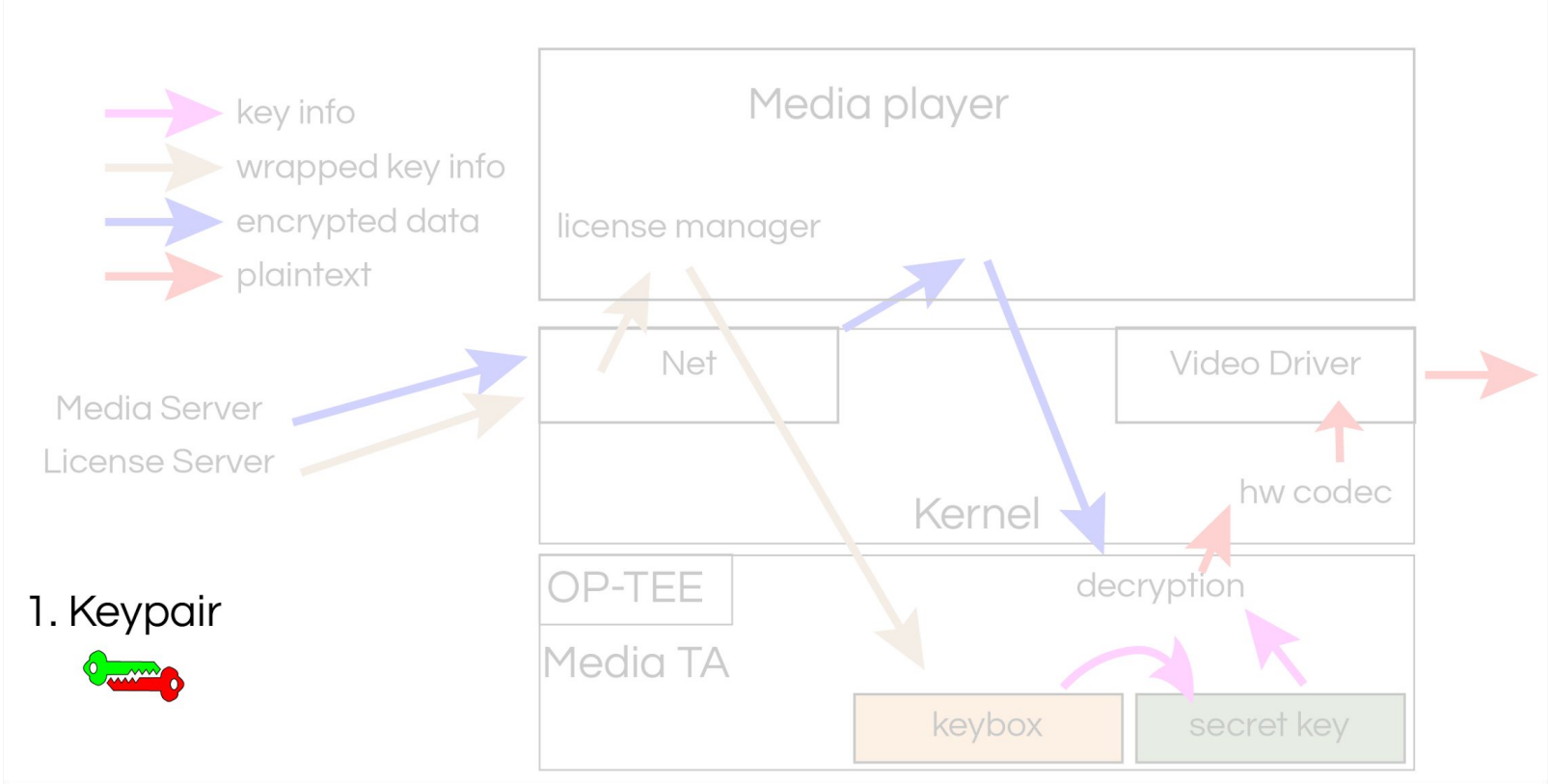
- We need a weird buffer
  - Accessible to secure side
  - Not readable by unsecure (even kernel)
  - Accessible by HW decoder
- SMAF
  - Secure memory allocator
  - TEE can decode into this memory
  - HW can play it back
- It’s tricky to get right, only certain HW should have access

ENGINEERS
AND DEVICES
WORKING
TOGETHER

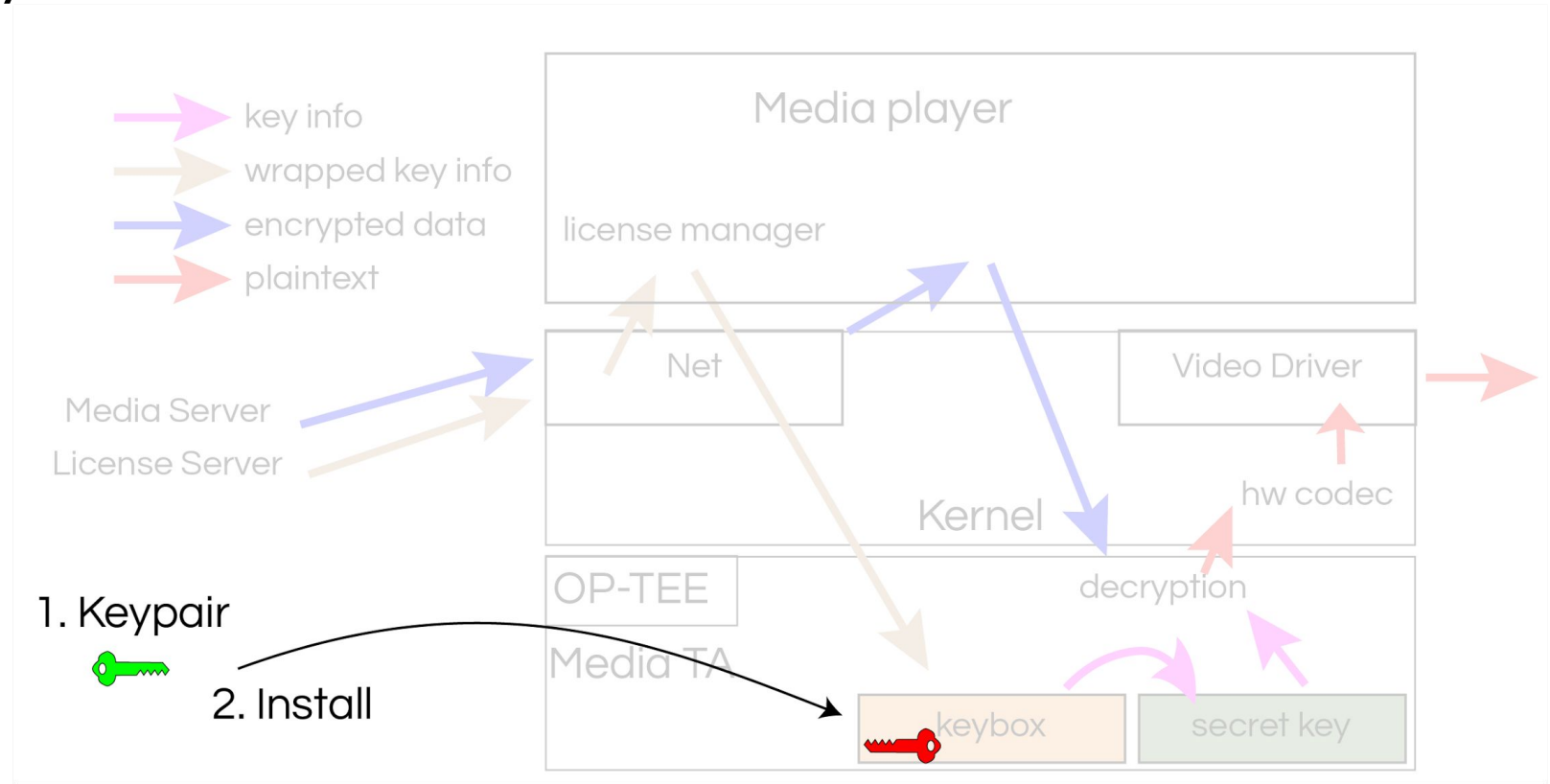
Agenda

- Motivations
- How not to do it
- OP-TEE
- **General solution**
- Overview of Widevine

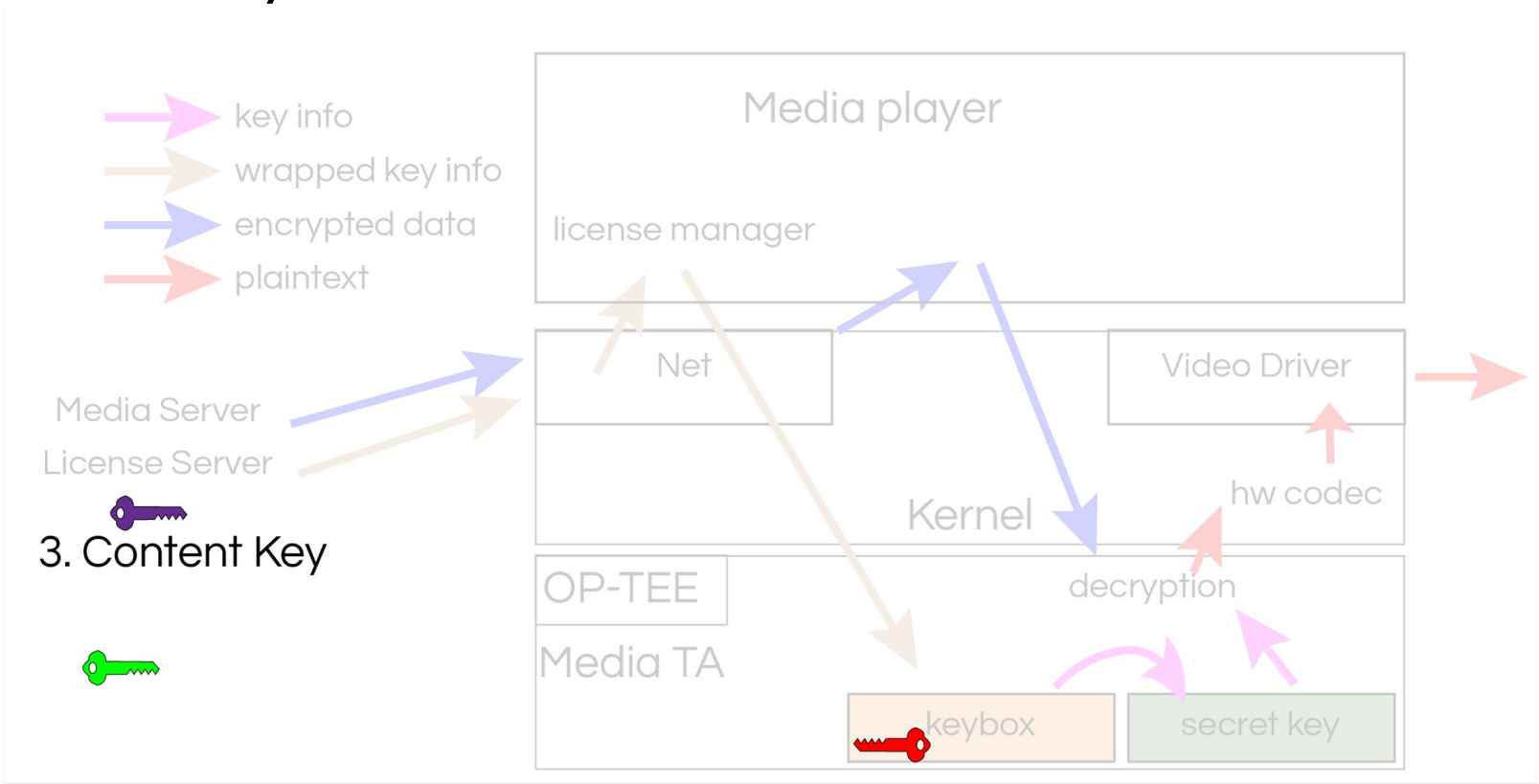
Keybox


key info
wrapped key info
encrypted data
plaintext
Media player
license manager
Net
Video Driver
Media Server
License Server
hw codec
Kernel
OP-TEE
decryption
Media TA
keybox
secret key
1. Keypair

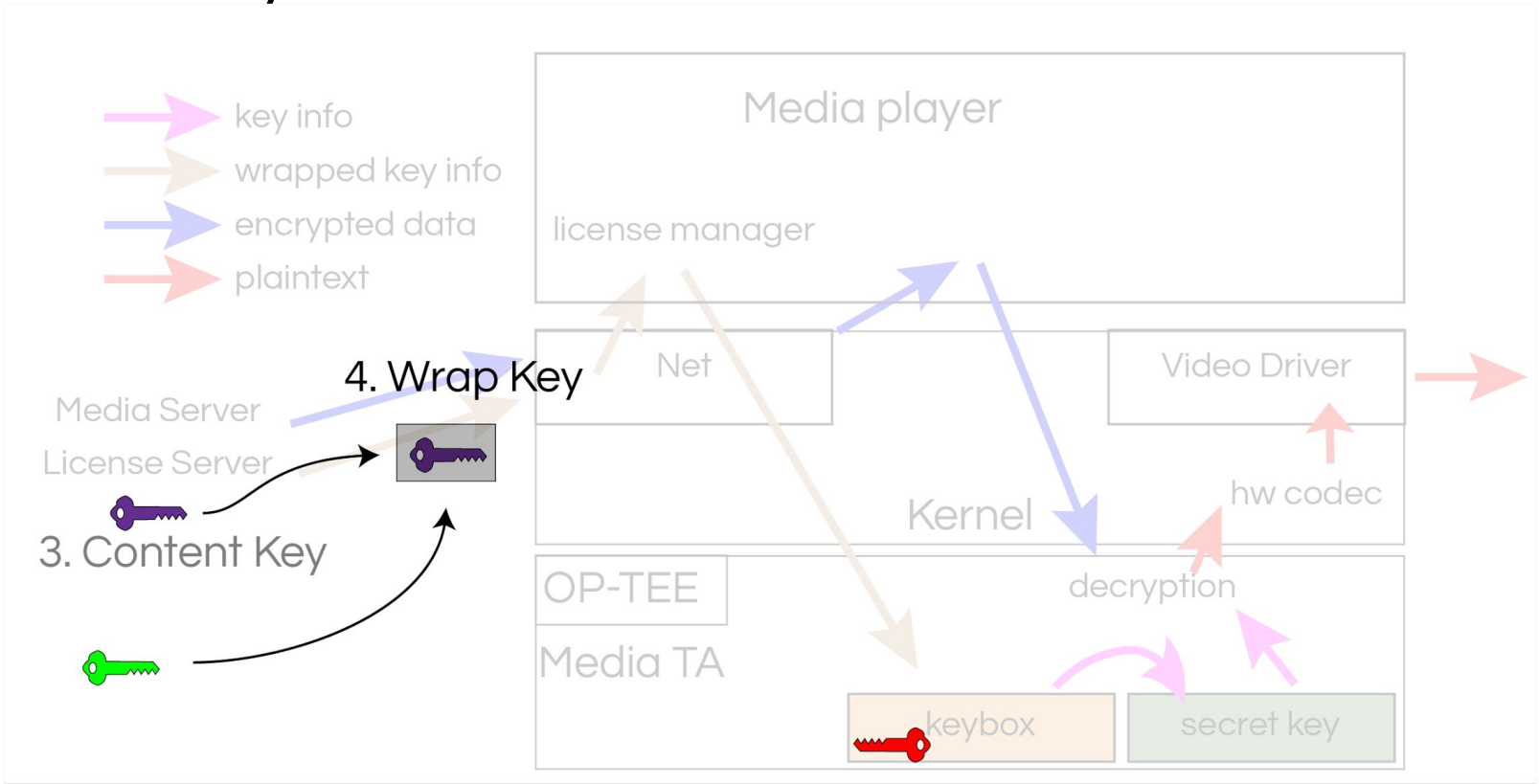
Keybox


key info
wrapped key info
encrypted data
plaintext
Media player
license manager
Net
Video Driver
Media Server
License Server
hw codec
Kernel
OP-TEE
decryption
1. Keypair
Media TA
2. Install
keybox
secret key

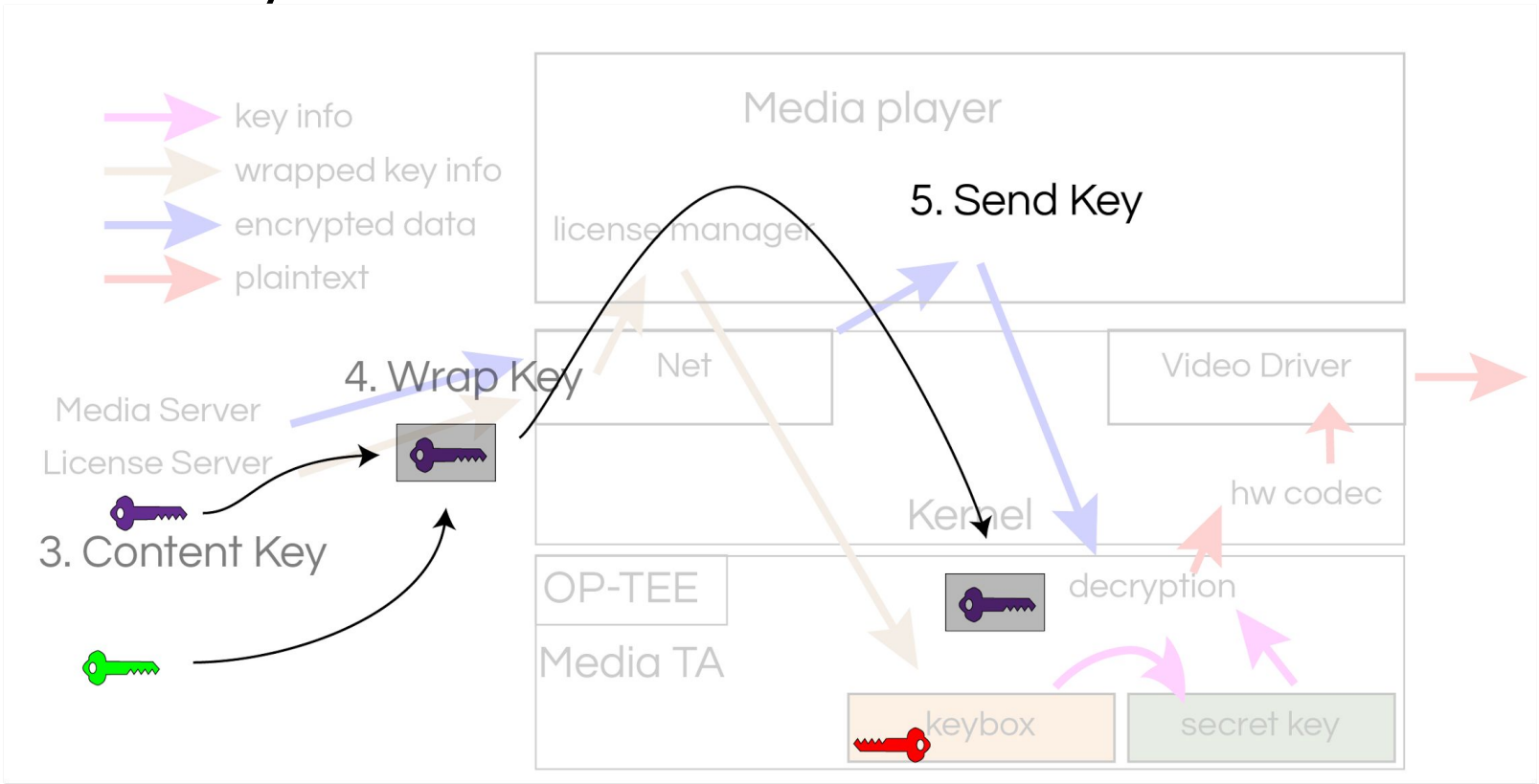
Content Key


key info
wrapped key info
encrypted data
plaintext
Media player
license manager
Net
Video Driver
Media Server
License Server
hw codec
Kernel
3. Content Key
OP-TEE
decryption
Media TA
keybox
secret key

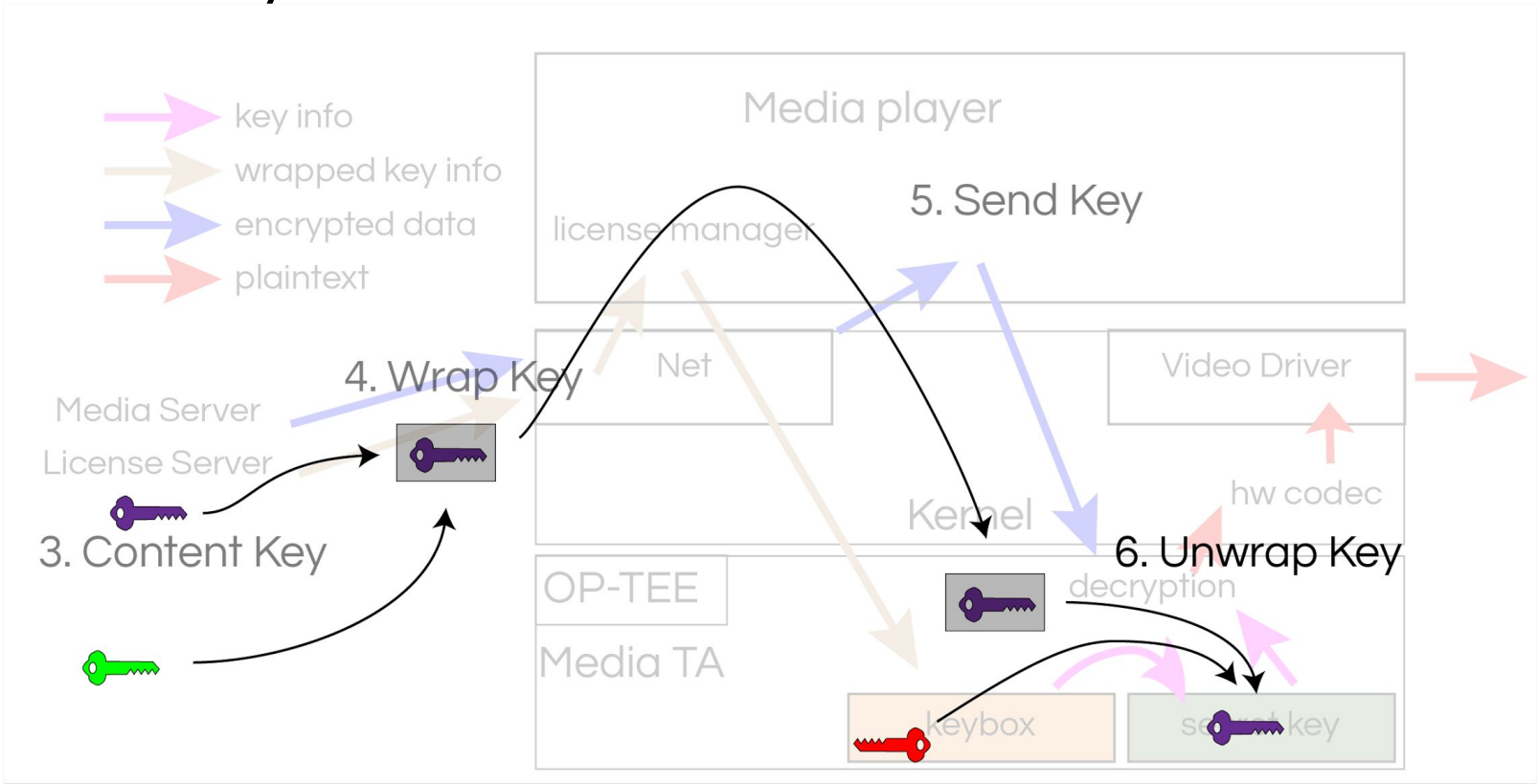
Content Key


key info
wrapped key info
encrypted data
plaintext
Media player
license manager
Net
Video Driver
hw codec
Kernel
OP-TEE
decryption
Media TA
keybox
secret key
4. Wrap Key
Media Server
License Server
3. Content Key

Content Key


key info
wrapped key info
encrypted data
plaintext
Media player
license manager
5. Send Key
Net
Video Driver
4. Wrap Key
Media Server
License Server
3. Content Key
hw codec
Kernel
OP-TEE
decryption
Media TA
keybox
secret key

Content Key


key info
wrapped key info
encrypted data
plaintext
Media player
license manager
5. Send Key
Net
Video Driver
4. Wrap Key
Media Server
License Server
3. Content Key
hw codec
Kernel
6. Unwrap Key
OP-TEE
decryption
Media TA
keybox
key

ENGINEERS
AND DEVICES
WORKING
TOGETHER

Agenda

- Motivations
- How not to do it
- OP-TEE
- General solution
- **Overview of Widevine**

Widevine

- CDM (content decryption module) for Android
- Specifics are for partners only
- Plugin based, we implement oemcrypto.so using our client lib and TA

Status

- Working on HiKey board
- OP-TEE available for Android AOSP
- We have a liboemcrypto.so and TA for Widevine CDM
- Several security things missing
  - No trusted boot chain, TEE could be modified (HiKey issue)
  - SMAF not yet supported (patches in progress)
    https://lkml.org/lkml/2016/9/7/133
  - No HW video playback, buffers still need to be visible to software (HiKey work in progress)

Thank You

#LAS16

For further information: www.linaro.org

LAS16 keynotes and videos on: connect.linaro.org