



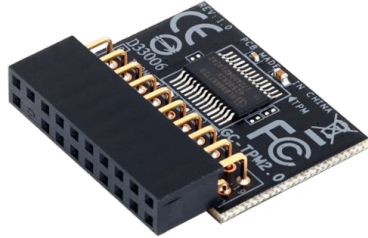
TPMs and the Linux Kernel

Unlocking a better path to hardware security

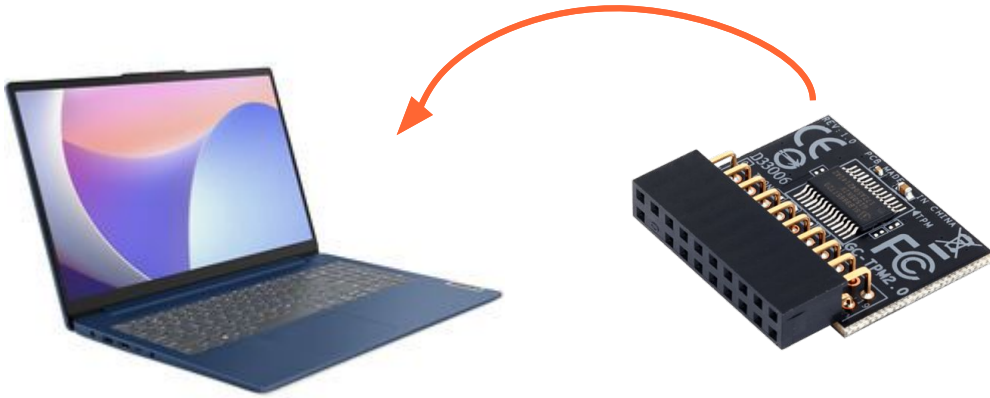
Ignat Korchagin
@ignatkn

What is a TPM?

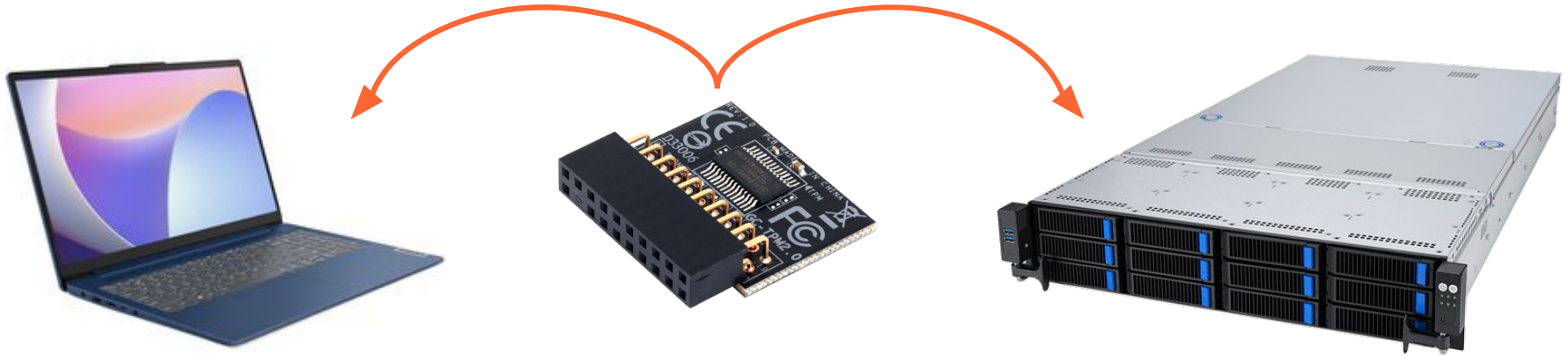
What is a TPM?



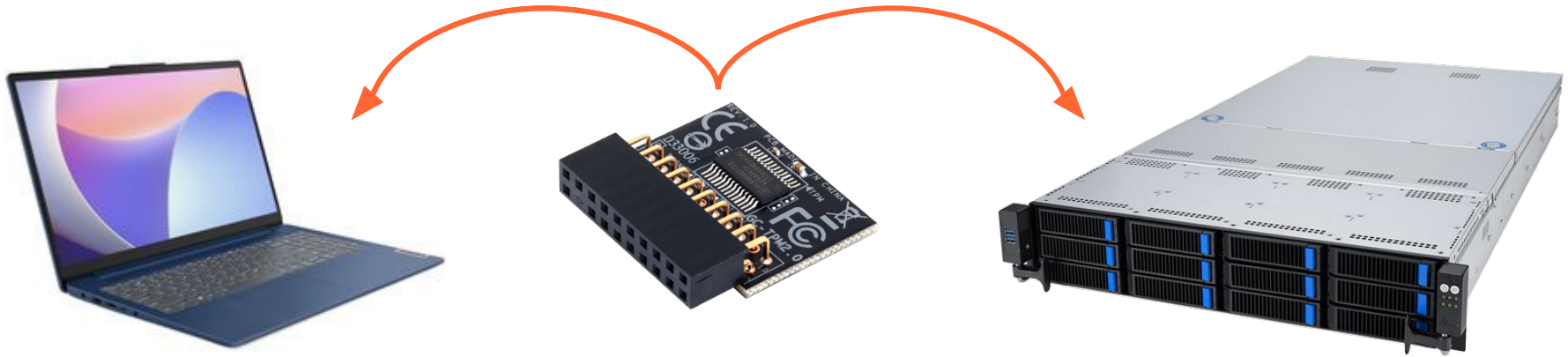
What is a TPM?



What is a TPM?



What is a TPM?



- A discrete security chip on modern laptops and servers
- Passive, non-intrusive: only responds to commands and performs cryptographic operations
- Foundation for platform integrity, authentication and remote attestation
- Can handle cryptographic keys

This talk is not about system integrity or attestation

Can TPM help me with my keys/secrets?

Why so little open source software has TPM support?

Application keys in the TPM



Application

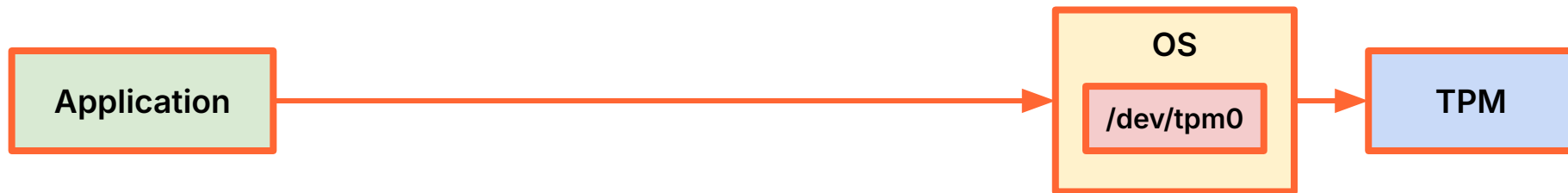


TPM

Application keys in the TPM



Application keys in the TPM



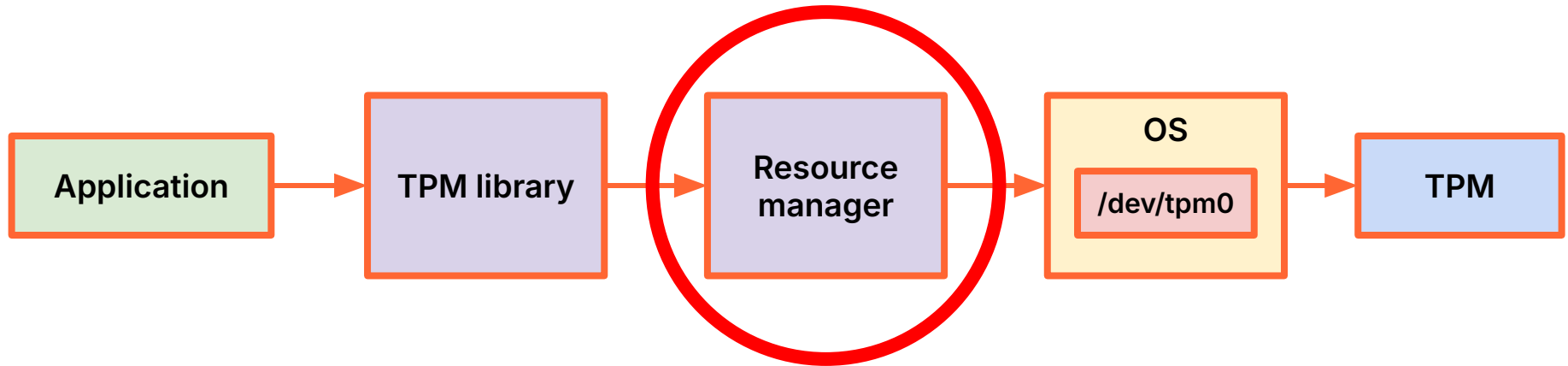
Application keys in the TPM



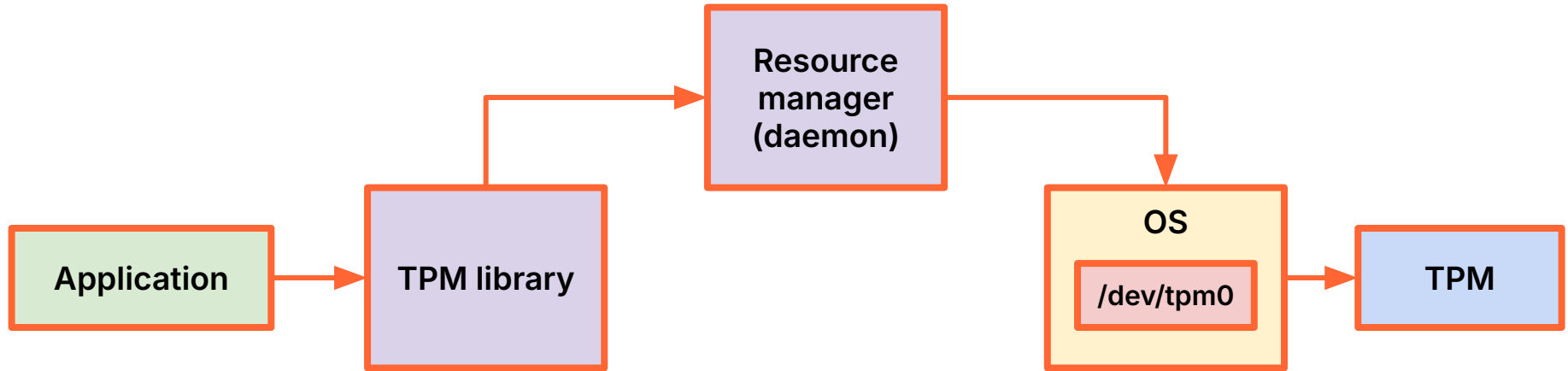
Application keys in the TPM



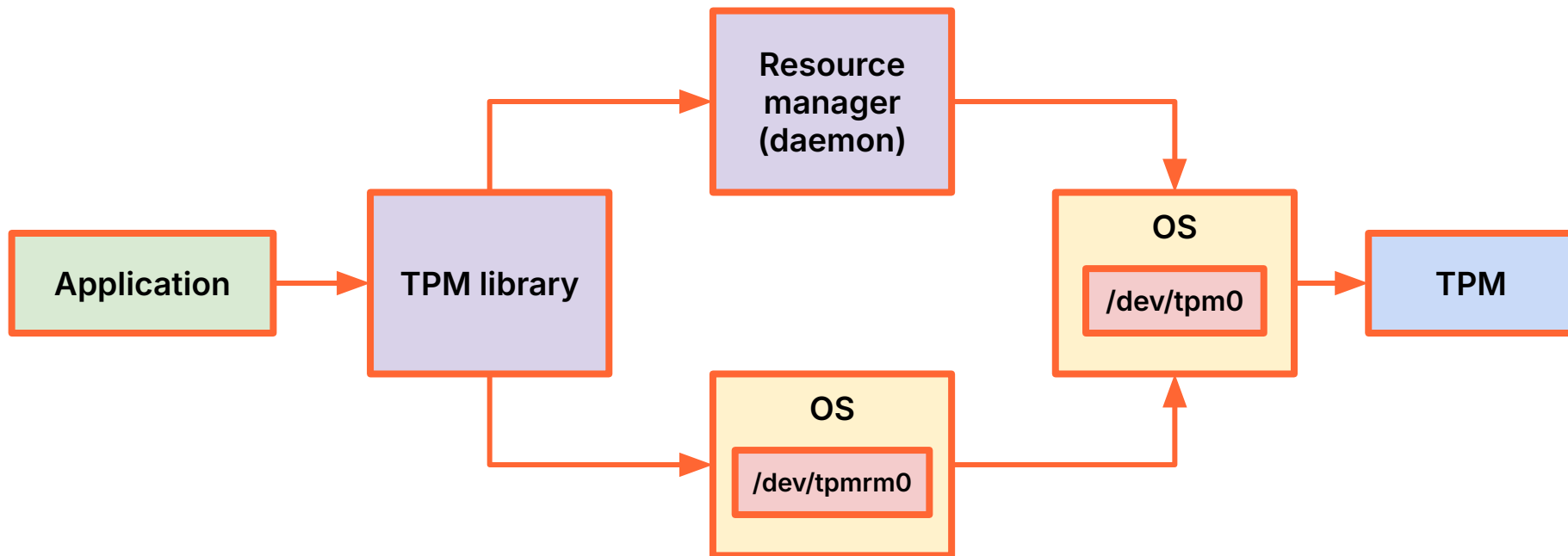
Application keys in the TPM



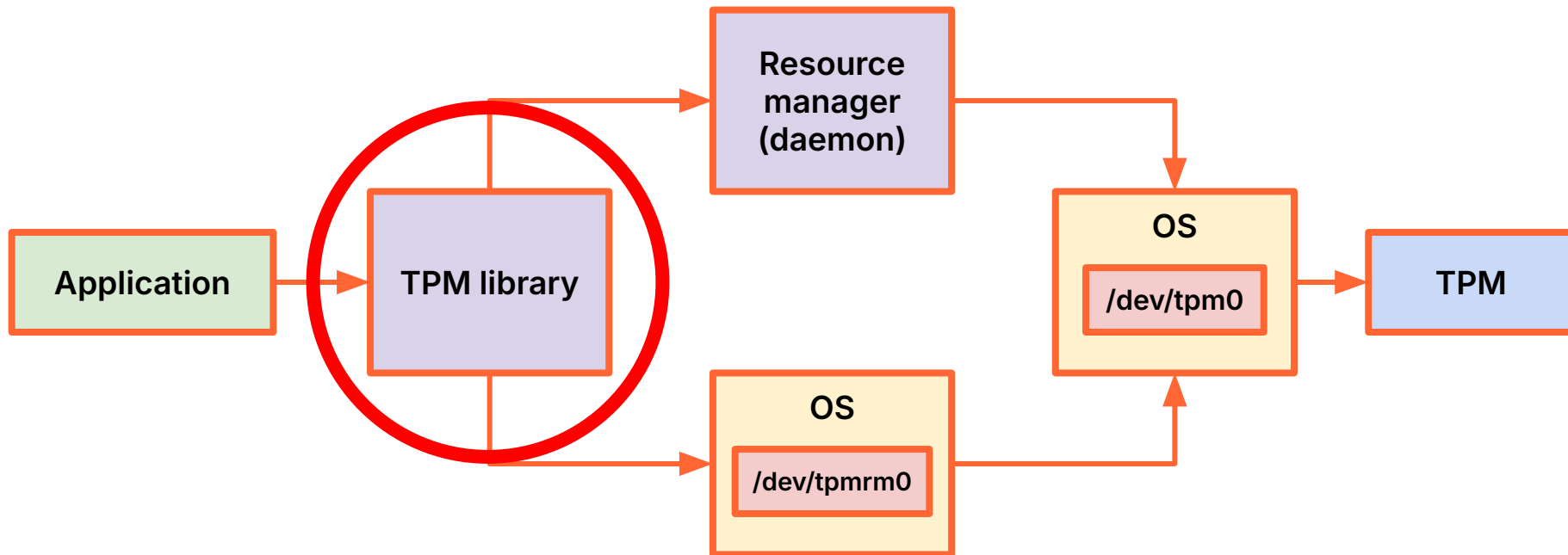
Application keys in the TPM



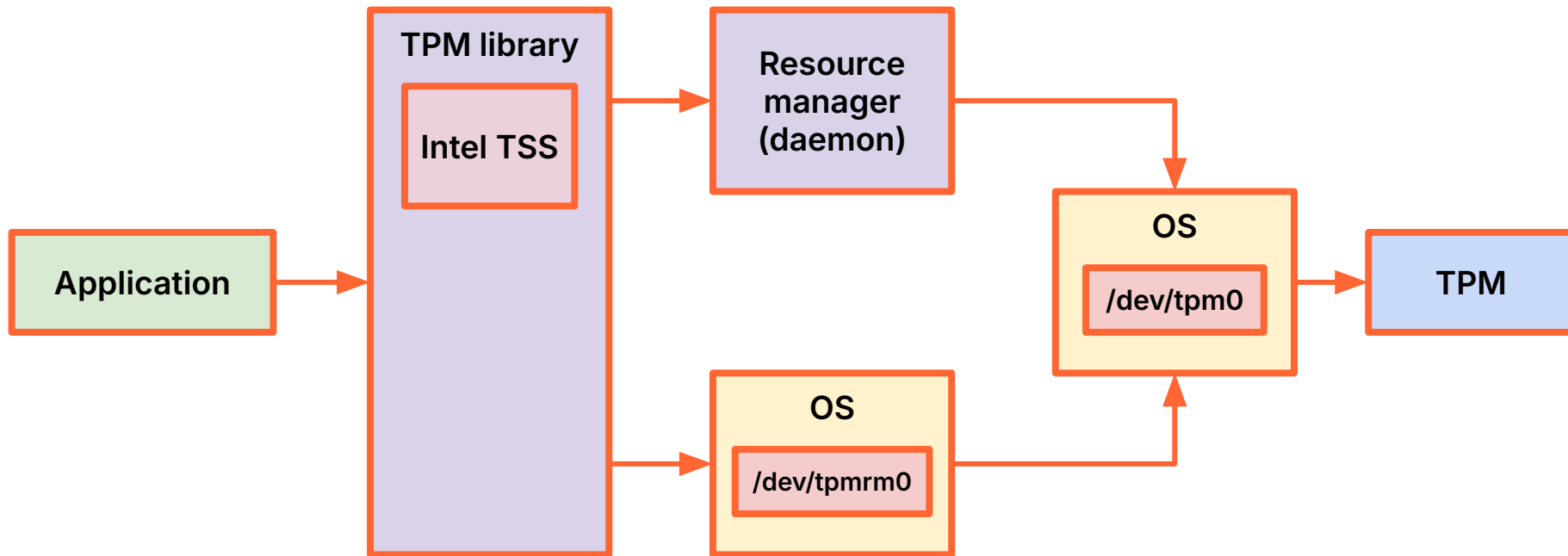
Application keys in the TPM



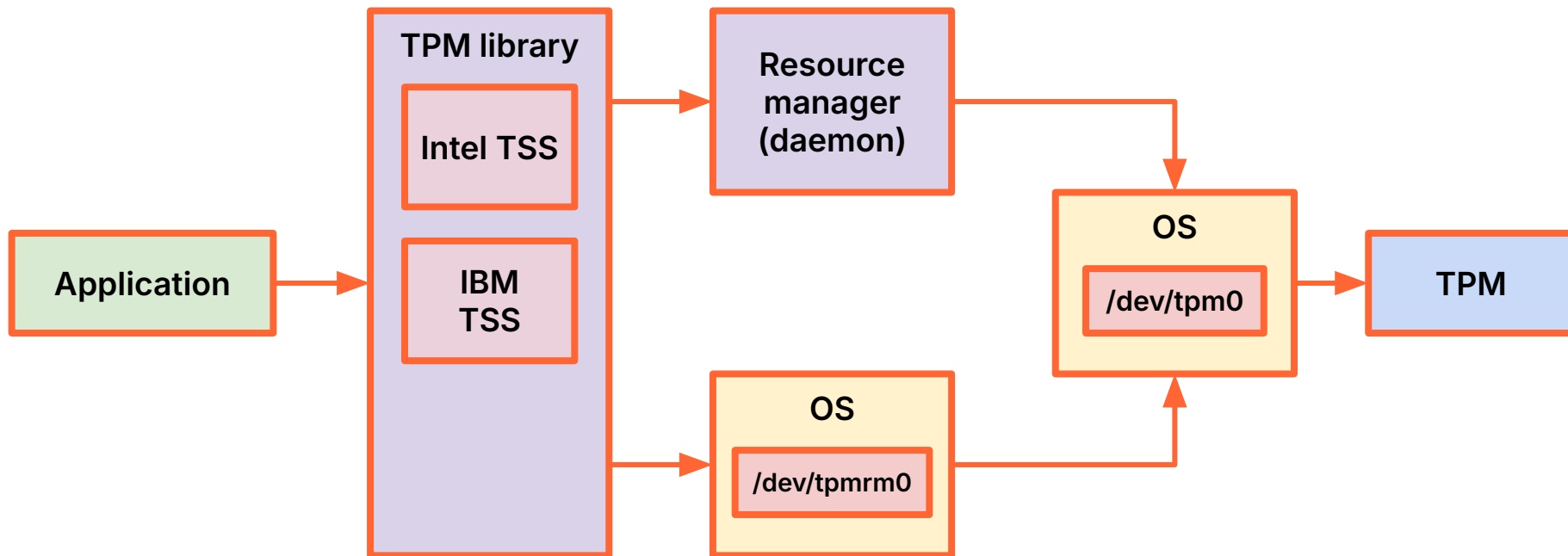
Application keys in the TPM



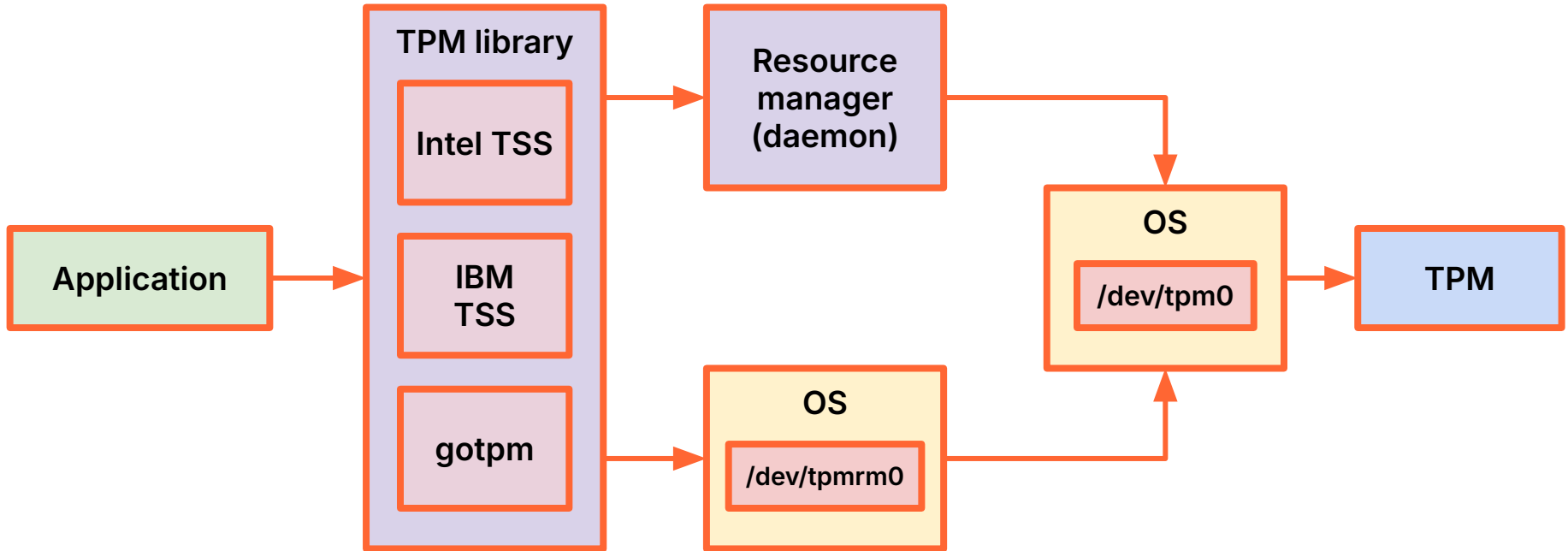
Application keys in the TPM



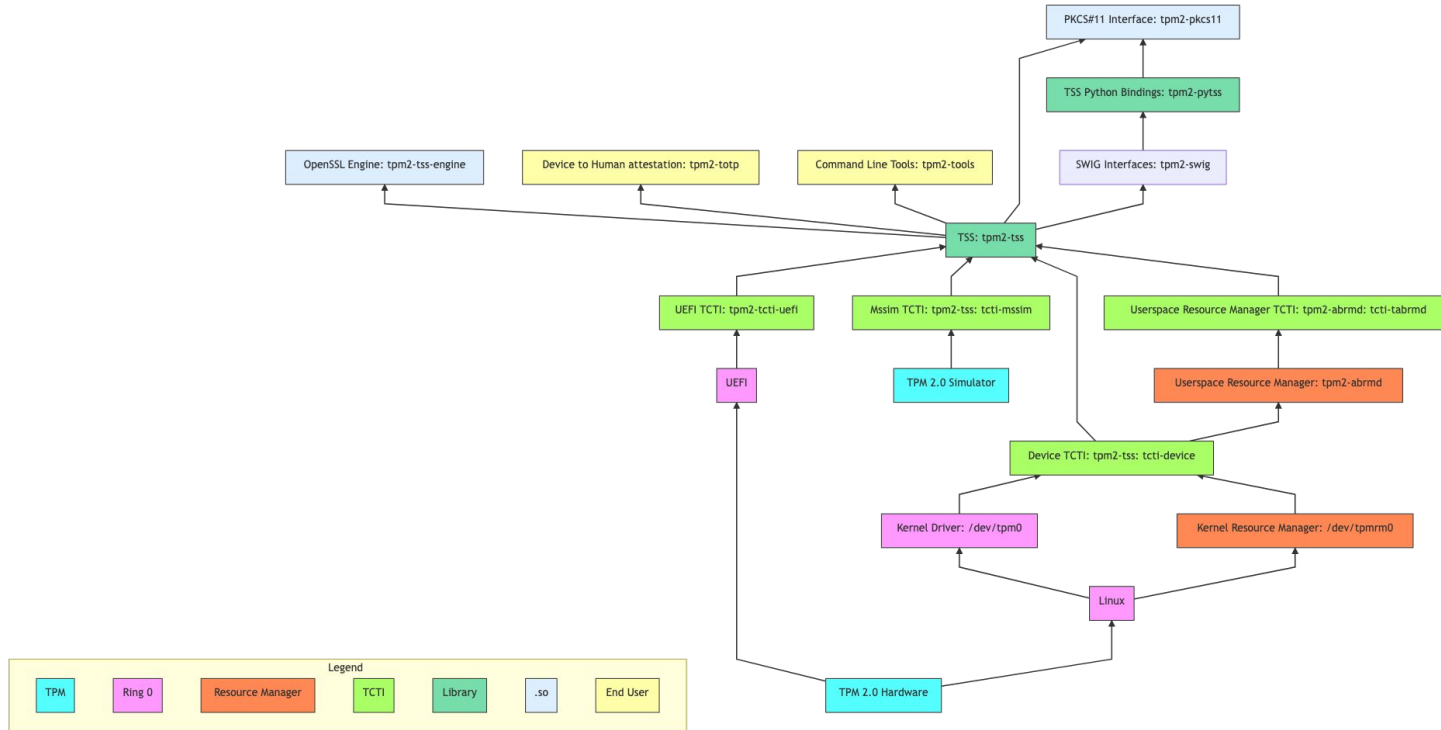
Application keys in the TPM



Application keys in the TPM



TPM2 software stack



<https://tpm2-software.github.io/>

Application keys in the TPM



Access permissions for the TPM

```
ignat@dev:~$ echo hello > /dev/tpmrm0  
-bash: /dev/tpmrm0: Permission denied
```

Access permissions for the TPM

```
ignat@dev:~$ echo hello > /dev/tpmrm0
-bash: /dev/tpmrm0: Permission denied
ignat@dev:~$ ls -l /dev/tpm0
crw----- 1 root root 10, 224 May 20 11:08 /dev/tpm0
```

Access permissions for the TPM

```
ignat@dev:~$ echo hello > /dev/tpmrm0
-bash: /dev/tpmrm0: Permission denied
ignat@dev:~$ ls -l /dev/tpm0
crw----- 1 root root 10, 224 May 20 11:08 /dev/tpm0
ignat@dev:~$ ls -l /dev/tpmrm0
crw----- 1 root root 254, 65536 May 20 11:08 /dev/tpmrm0
```

Access permissions for the TPM

```
ignat@dev:~$ echo hello > /dev/tpmrm0
-bash: /dev/tpmrm0: Permission denied
ignat@dev:~$ ls -l /dev/tpm0
crw----- 1 root root 10, 224 May 20 11:08 /dev/tpm0
ignat@dev:~$ ls -l /dev/tpmrm0
crw----- 1 root root 254, 65536 May 20 11:08 /dev/tpmrm0
ignat@dev:~$ sudo apt-get install tpm2-tools
...
```

Access permissions for the TPM

```
ignat@dev:~$ echo hello > /dev/tpmrm0
-bash: /dev/tpmrm0: Permission denied
ignat@dev:~$ ls -l /dev/tpm0
crw----- 1 root root 10, 224 May 20 11:08 /dev/tpm0
ignat@dev:~$ ls -l /dev/tpmrm0
crw----- 1 root root 254, 65536 May 20 11:08 /dev/tpmrm0
ignat@dev:~$ sudo apt-get install tpm2-tools
...
ignat@dev:~$ ls -l /dev/tpm0
crw-rw---- 1 tss root 10, 224 May 20 13:25 /dev/tpm0
```

Access permissions for the TPM

```
ignat@dev:~$ echo hello > /dev/tpmrm0
-bash: /dev/tpmrm0: Permission denied
ignat@dev:~$ ls -l /dev/tpm0
crw----- 1 root root 10, 224 May 20 11:08 /dev/tpm0
ignat@dev:~$ ls -l /dev/tpmrm0
crw----- 1 root root 254, 65536 May 20 11:08 /dev/tpmrm0
ignat@dev:~$ sudo apt-get install tpm2-tools
...
ignat@dev:~$ ls -l /dev/tpm0
crw-rw---- 1 tss root 10, 224 May 20 13:25 /dev/tpm0
ignat@dev:~$ ls -l /dev/tpmrm0
crw-rw---- 1 tss tss 254, 65536 May 20 13:25 /dev/tpmrm0
```

Linux Kernel key retention service

AKA keyrings or keystore

Linux Kernel key retention service

Application

Application

Application

<https://www.kernel.org/doc/html/latest/security/keys/core.html>

Linux Kernel key retention service

Application

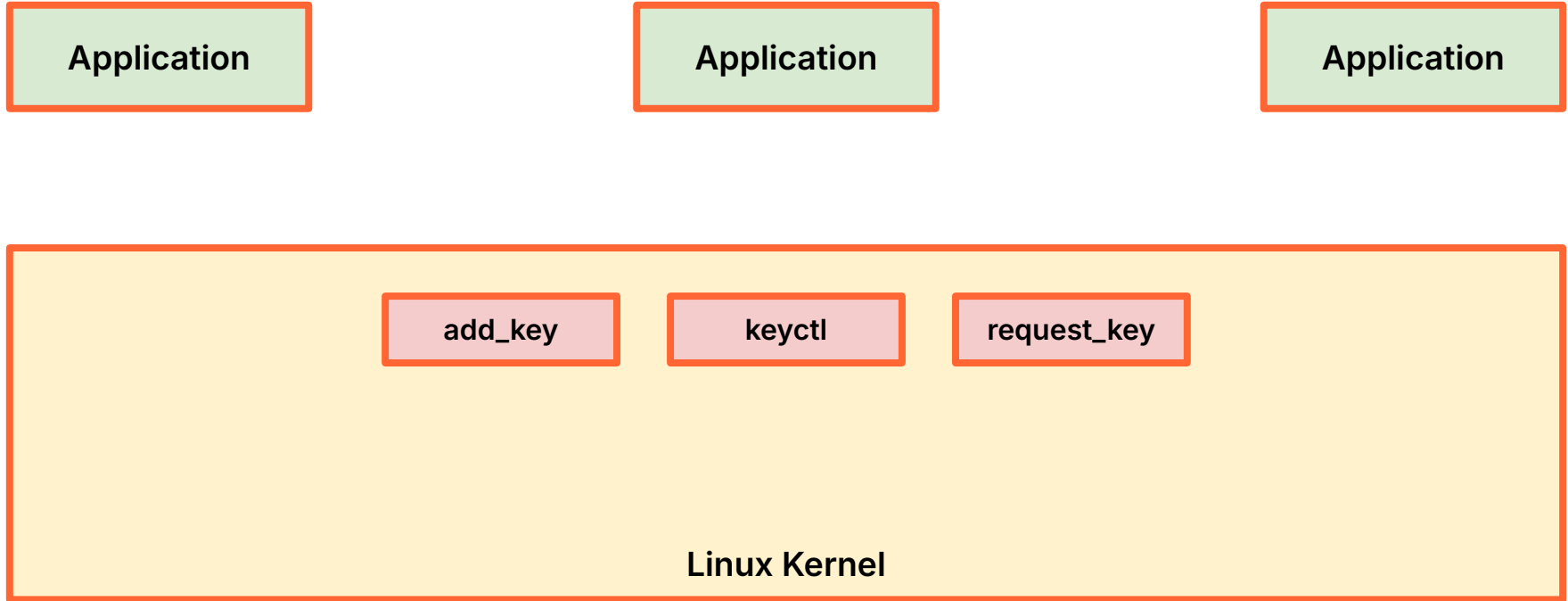
Application

Application

Linux Kernel

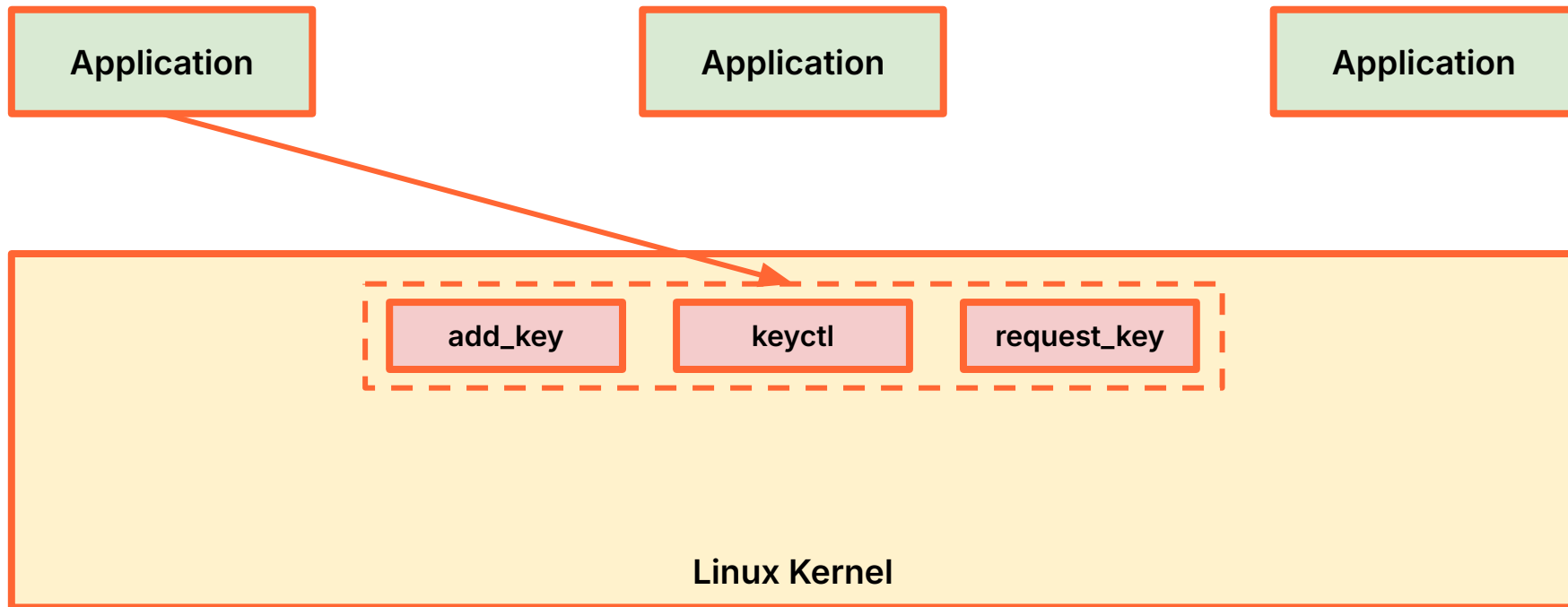
<https://www.kernel.org/doc/html/latest/security/keys/core.html>

Linux Kernel key retention service



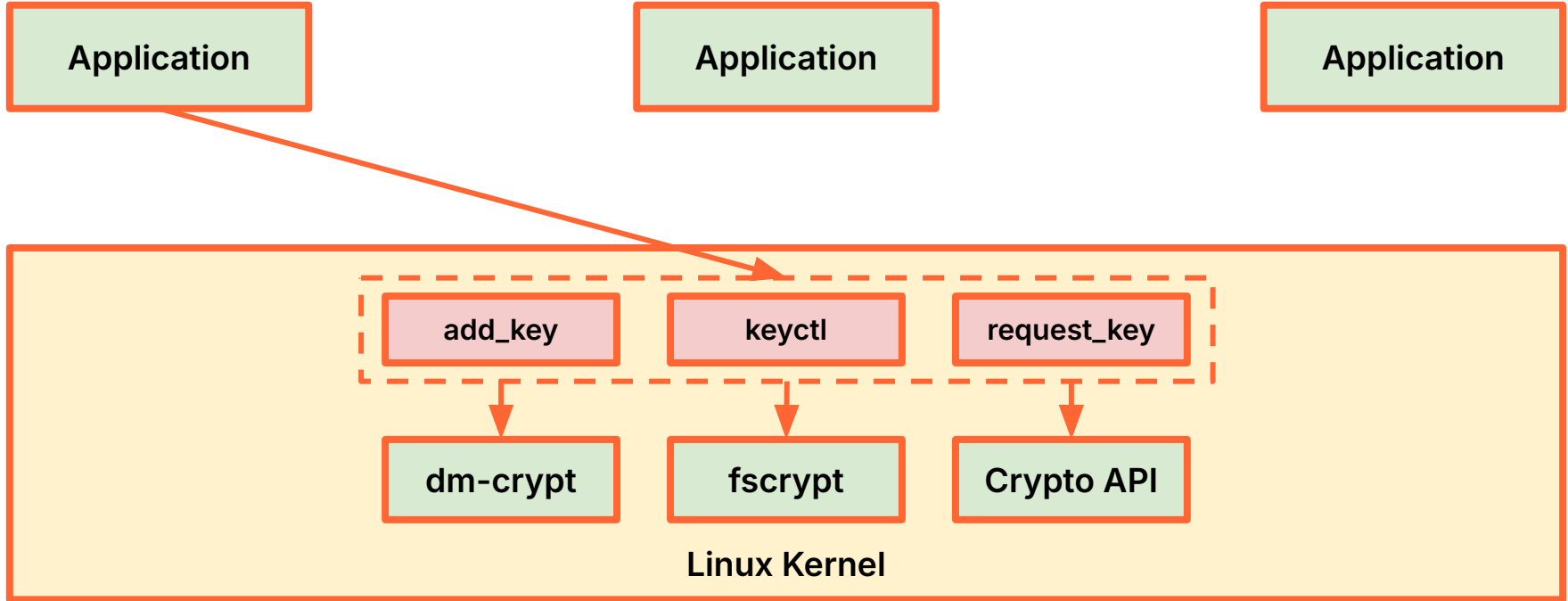
<https://www.kernel.org/doc/html/latest/security/keys/core.html>

Linux Kernel key retention service



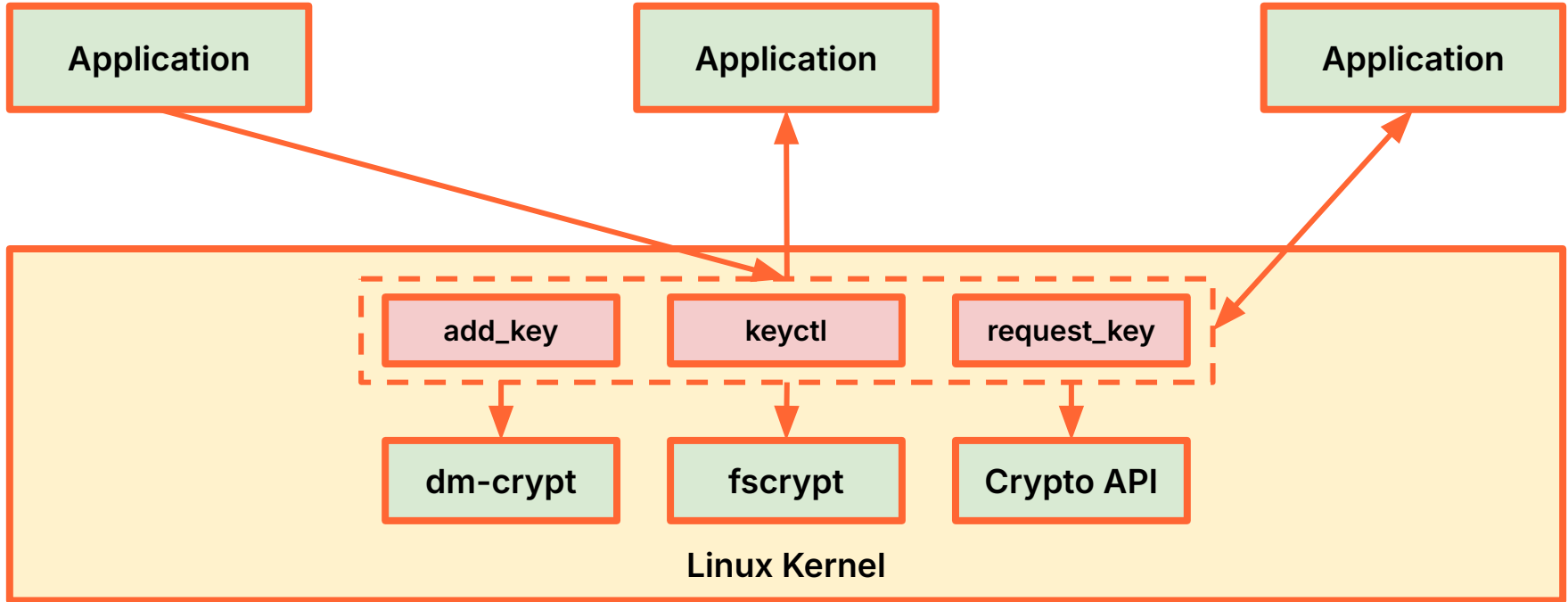
<https://www.kernel.org/doc/html/latest/security/keys/core.html>

Linux Kernel key retention service



<https://www.kernel.org/doc/html/latest/security/keys/core.html>

Linux Kernel key retention service

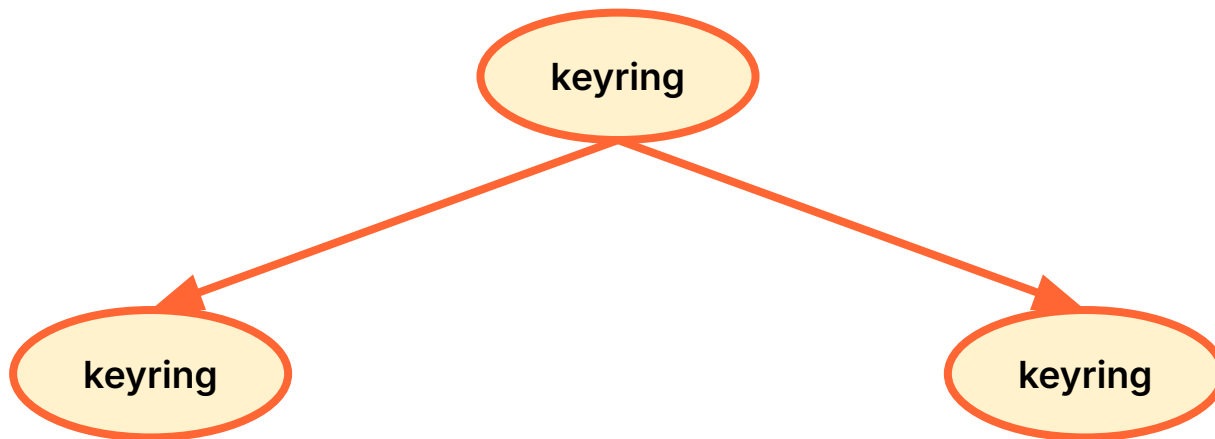


<https://www.kernel.org/doc/html/latest/security/keys/core.html>

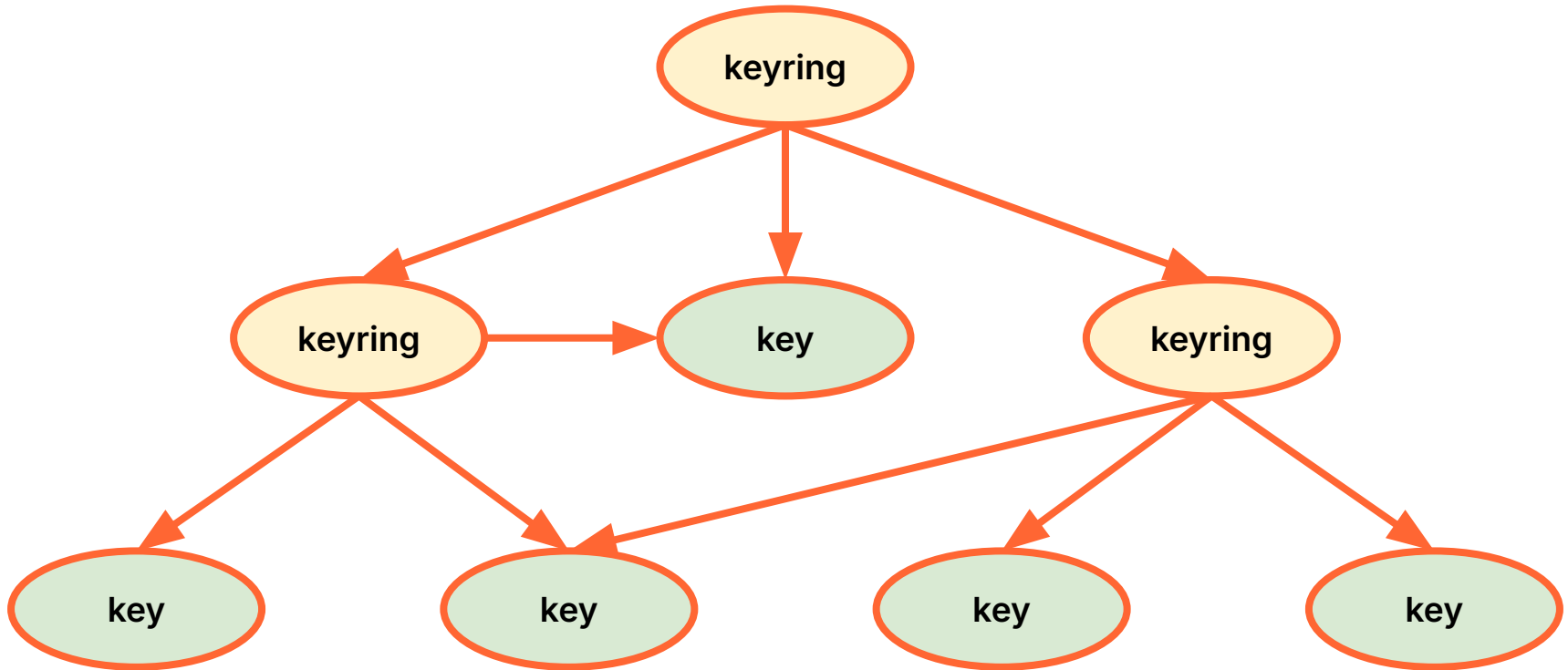
Keys and keyrings

keyring

Keys and keyrings



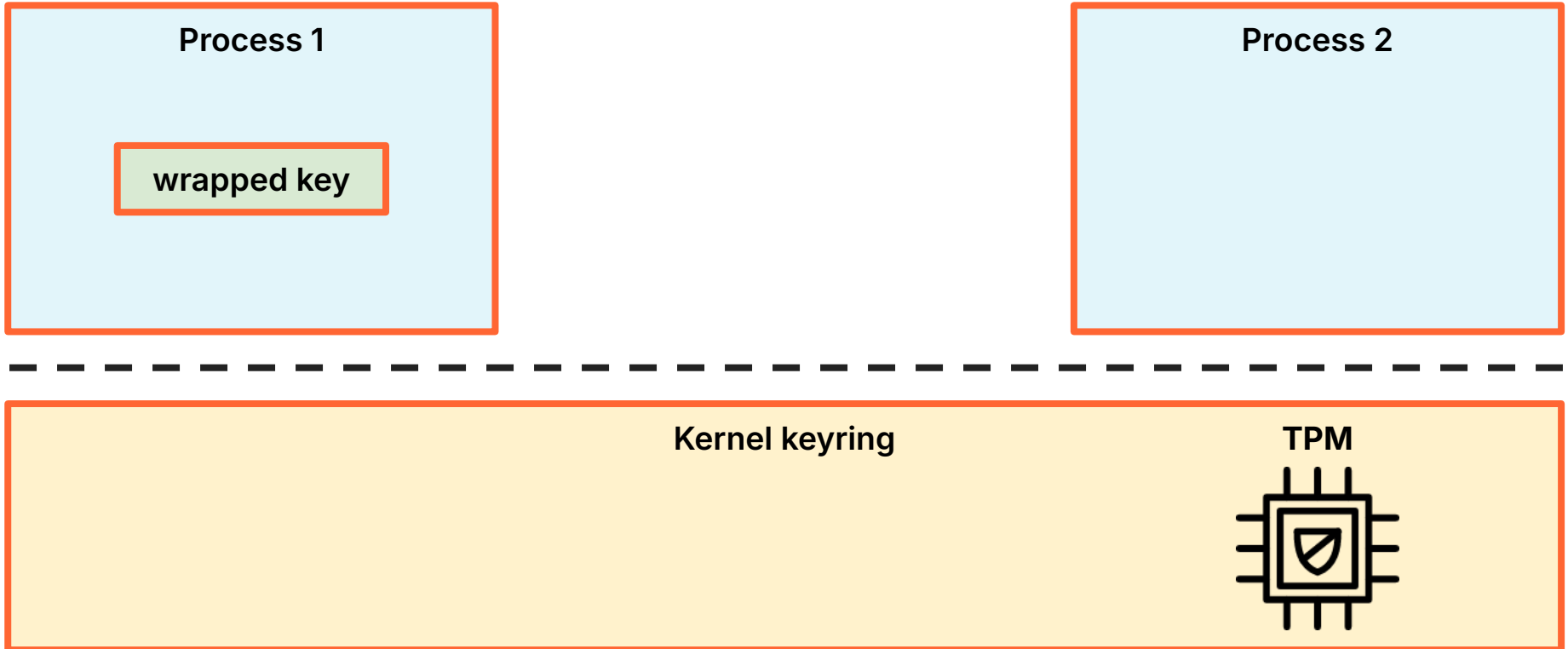
Keys and keyrings



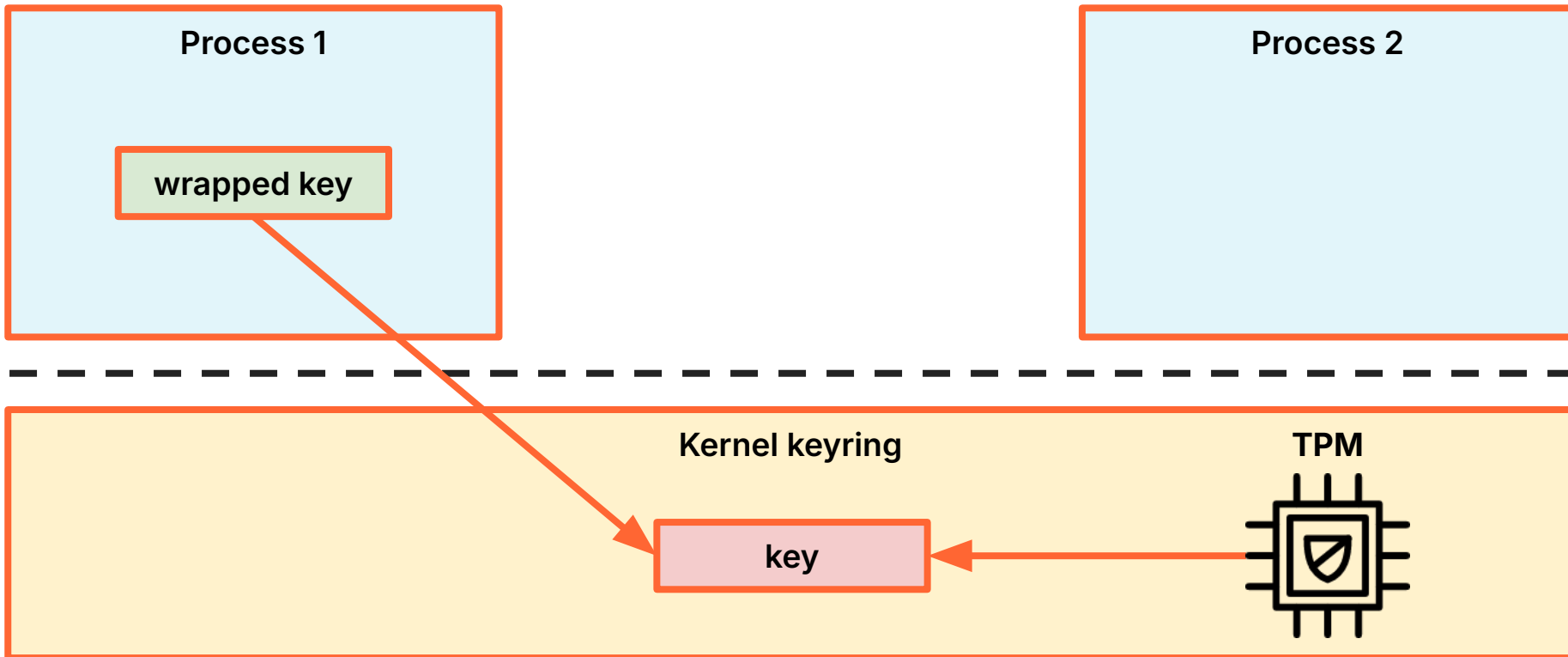
Linux keystore and TPMs

Better together?

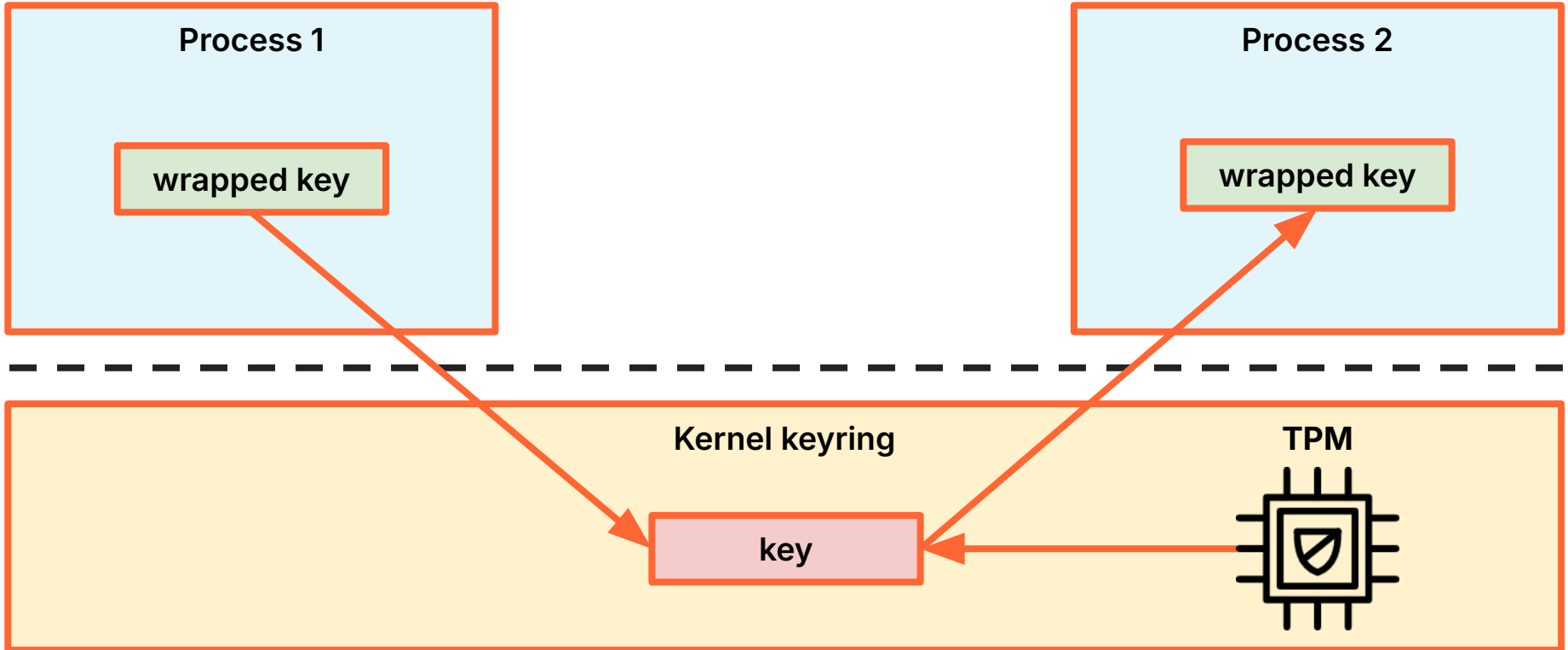
Trusted keys



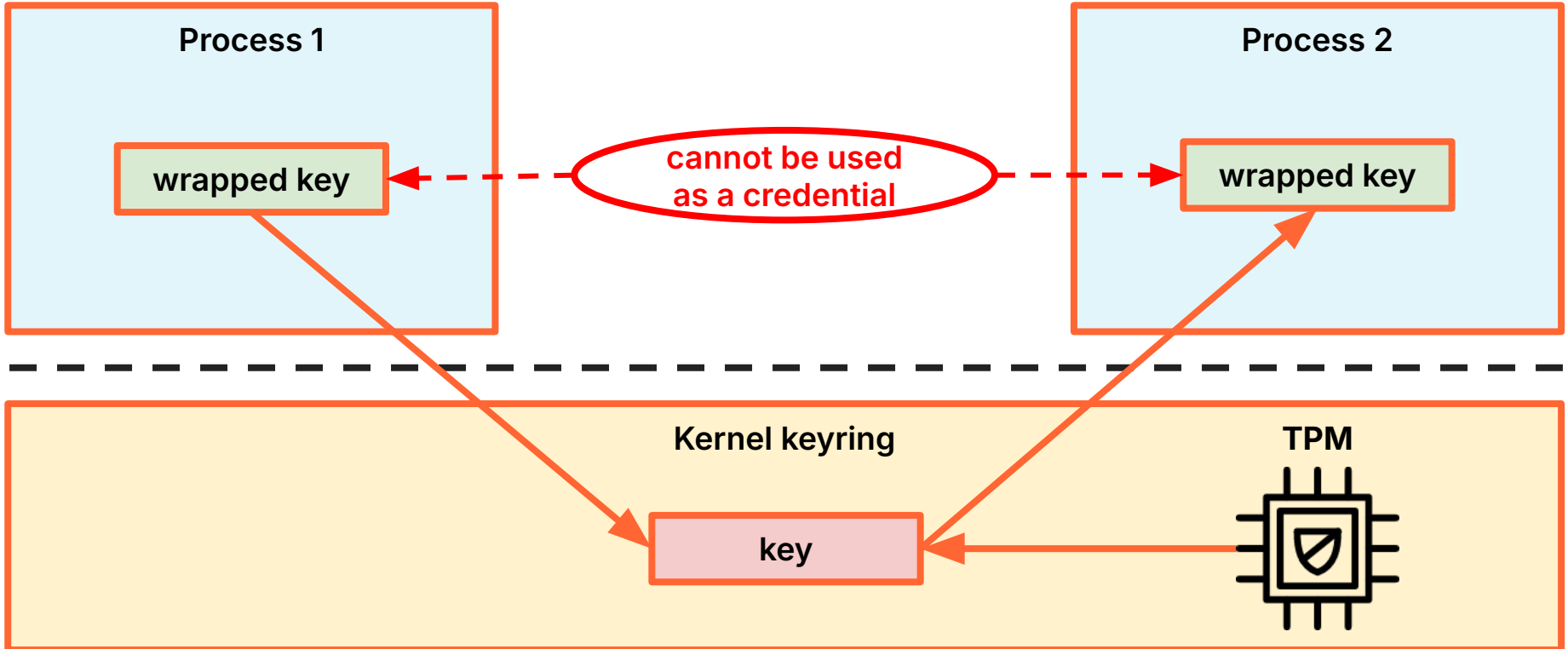
Trusted keys



Trusted keys



Trusted keys

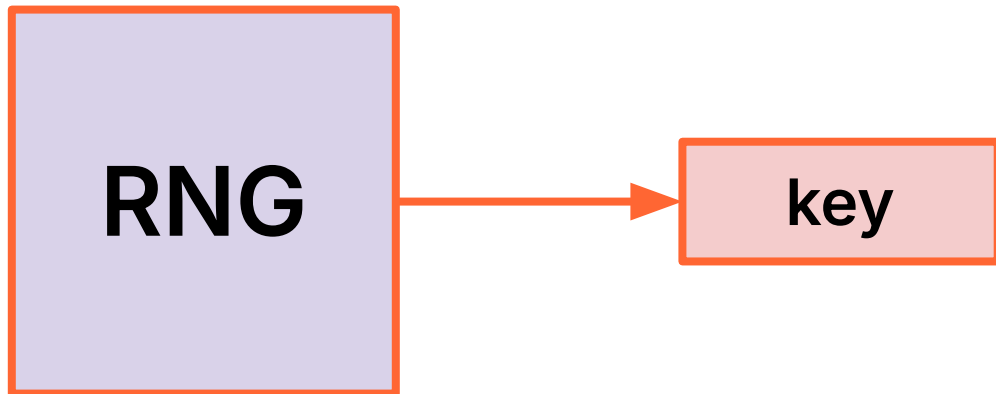


Wrapped keys



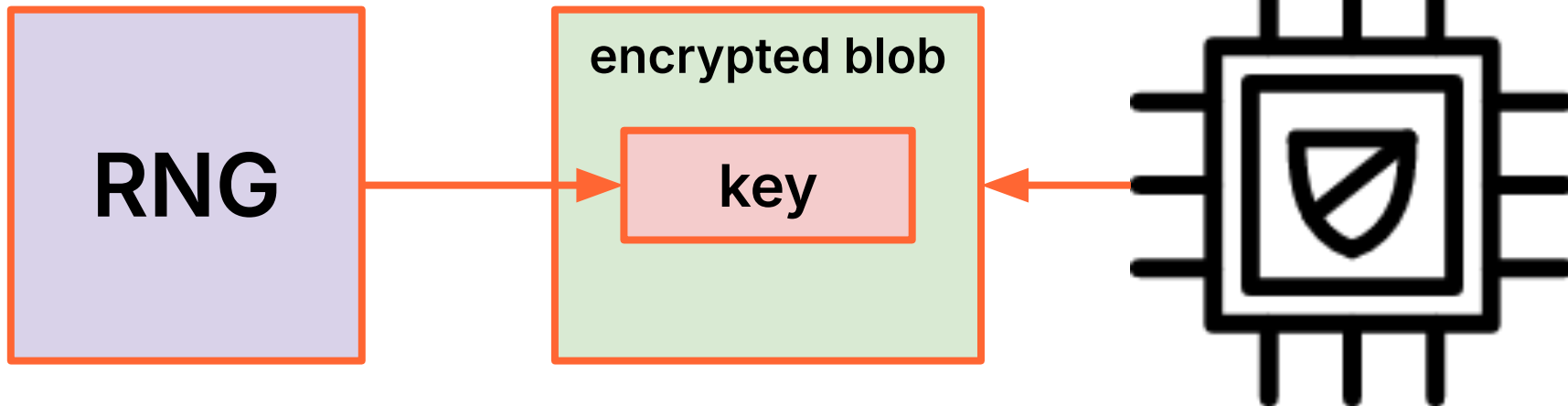
RNG

Wrapped keys

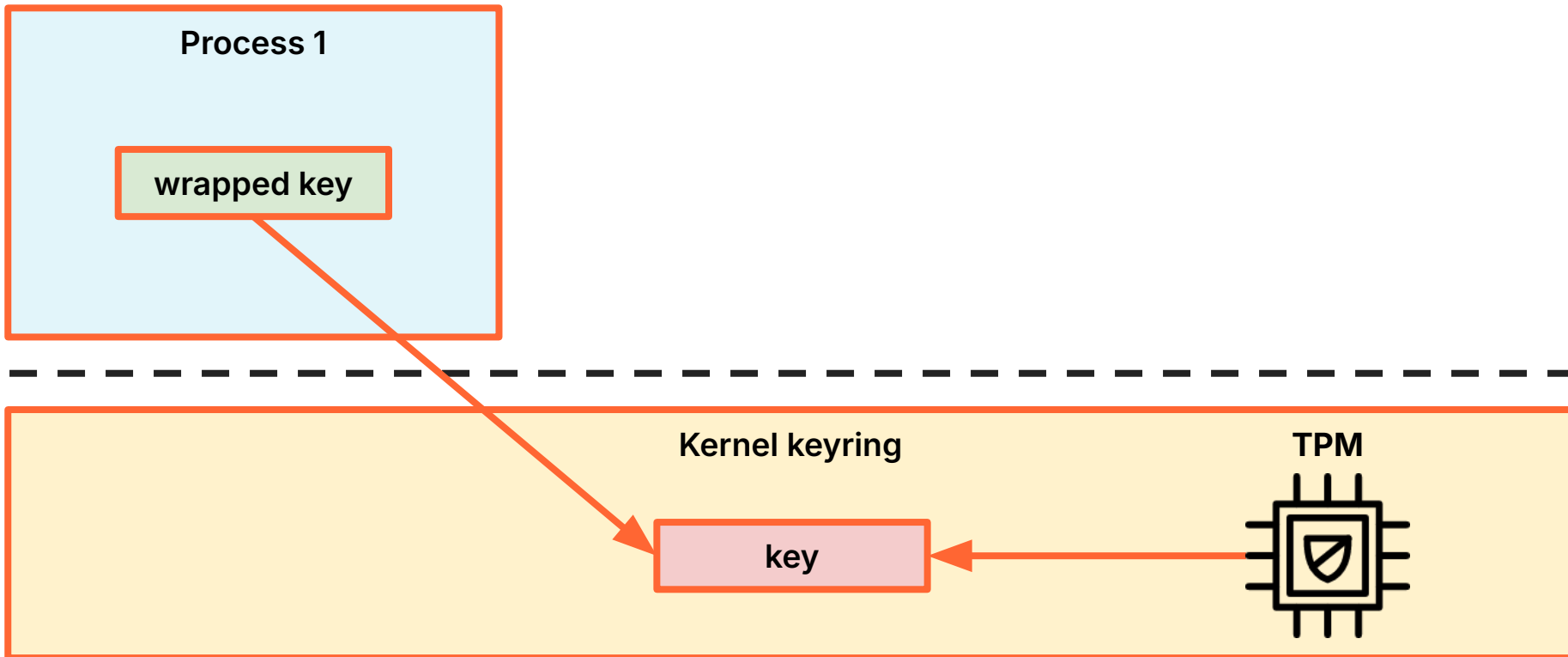


Wrapped keys

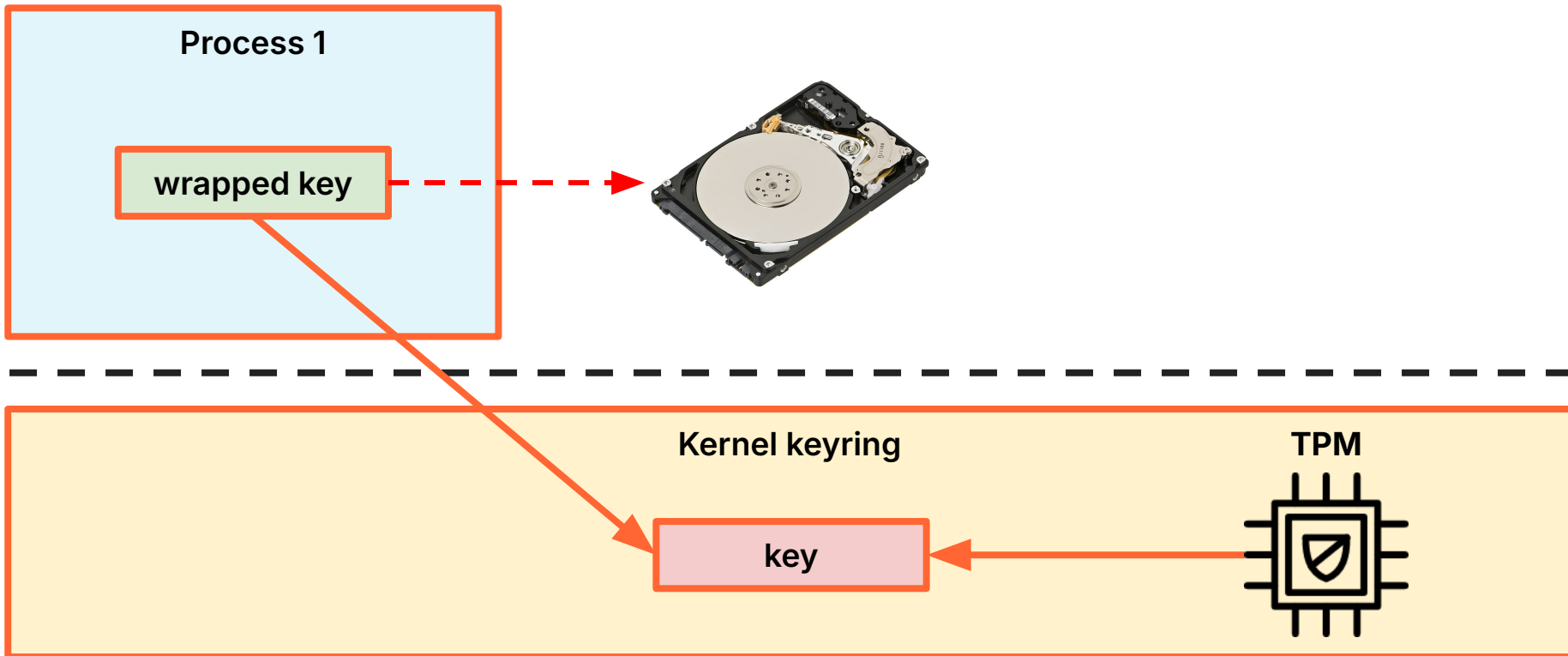
TPM



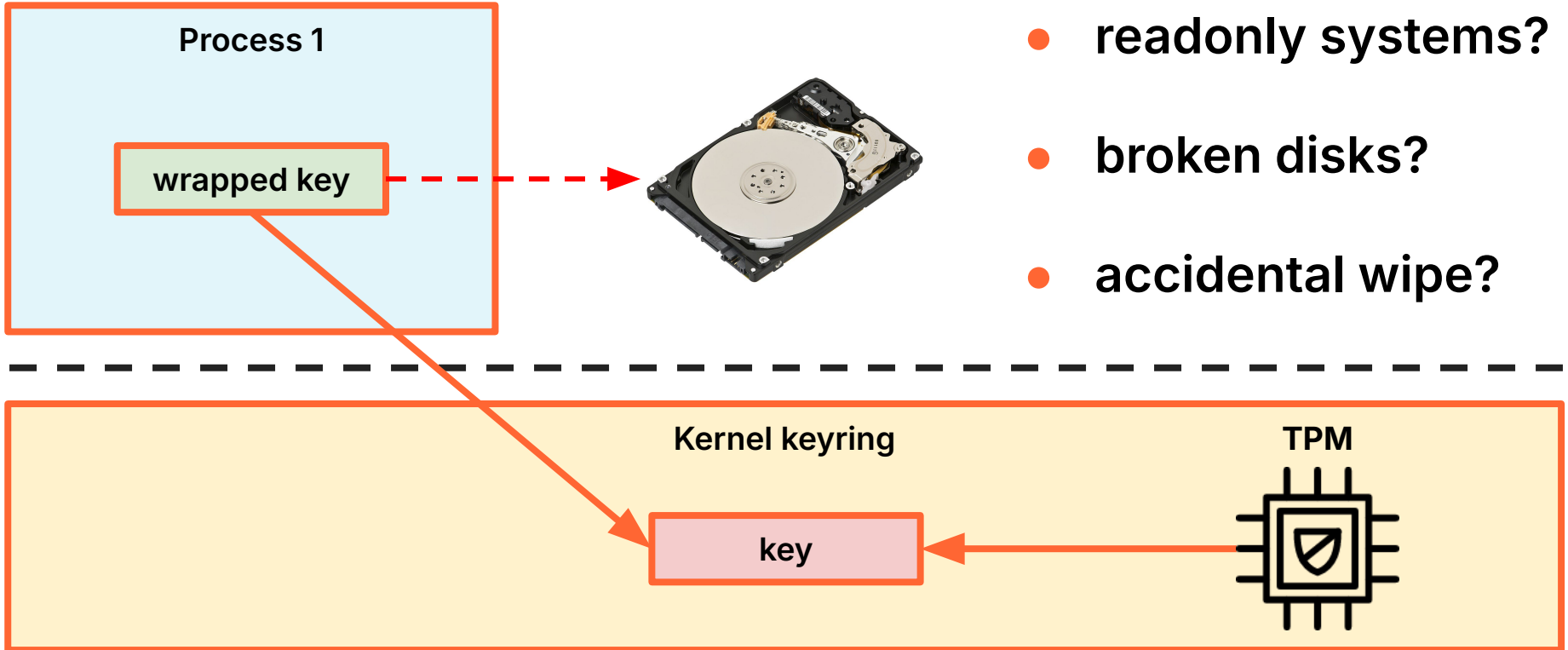
Trusted key management



Trusted key management



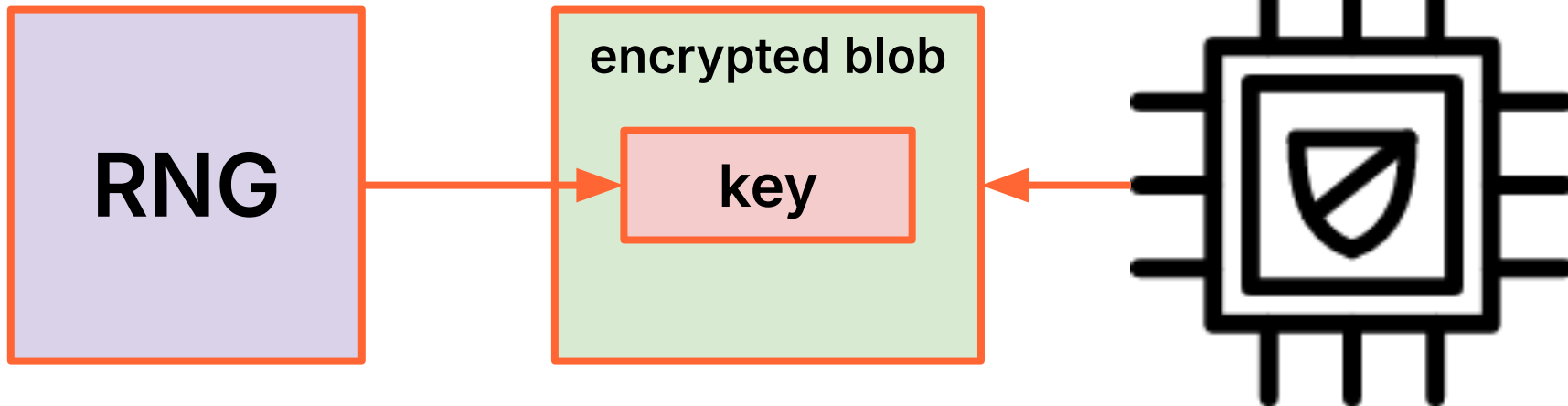
Trusted key management



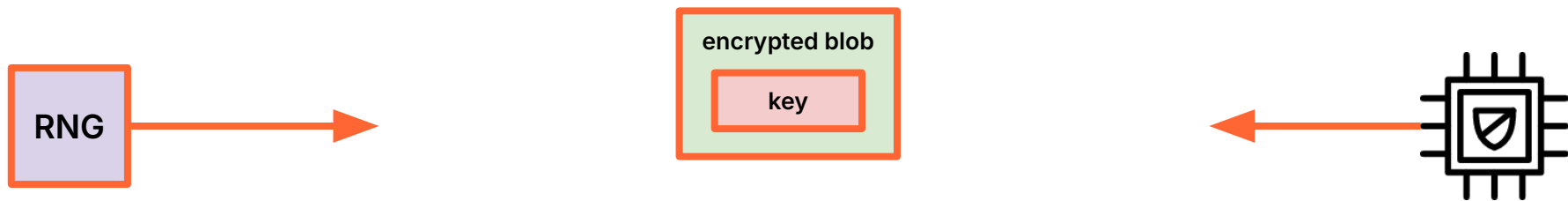
- **readonly systems?**
- **broken disks?**
- **accidental wipe?**

Wrapped keys

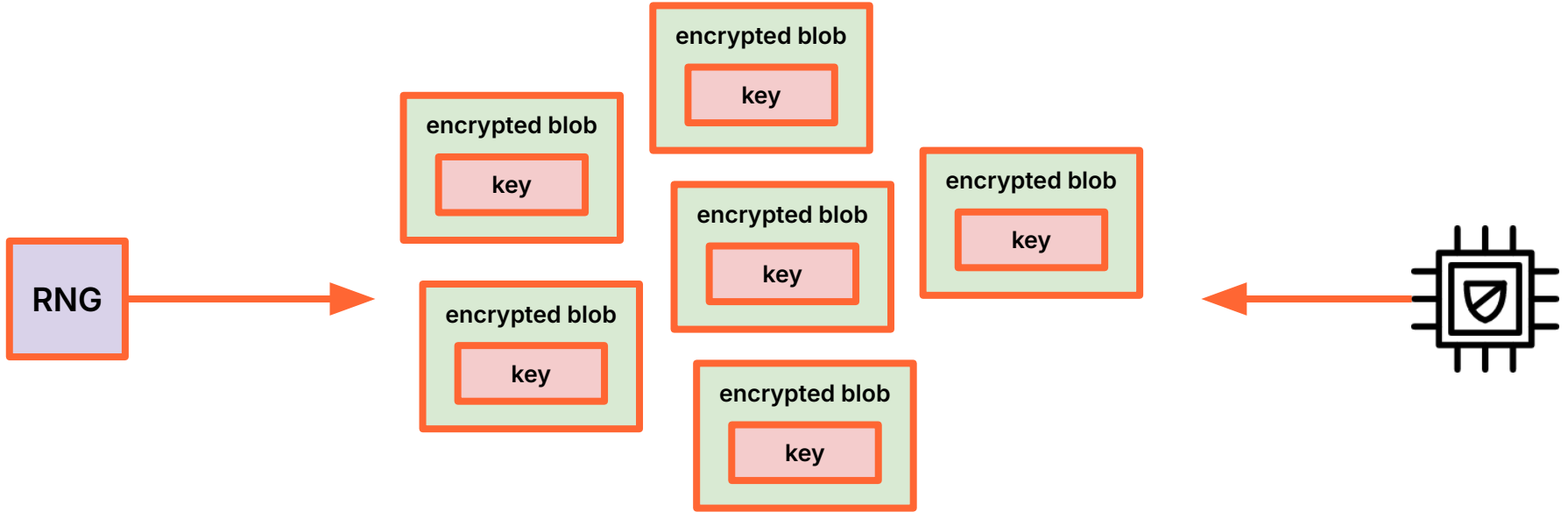
TPM



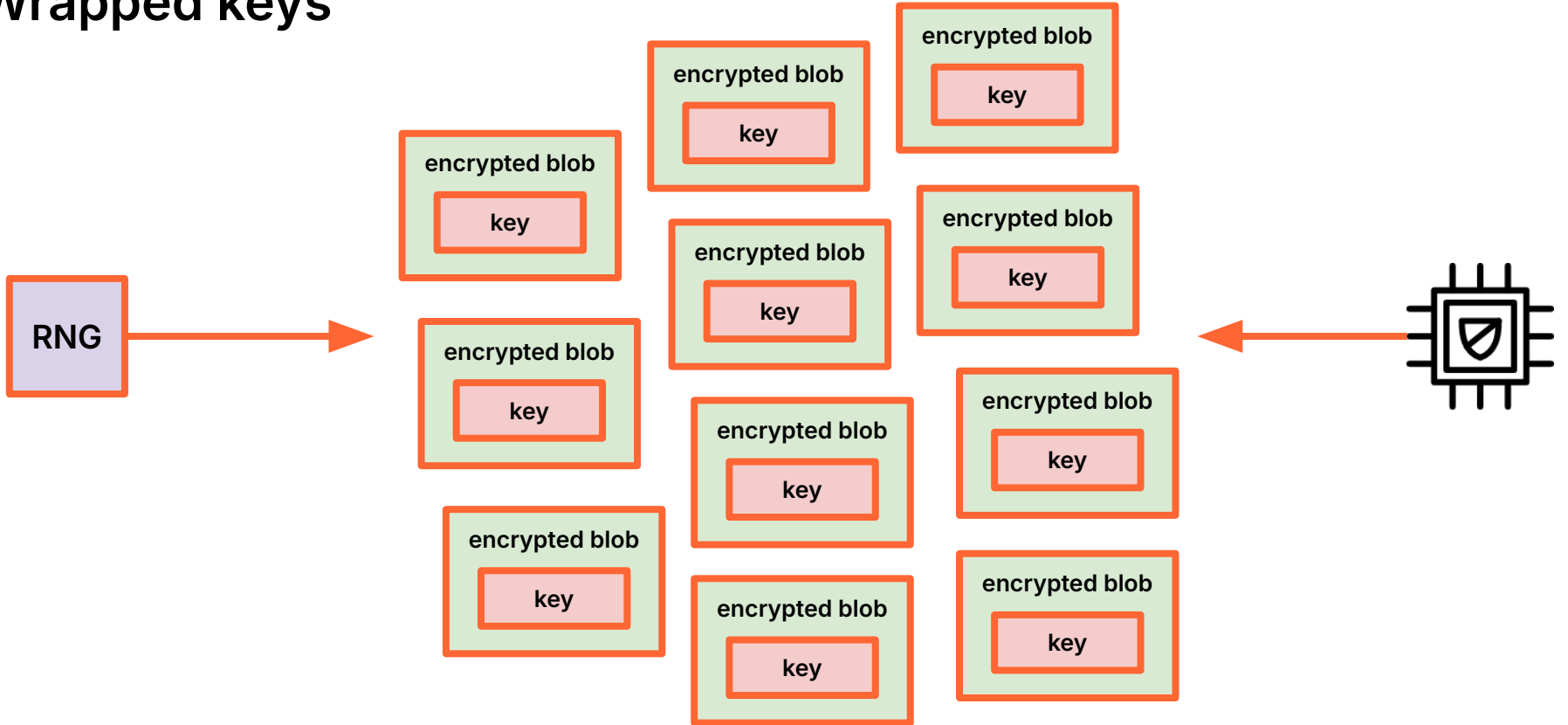
Wrapped keys



Wrapped keys

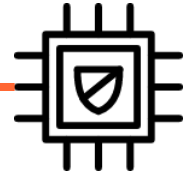
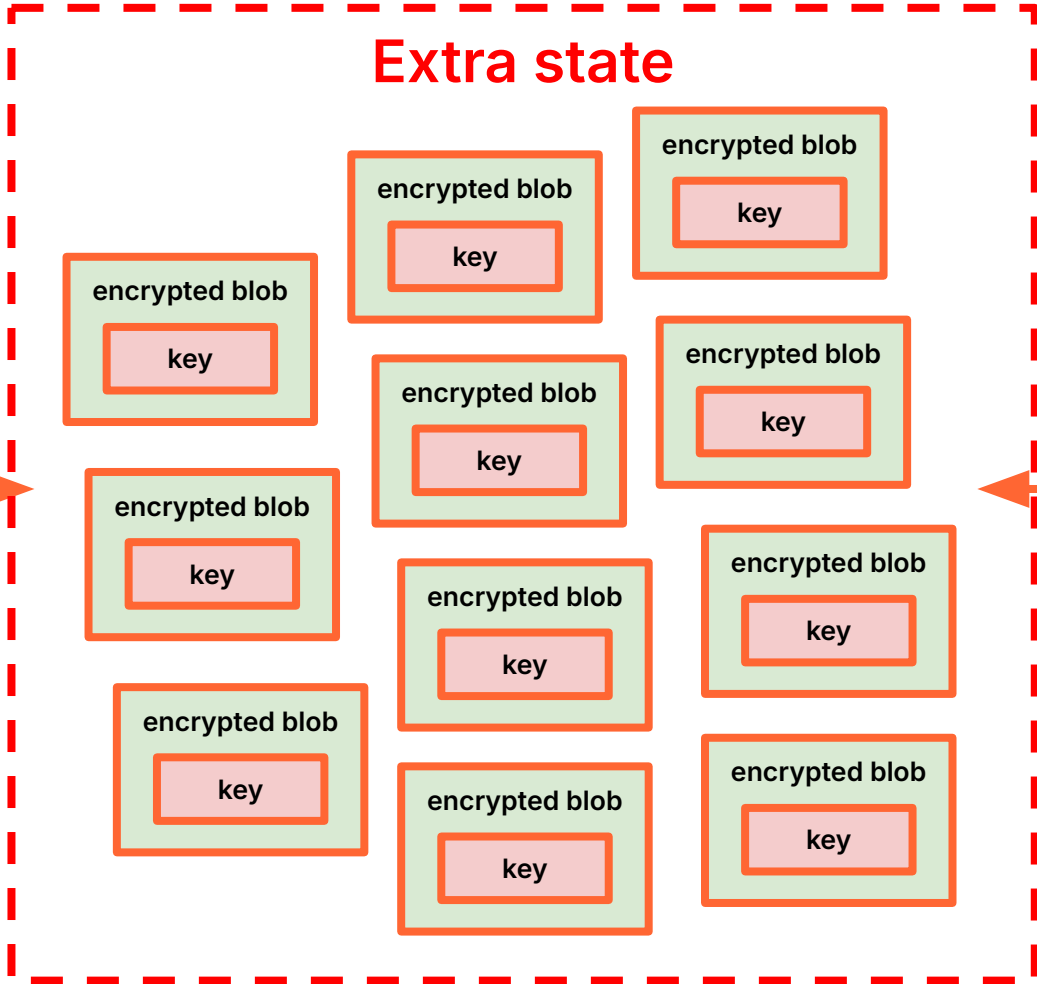


Wrapped keys



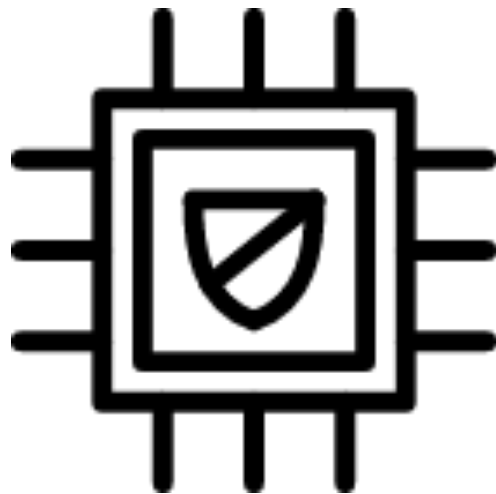
Wrapped keys

Extra state



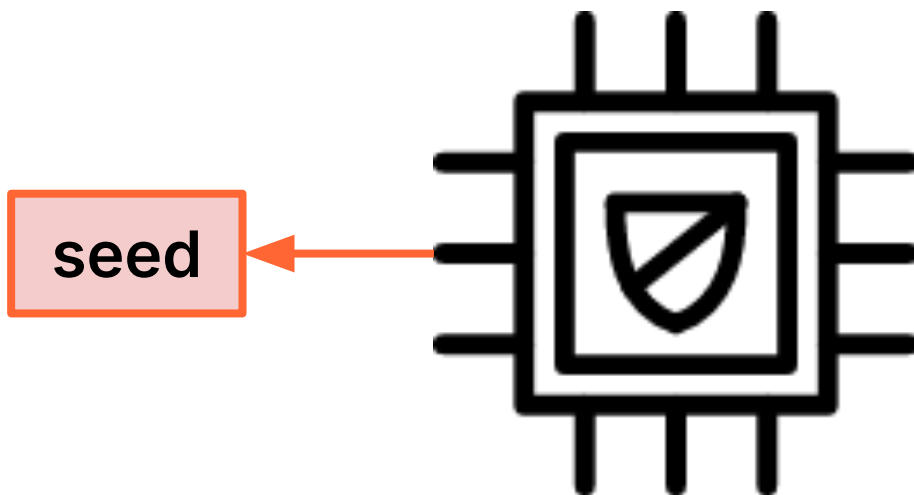
Derived keys

TPM

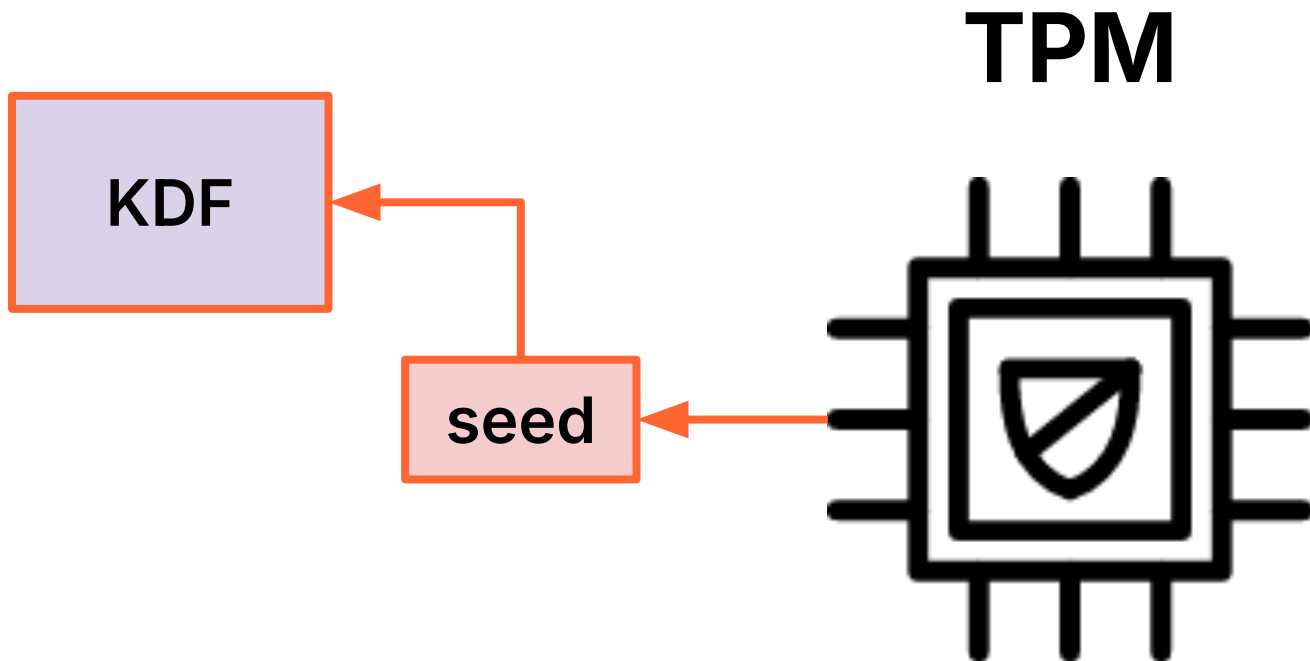


Derived keys

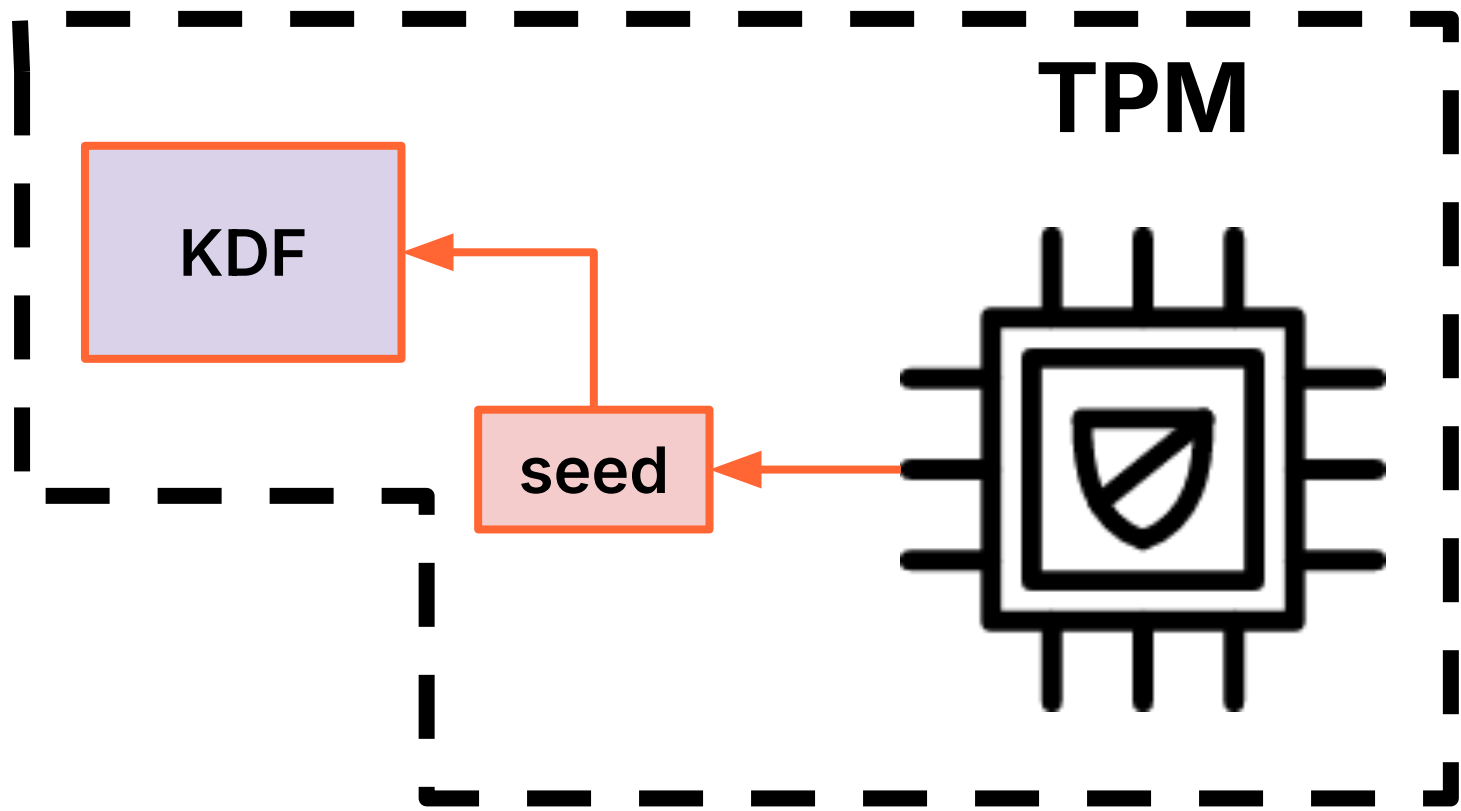
TPM



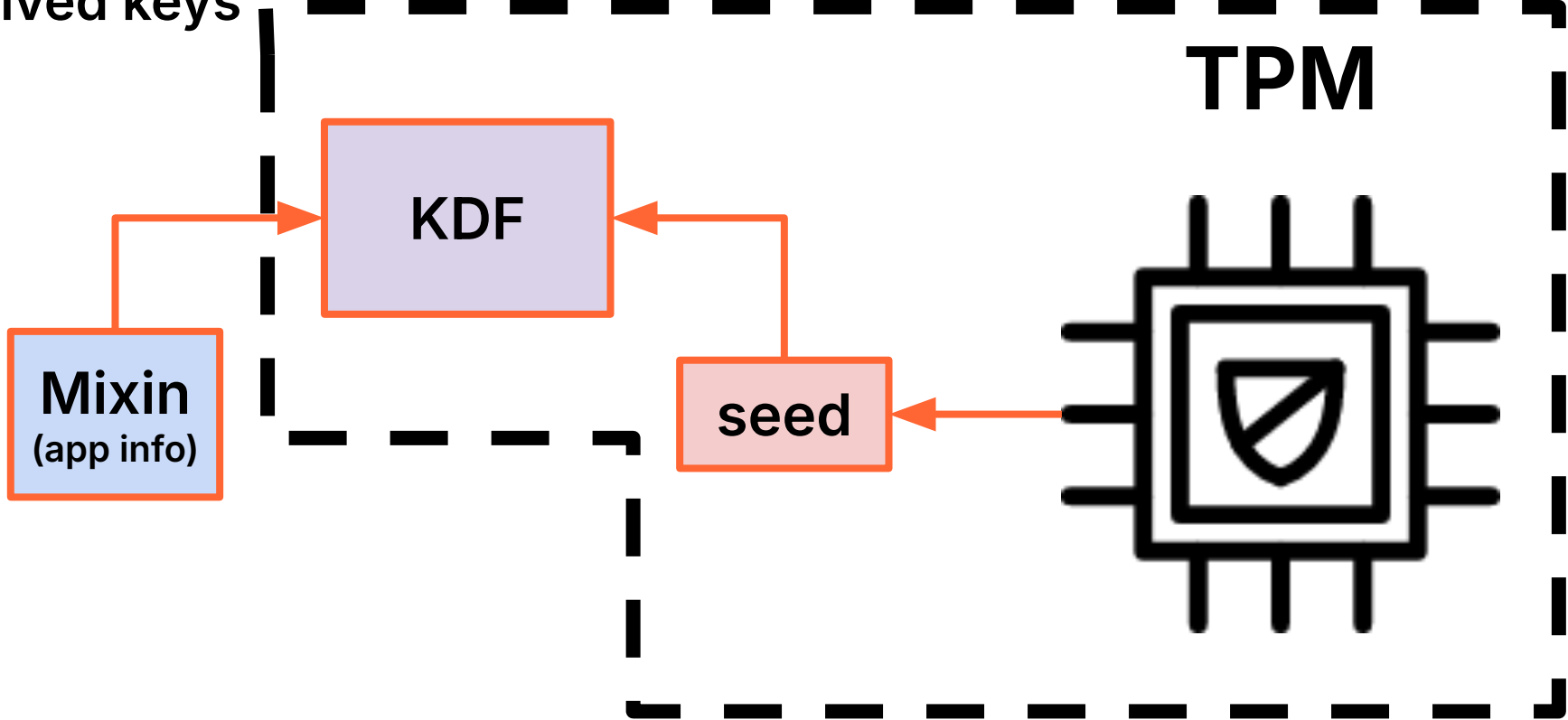
Derived keys



Derived keys

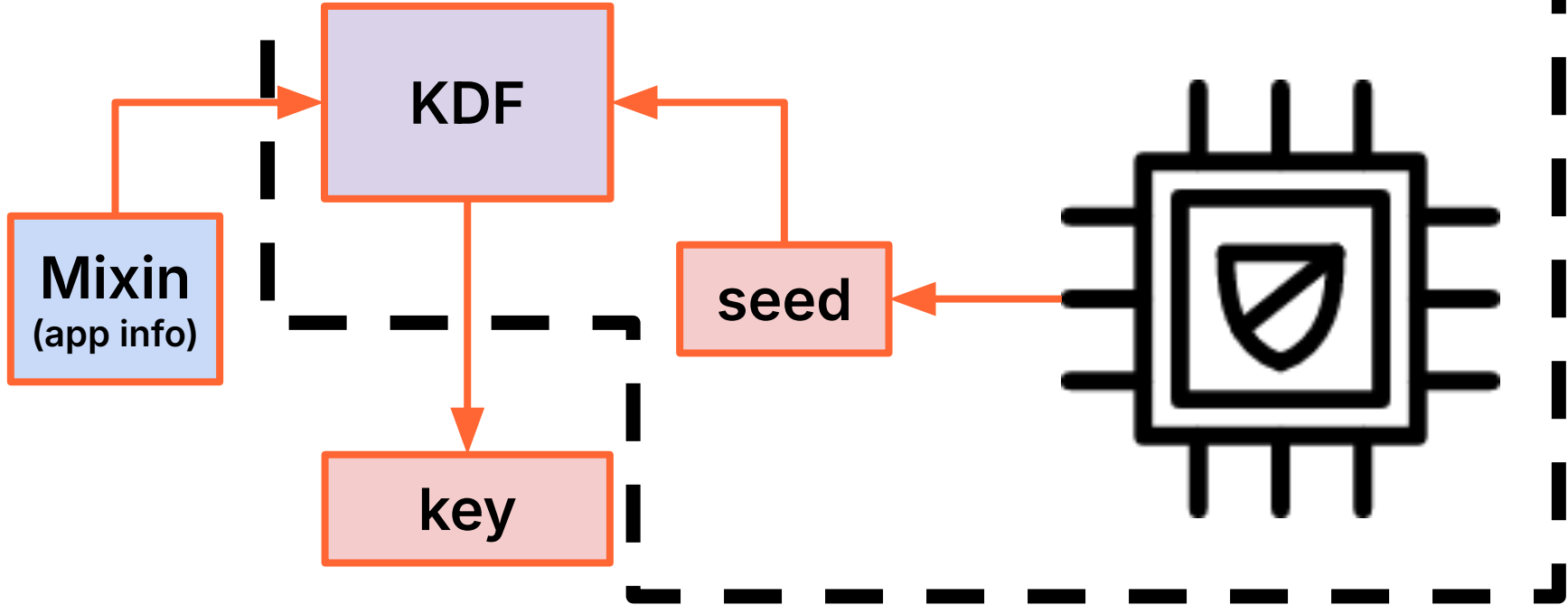


Derived keys



Derived keys

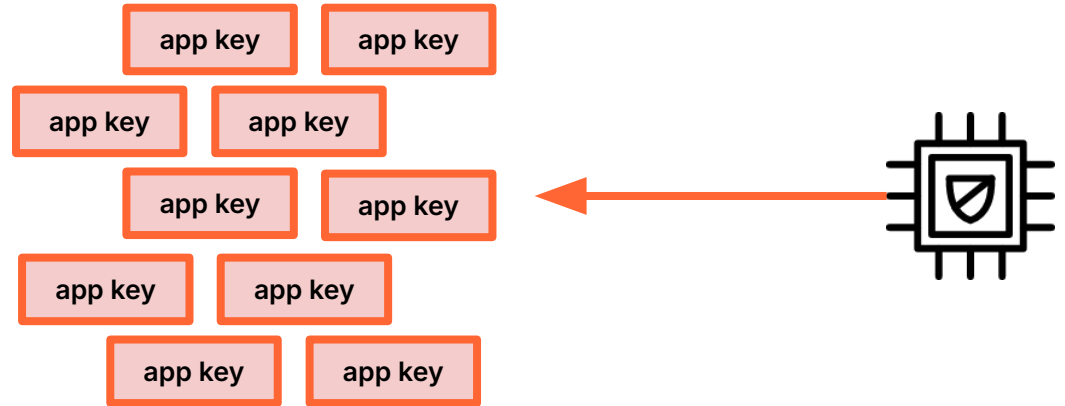
TPM



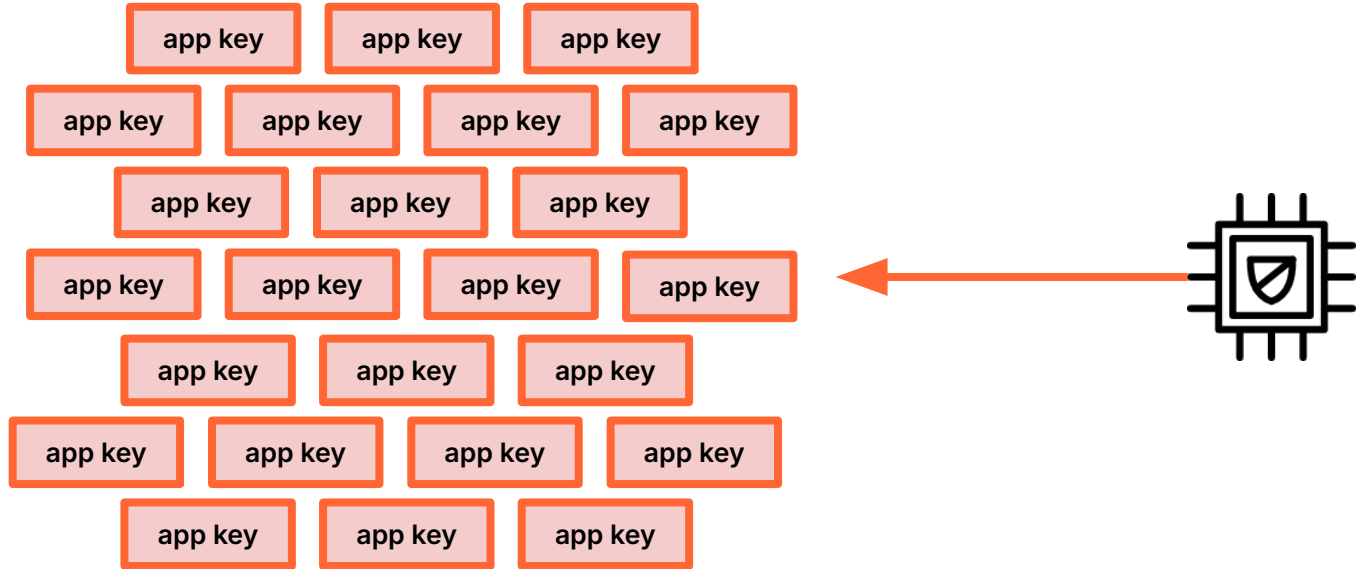
Derived keys



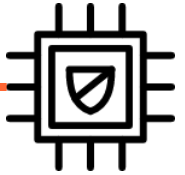
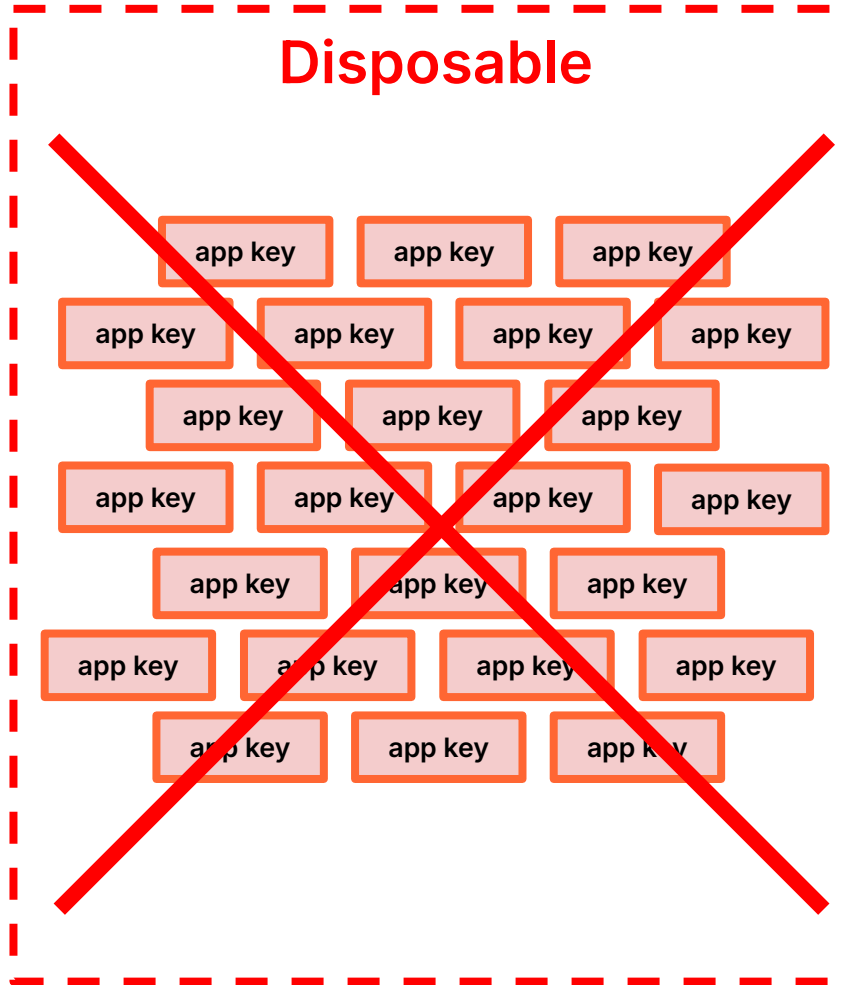
Derived keys



Derived keys



Derived keys



TPM derived keys

- <https://lore.kernel.org/all/20240503221634.44274-1-ignat@cloudflare.com/T/>

TPM derived keys

- <https://lore.kernel.org/all/20240503221634.44274-1-ignat@cloudflare.com/T/>
 - "I don't honestly believe that this will ever be a solution for any possible problem that exist in this planet"

TPM derived keys

- <https://lore.kernel.org/all/20240503221634.44274-1-ignat@cloudflare.com/T/>
 - "I don't honestly believe that this will ever be a solution for any possible problem that exist in this planet"
 - https://optee.readthedocs.io/en/latest/architecture/porting_guidelines.html#hardware-unique-key

TPM derived keys

- <https://lore.kernel.org/all/20240503221634.44274-1-ignat@cloudflare.com/T/>
 - "I don't honestly believe that this will ever be a solution for any possible problem that exist in this planet"
 - https://optee.readthedocs.io/en/latest/architecture/porting_guidelines.html#hardware-unique-key
 - <https://github.com/cloudflare/gokey>

TPM derived keys

- <https://lore.kernel.org/all/20240503221634.44274-1-ignat@cloudflare.com/T/>
 - "I don't honestly believe that this will ever be a solution for any possible problem that exist in this planet"
 - https://optee.readthedocs.io/en/latest/architecture/porting_guidelines.html#hardware-unique-key
 - <https://github.com/cloudflare/gokey>
 - <https://youtu.be/2RPclbP2xsM?si=nyBCFkhuzwbXBLZf>

TPM derived keys

- <https://lore.kernel.org/all/20240503221634.44274-1-ignat@cloudflare.com/T/>
 - "I don't honestly believe that this will ever be a solution for any possible problem that exist in this planet"
 - https://optee.readthedocs.io/en/latest/architecture/porting_guidelines.html#hardware-unique-key
 - <https://github.com/cloudflare/gokey>
 - <https://youtu.be/2RPclbP2xsM?si=nyBCFkhuzwbXBLZf>
- Since then
 - Reimplemented key derivation approach: replaced TPM-based HMAC with TPM-based AES256CTR PRNG

TPM derived keys

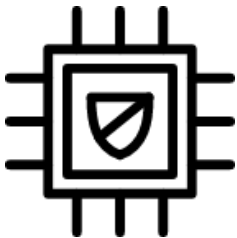
- <https://lore.kernel.org/all/20240503221634.44274-1-ignat@cloudflare.com/T/>
 - "I don't honestly believe that this will ever be a solution for any possible problem that exist in this planet"
 - https://optee.readthedocs.io/en/latest/architecture/porting_guidelines.html#hardware-unique-key
 - <https://github.com/cloudflare/gokey>
 - <https://youtu.be/2RPclbP2xsM?si=nyBCFkhuzwbXBLZf>
- Since then
 - Reimplemented key derivation approach: replaced TPM-based HMAC with TPM-based AES256CTR PRNG
 - Integrated support for TPM encrypted sessions

TPM derived keys

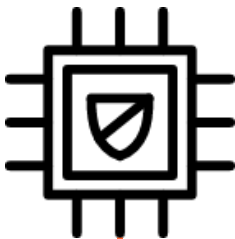
- <https://lore.kernel.org/all/20240503221634.44274-1-ignat@cloudflare.com/T/>
 - "I don't honestly believe that this will ever be a solution for any possible problem that exist in this planet"
 - https://optee.readthedocs.io/en/latest/architecture/porting_guidelines.html#hardware-unique-key
 - <https://github.com/cloudflare/gokey>
 - <https://youtu.be/2RPclbP2xsM?si=nyBCFkhuzwbXBLZf>
- Since then
 - Reimplemented key derivation approach: replaced TPM-based HMAC with TPM-based AES256CTR PRNG
 - Integrated support for TPM encrypted sessions
 - Compiles as a module

@ignatkn

TPM derived keys

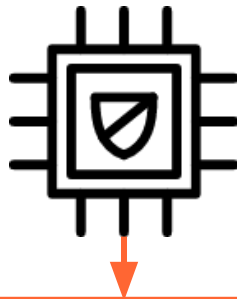


TPM derived keys



TPM2_CreatePrimary
(AES256CTR, UNIQUE)

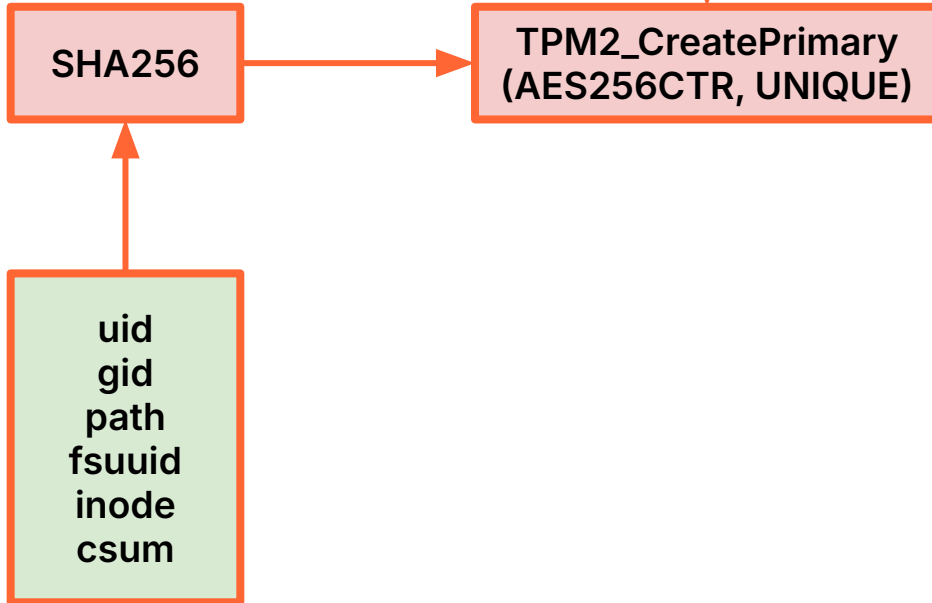
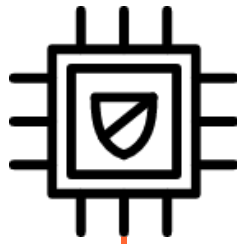
TPM derived keys



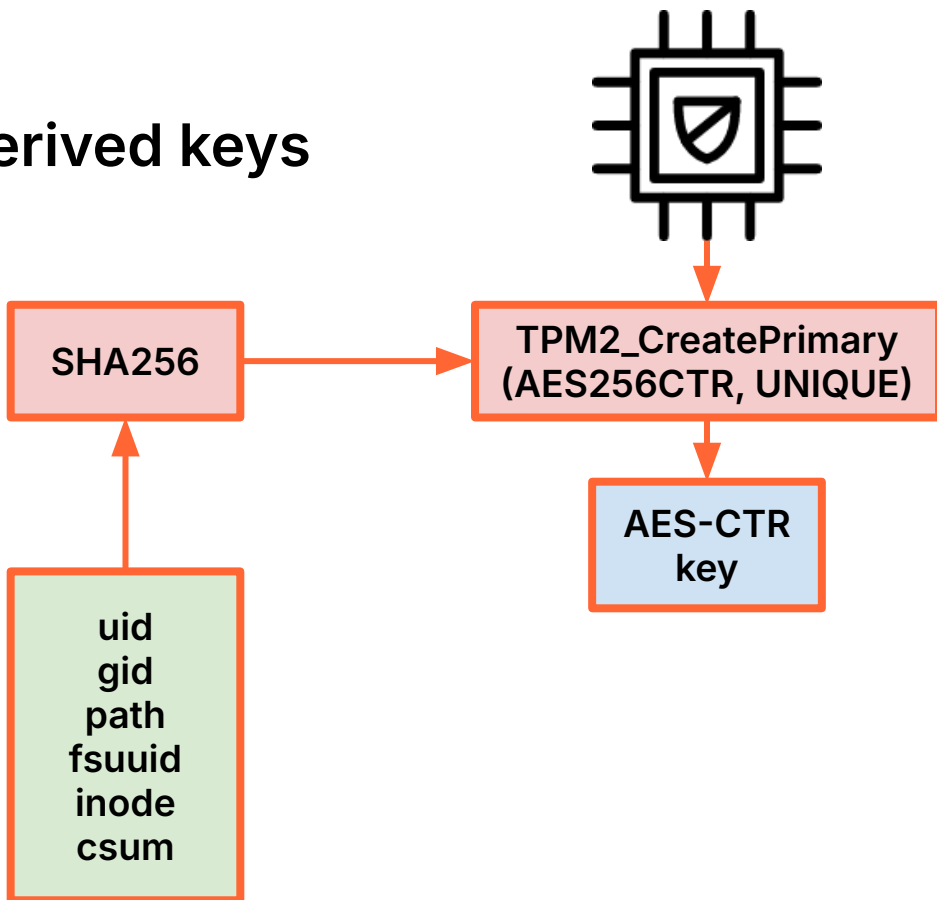
TPM2_CreatePrimary
(AES256CTR, UNIQUE)

uid
gid
path
fsuid
inode
csum

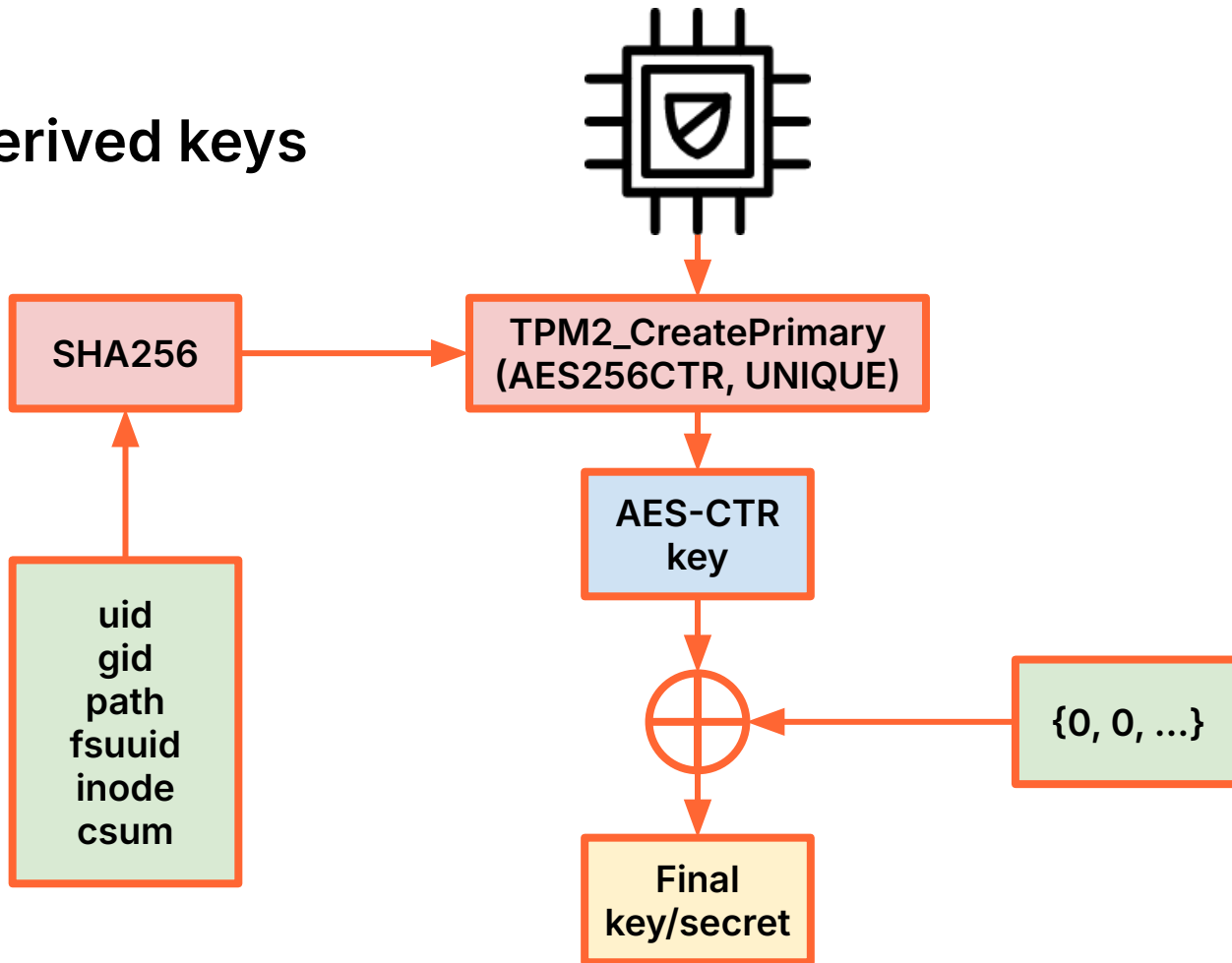
TPM derived keys



TPM derived keys



TPM derived keys



TPM user specific derived keys

```
$ keyctl request2 derived usr 'size=32 uid' @u
54647512
$ keyctl print 54647512
:hex:3254ee2cc1e1d79ccb22f15758a7b9504087222dd889a5efbc1c8b8b87b7148f
```

TPM user specific derived keys

```
$ keyctl request2 derived usr 'size=32 uid' @u
54647512
$ keyctl print 54647512
:hex:3254ee2cc1e1d79ccb22f15758a7b9504087222dd889a5efbc1c8b8b87b7148f
$ keyctl unlink 54647512
1 links removed
```

TPM user specific derived keys

```
$ keyctl request2 derived usr 'size=32 uid' @u
54647512
$ keyctl print 54647512
:hex:3254ee2cc1e1d79ccb22f15758a7b9504087222dd889a5efbc1c8b8b87b7148f
$ keyctl unlink 54647512
1 links removed
$ keyctl request2 derived usr 'size=32 uid' @u
265546475
$ keyctl print 265546475
:hex:3254ee2cc1e1d79ccb22f15758a7b9504087222dd889a5efbc1c8b8b87b7148f
```

TPM user specific derived keys

```
$ keyctl request2 derived usr 'size=32 uid' @u
54647512
$ keyctl print 54647512
:hex:3254ee2cc1e1d79ccb22f15758a7b9504087222dd889a5efbc1c8b8b87b7148f
$ keyctl unlink 54647512
1 links removed
$ keyctl request2 derived usr 'size=32 uid' @u
265546475
$ keyctl print 265546475
:hex:3254ee2cc1e1d79ccb22f15758a7b9504087222dd889a5efbc1c8b8b87b7148f
$ sudo keyctl request2 derived usr 'size=32 uid' @u
136468149
$ sudo keyctl print 136468149
:hex:9a360182012557e5e777ff3cb41737dcdaeab5efc8f0edbb4dbd3eae41a4b3a
```

TPM path specific derived keys

```
$ /usr/bin/keyctl request2 derived path 'size=16 path' @u  
452878500  
$ keyctl print 452878500  
:hex:59e4f47de768245442b259fe7c1d63a3
```

TPM path specific derived keys

```
$ /usr/bin/keyctl request2 derived path 'size=16 path' @u  
452878500  
$ keyctl print 452878500  
:hex:59e4f47de768245442b259fe7c1d63a3  
$ sudo cp /usr/bin/keyctl /opt/bin/
```

TPM path specific derived keys

```
$ /usr/bin/keyctl request2 derived path 'size=16 path' @u
452878500
$ keyctl print 452878500
:hex:59e4f47de768245442b259fe7c1d63a3
$ sudo cp /usr/bin/keyctl /opt/bin/
$ /opt/bin/keyctl request2 derived path2 'size=16 path' @u
857975889
$ keyctl print 857975889
:hex:d2a11b4c7c26989f7f2b540cfaee3614
```

TPM path specific derived keys

```
$ keyctl request2 derived usrpath 'size=16 uid path' @u
232879988
$ keyctl print 232879988
:hex:f3bf22ea6af497e6db8a607d92458db8
```

TPM path specific derived keys

```
$ keyctl request2 derived usrpath 'size=16 uid path' @u  
232879988  
$ keyctl print 232879988  
:hex:f3bf22ea6af497e6db8a607d92458db8  
$ keyctl request2 derived fsinfo 'size=16 uid fsuid inode' @u  
521409059  
$ keyctl print 521409059  
:hex:cf1a11a887a5e09d8b04efac4233c32d
```

TPM executable specific derived keys

```
$ /opt/bin/keyctl request2 derived exec 'size=16 csum' @u
92734356
$ keyctl print 92734356
:hex:904efb23fa808d9181a7824d1a251f41
```

TPM executable specific derived keys

```
$ /opt/bin/keyctl request2 derived exec 'size=16 csum' @u
92734356
$ keyctl print 92734356
:hex:904efb23fa808d9181a7824d1a251f41
$ sudo sed -i 's/Bad message/Bad message/' /opt/bin/keyctl
$ keyctl unlink 92734356
1 links removed
```

TPM executable specific derived keys

```
$ /opt/bin/keyctl request2 derived exec 'size=16 csum' @u
92734356
$ keyctl print 92734356
:hex:904efb23fa808d9181a7824d1a251f41
$ sudo sed -i 's/Bad message/Bad message/' /opt/bin/keyctl
$ keyctl unlink 92734356
1 links removed
$ /opt/bin/keyctl request2 derived exec 'size=16 csum' @u
251529703
$ keyctl print 251529703
:hex:020ea5f206f93f4c5d44519192888ef1
```



What if the application needs to rotate keys because of a suspected compromise?



TPM derived keys with labels

```
$ keyctl request2 derived v1 'size=16 label=v1' @u  
274539938  
$ keyctl print 274539938  
:hex:b318728ff0f37e68bbaa5086480c3e25
```

TPM derived keys with labels

```
$ keyctl request2 derived v1 'size=16 label=v1' @u  
274539938
```

```
$ keyctl print 274539938
```

```
:hex:b318728ff0f37e68bbaa5086480c3e25
```

```
$ keyctl request2 derived v2 'size=16 label=v2' @u  
17456321
```

```
$ keyctl print 17456321
```

```
:hex:1e290b243aa46a9d2020eb14273dd214
```

“

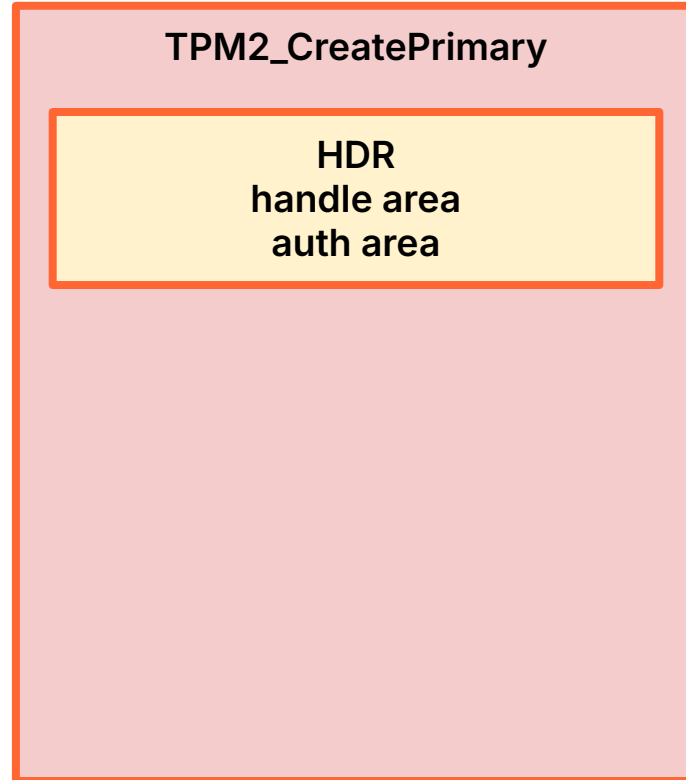
Those mixing values are well known ... then anyone with access to the TPM can derive the key from user space because they can easily obtain the mixing parameters and there's no protection to the TPM keyed hash operation



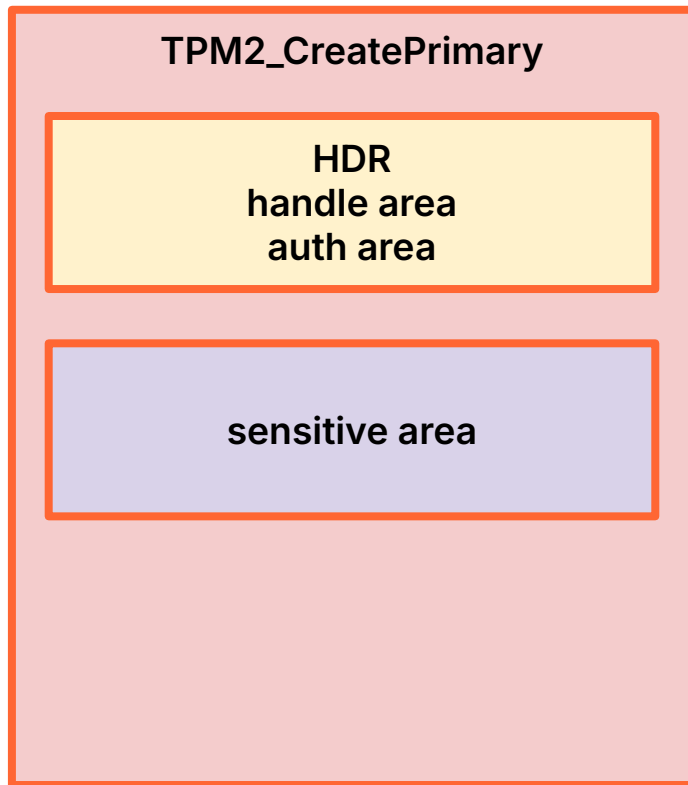
Kernel reserved unique domain

TPM2_CreatePrimary

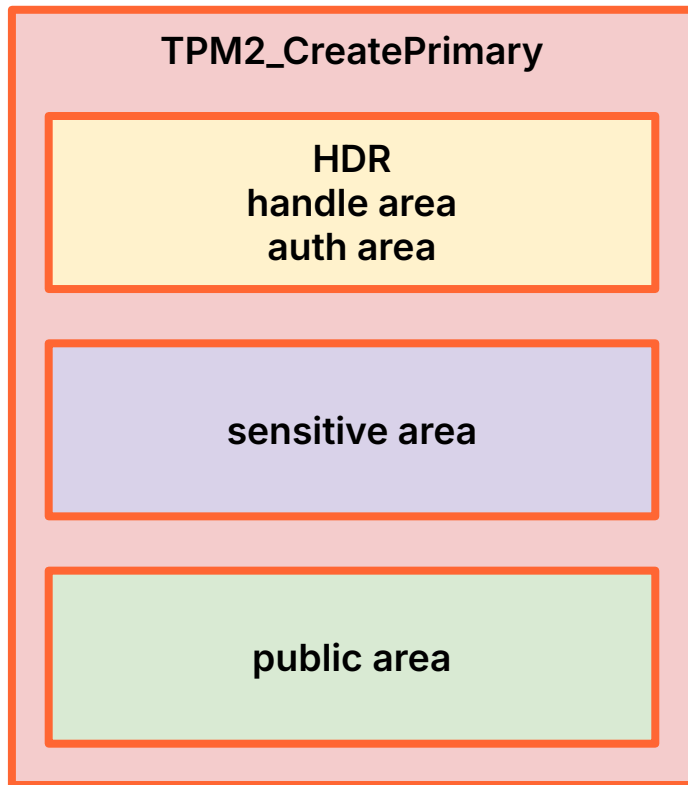
Kernel reserved unique domain



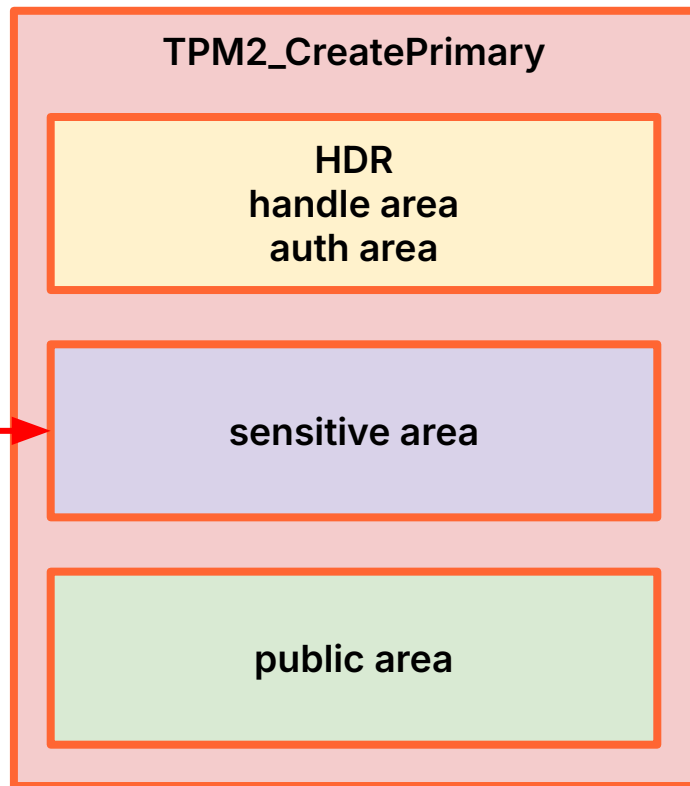
Kernel reserved unique domain



Kernel reserved unique domain



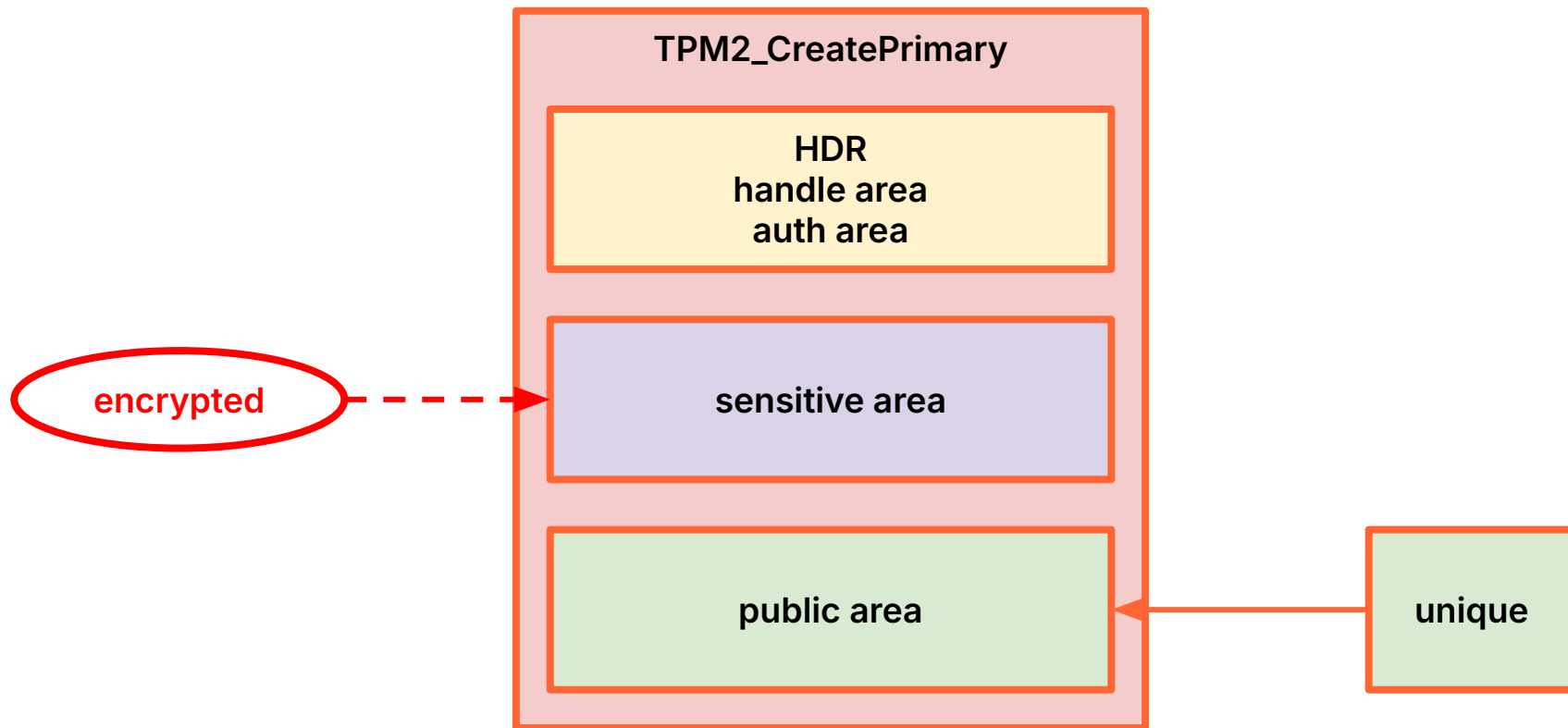
Kernel reserved unique domain



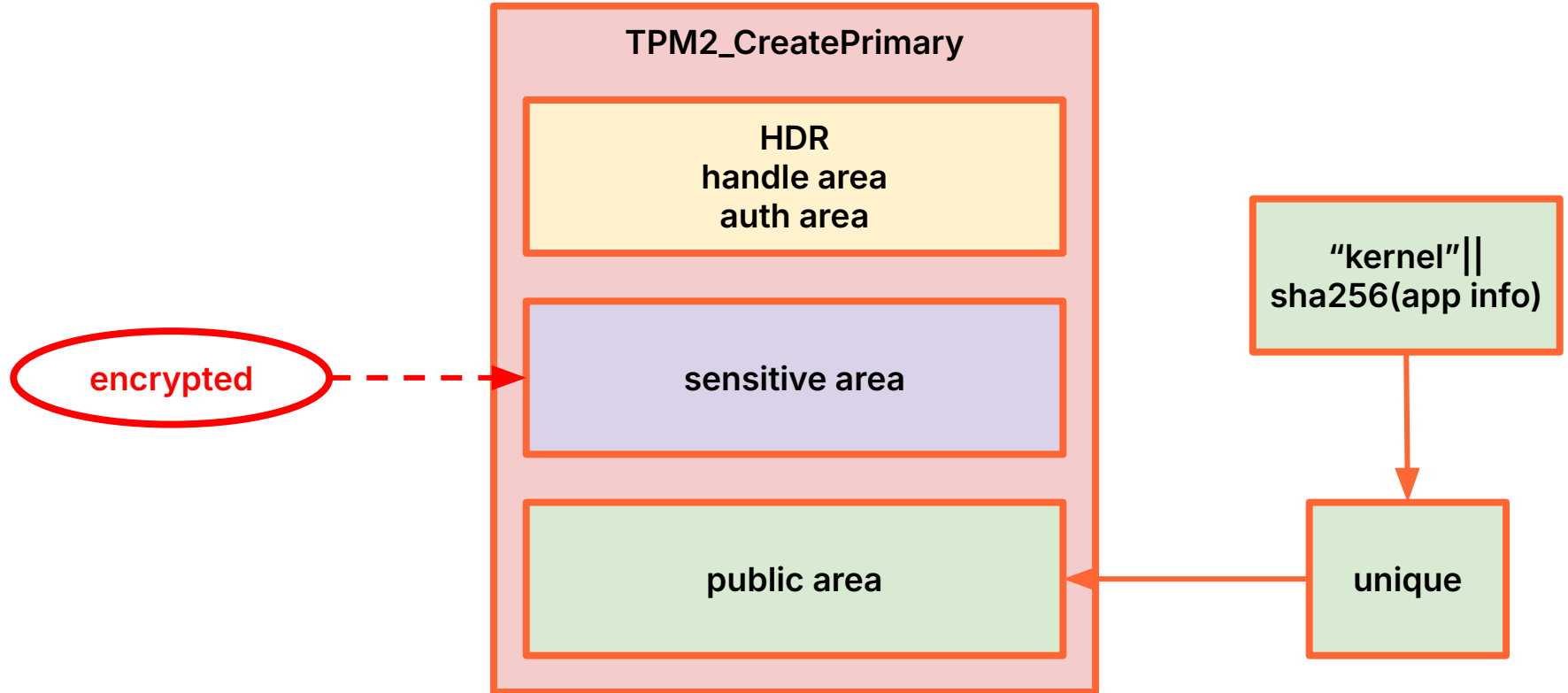
encrypted



Kernel reserved unique domain



Kernel reserved unique domain



Kernel reserved unique domain

```
$ echo abc | sudo tpm2_createprimary -G aes256ctr -u -  
...  
symcipher:  
6d235c411a6f23ba2d88f81269cca65962a3a95b734ac9ba7d3fc6066  
9b5fc24
```

Kernel reserved unique domain

```
$ echo abc | sudo tpm2_createprimary -G aes256ctr -u -  
...  
symcipher:  
6d235c411a6f23ba2d88f81269cca65962a3a95b734ac9ba7d3fc6066  
9b5fc24  
$ echo kernel | sudo tpm2_createprimary -G aes256ctr -u -  
ERROR:tcti:src/tss2-tcti/tcti-device.c:198:tcti_device_re  
ceive() Failed to get response size fd 3, got errno 1:  
Operation not permitted  
...
```

RFC

- What else is missing for easier adoption of TPMs in Linux software?
 - Any other application mixin parameters to be implemented?
 - Any other use-cases to be considered?

RFC

- What else is missing for easier adoption of TPMs in Linux software?
 - Any other application mixin parameters to be implemented?
 - Any other use-cases to be considered?
- Should we support better separation between generic secrets and non-exportable keys?

RFC

- What else is missing for easier adoption of TPMs in Linux software?
 - Any other application mixin parameters to be implemented?
 - Any other use-cases to be considered?
- Should we support better separation between generic secrets and non-exportable keys?
- Would be nice to piggy-back on advanced TPM capabilities to prove to a remote party that a particular key/secret was derived with the help of a particular TPM
 - How to add opt-in support for credential activation?

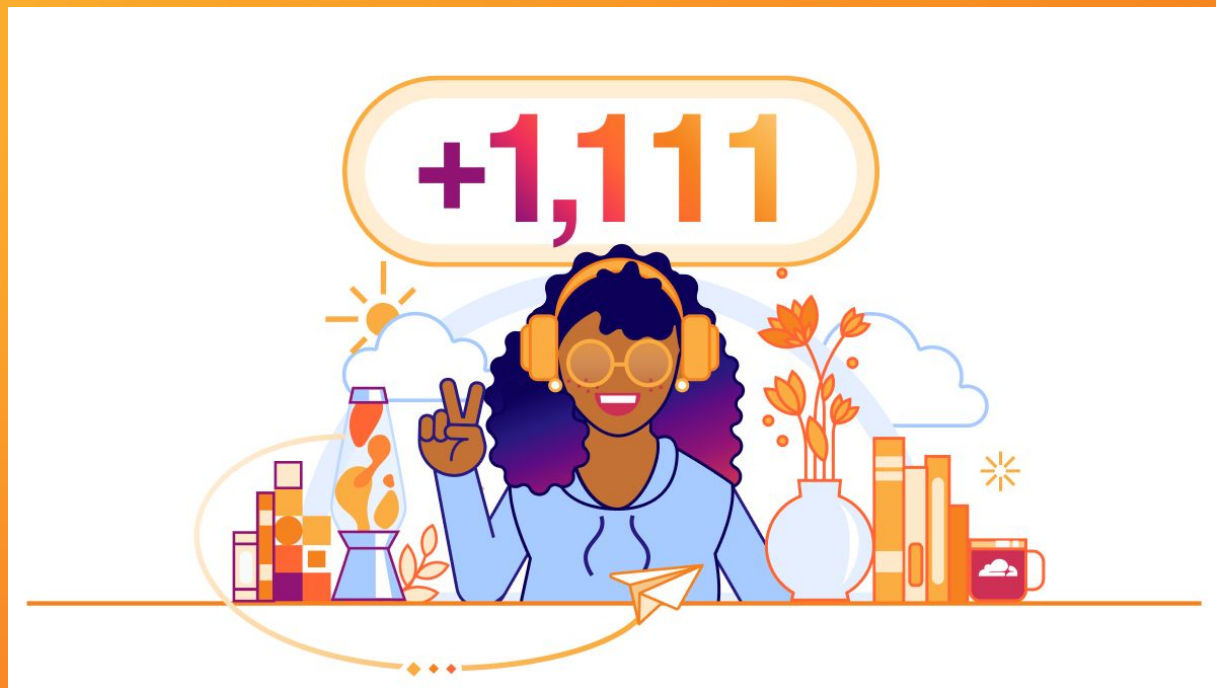
RFC

- What else is missing for easier adoption of TPMs in Linux software?
 - Any other application mixin parameters to be implemented?
 - Any other use-cases to be considered?
- Should we support better separation between generic secrets and non-exportable keys?
- Would be nice to piggy-back on advanced TPM capabilities to prove to a remote party that a particular key/secret was derived with the help of a particular TPM
 - How to add opt-in support for credential activation?

<https://github.com/ignatkn/linux/tree/b4/tpm-derived-keys>

Thank you!

Questions?



<https://blog.cloudflare.com/cloudflare-1111-intern-program/>