TPMs and the Linux Kernel

Unlocking a better path to hardware security

Ignat Korchagin
@ignatkn

@ignatkn

CLOUDFLARE

$ whoami

- Linux team at Cloudflare
- Systems security and performance
- Low-level programming

@ignatkn

CLOUDFLARE

What is a TPM?

@ignatkn

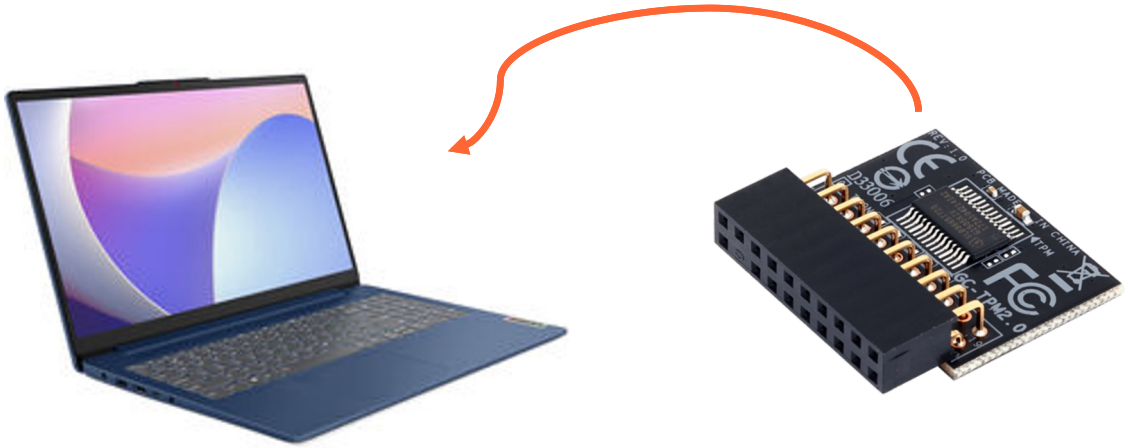
CLOUDFLARE

What is a TPM?

@ignatkn

CLOUDFLARE

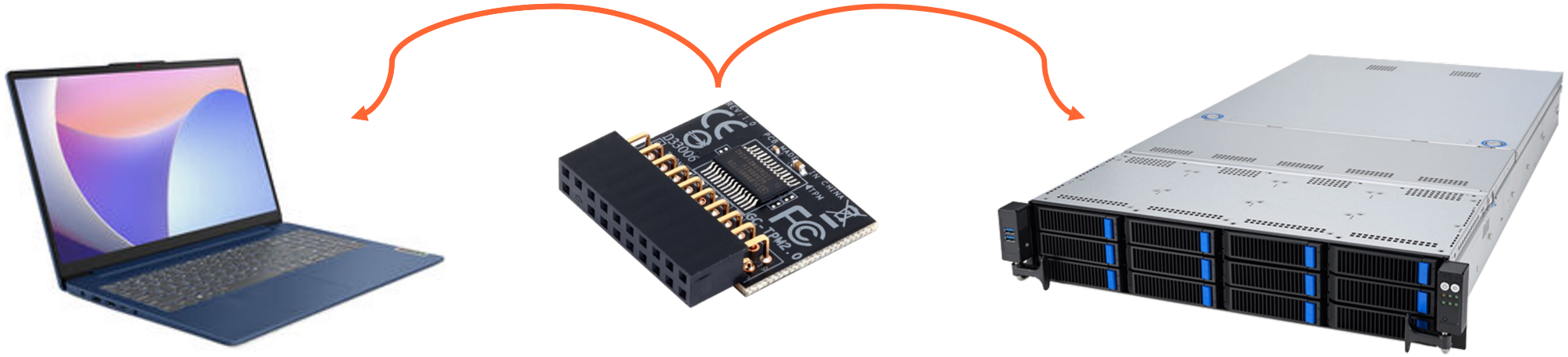
What is a TPM?



@ignatkn

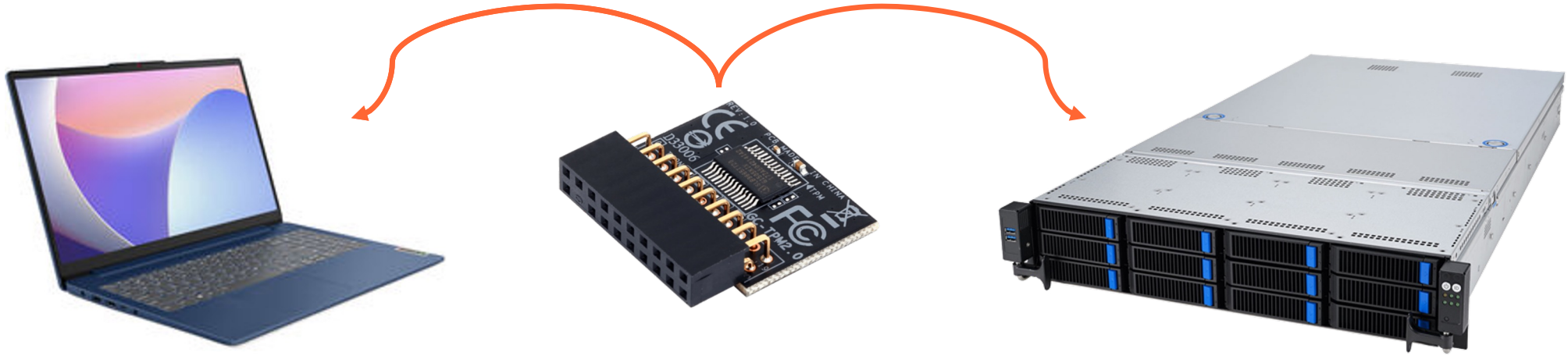
CLOUDFLARE

What is a TPM?



CLOUDFLARE

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

@ignatkn

CLOUDFLARE

This talk is not about system integrity or attestation

Can I store my keys in the TPM?

And use them without exposing the key material to the main memory?

@ignatkn

CLOUDFLARE

Application keys in the TPM

@ignatkn

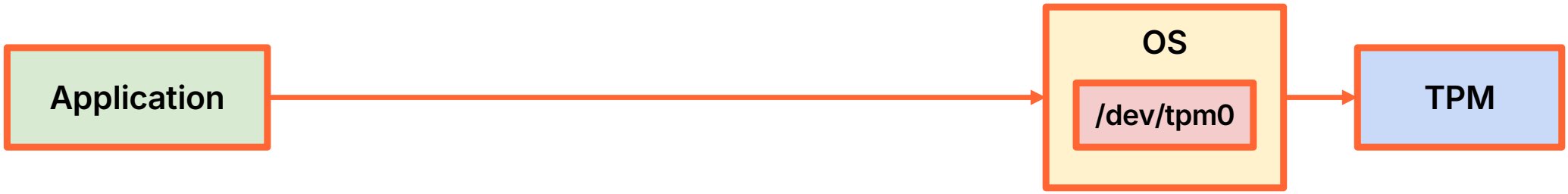
CLOUDFLARE

Application keys in the TPM

@ignatkn

CLOUDFLARE

Application keys in the TPM



CLOUDFLARE

Application keys in the TPM

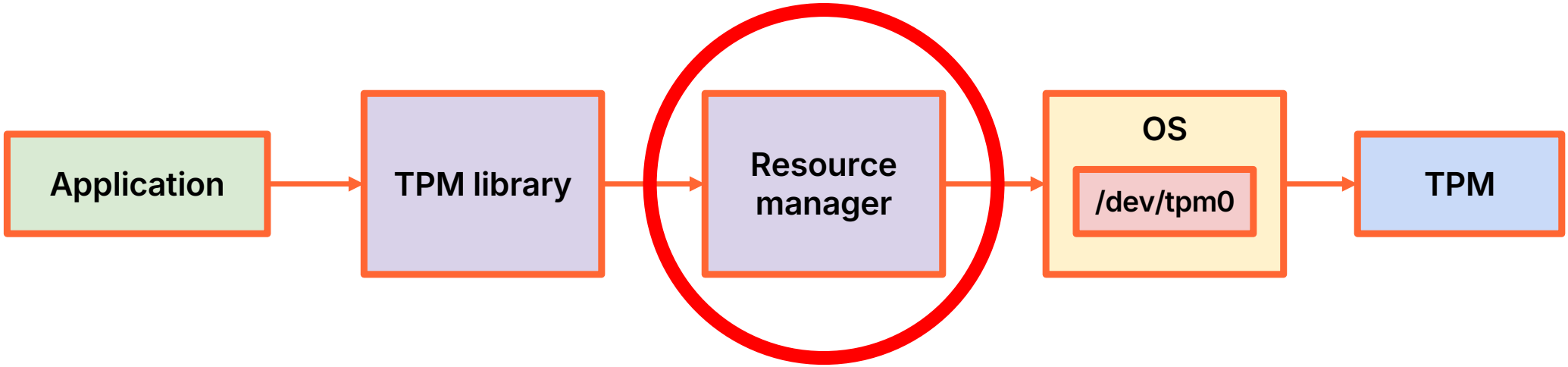
@ignatkn

CLOUDFLARE

Application keys in the TPM

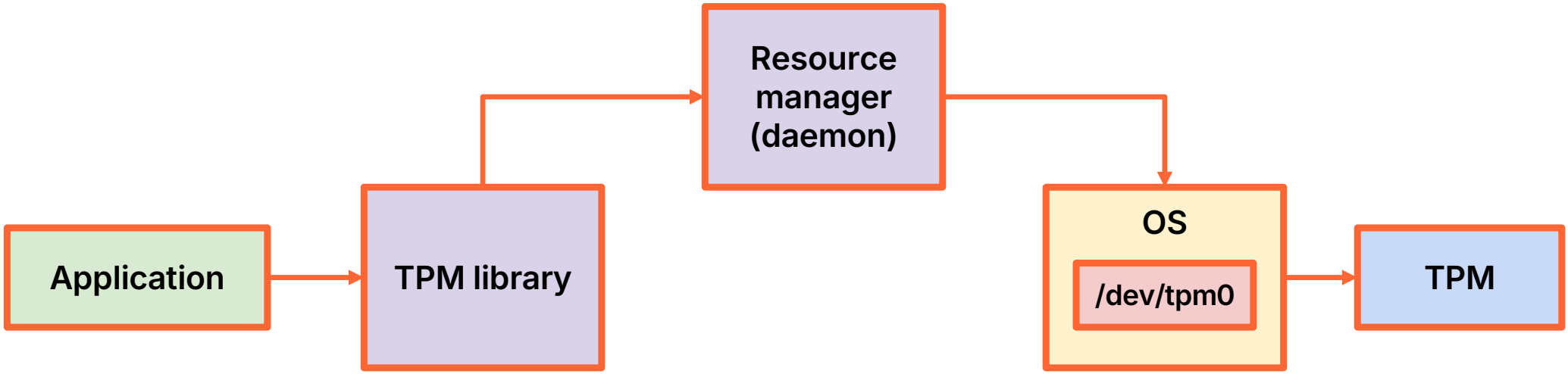
CLOUDFLARE

Application keys in the TPM



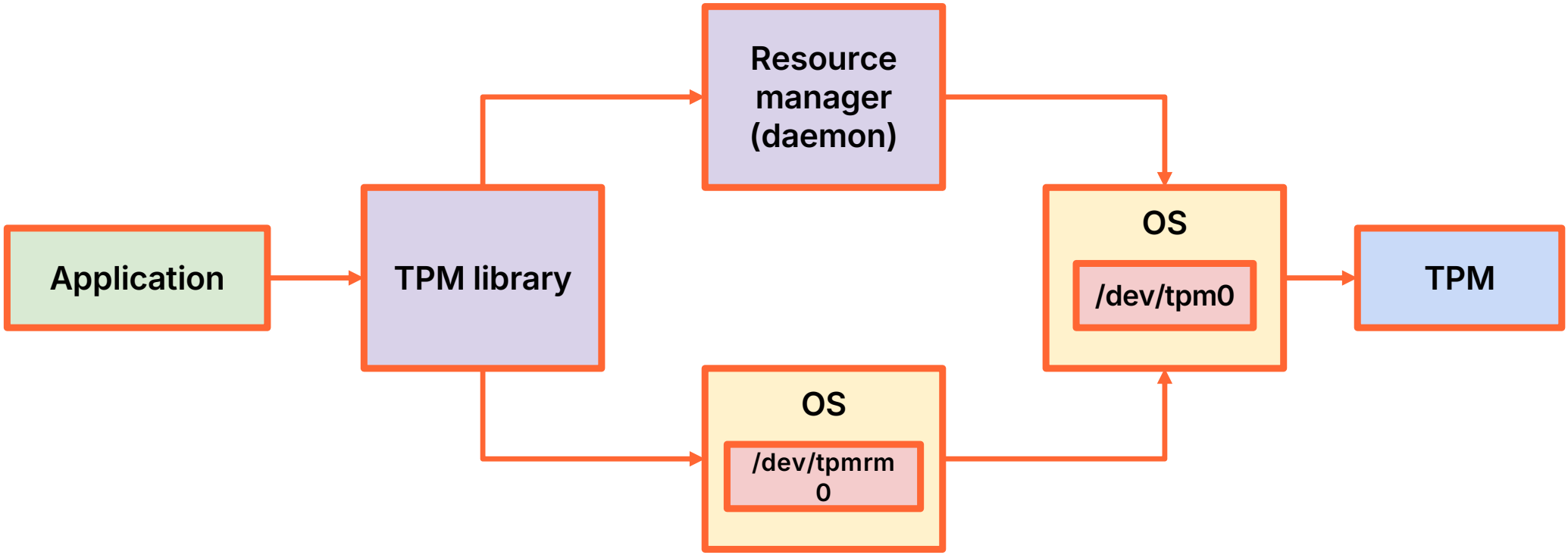
CLOUDFLARE

Application keys in the TPM



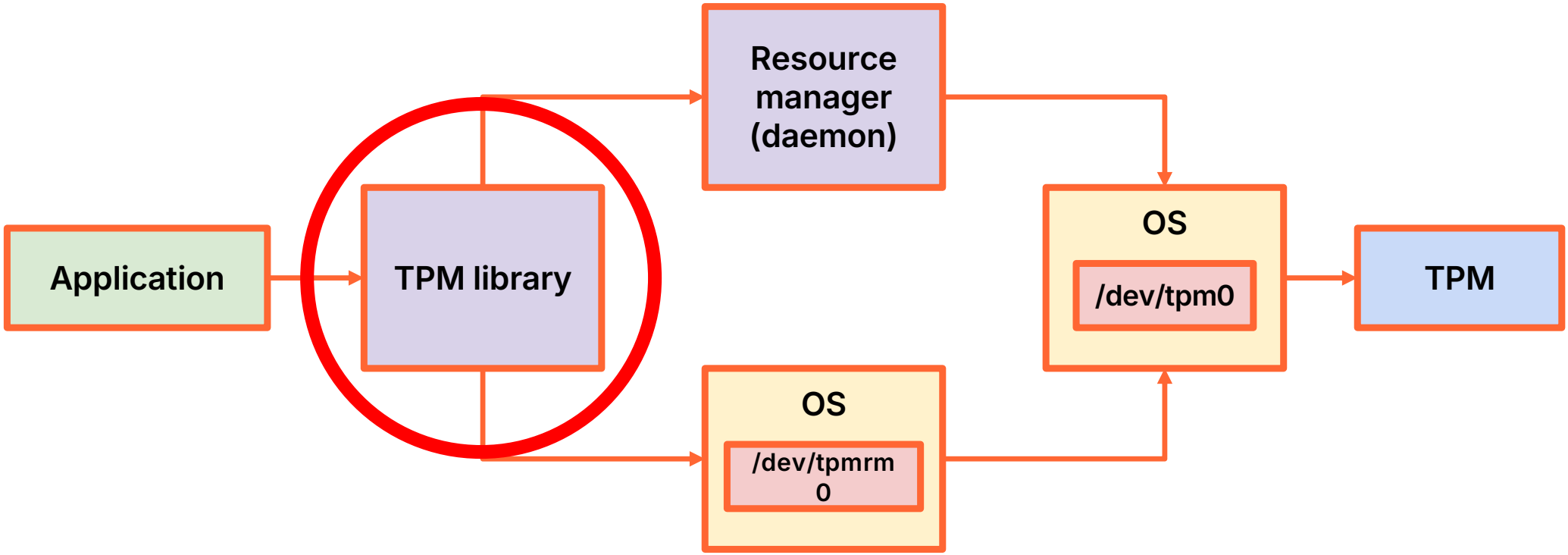
CLOUDFLARE

Application keys in the TPM



CLOUDFLARE

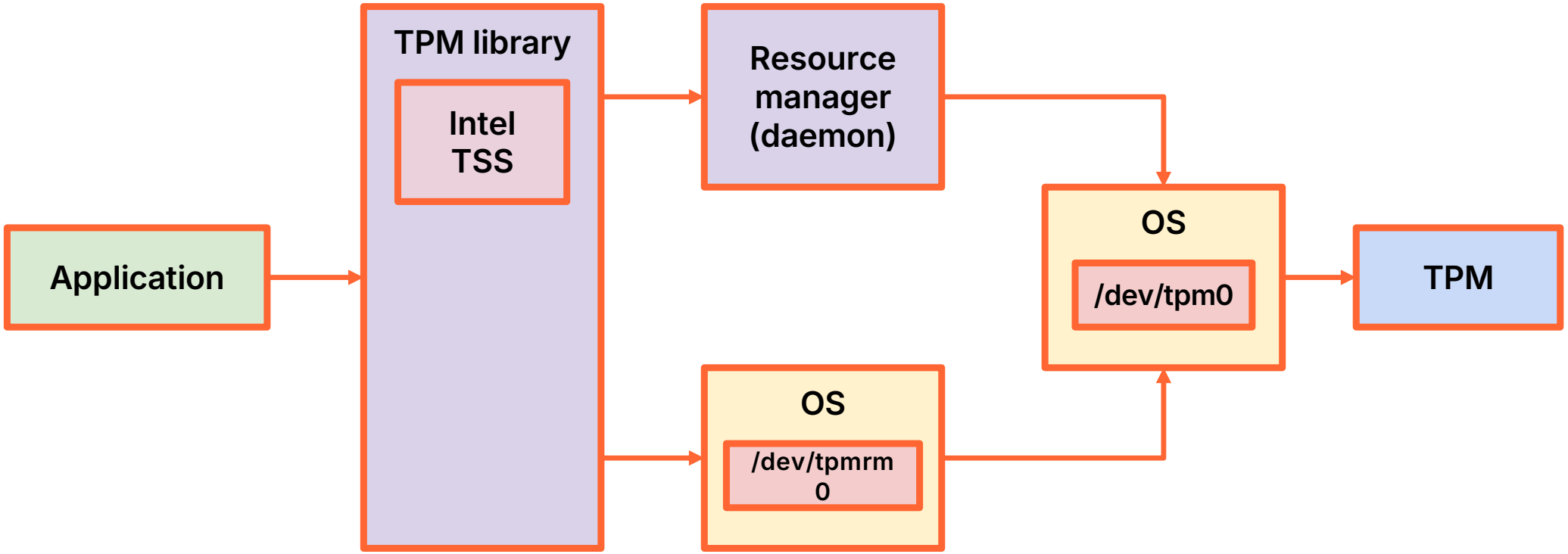
Application keys in the TPM



@ignatkn

CLOUDFLARE

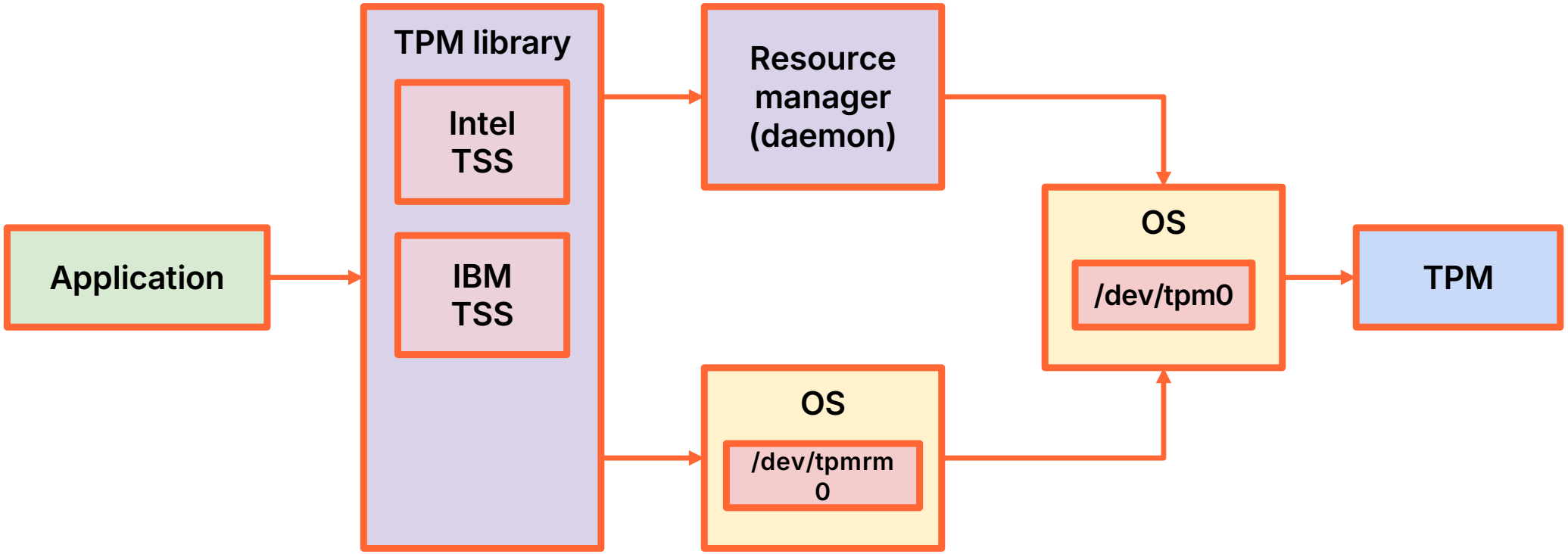
Application keys in the TPM



@ignatkn

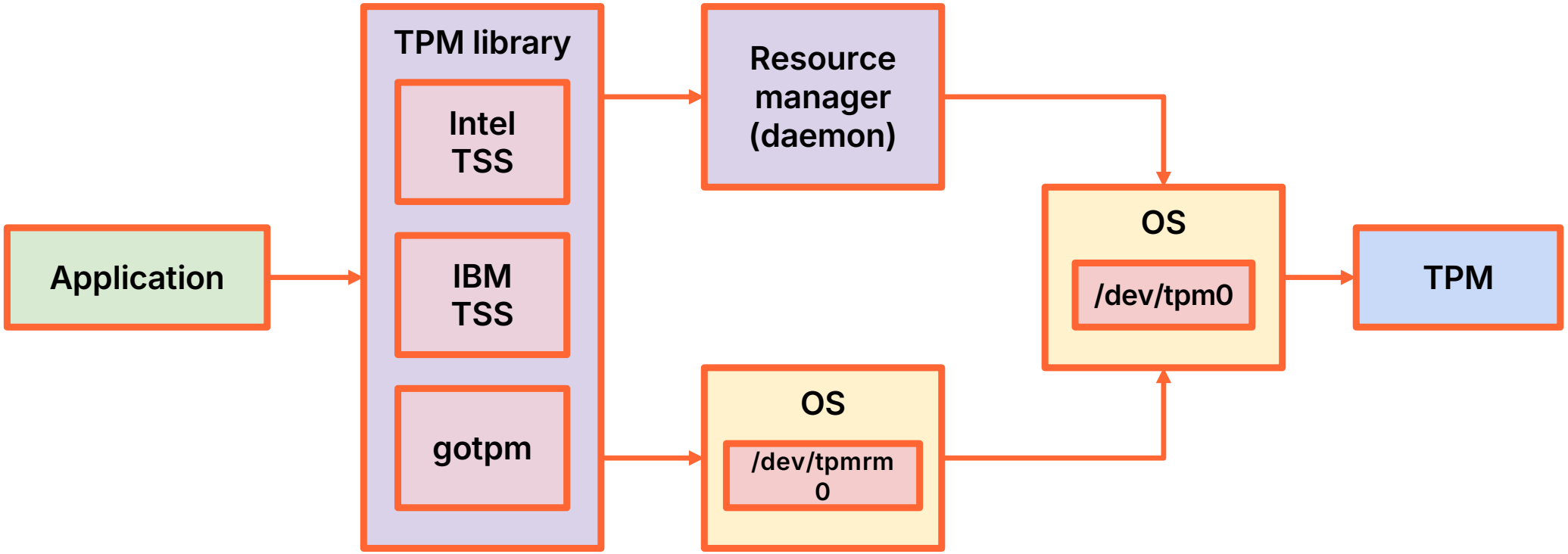
CLOUDFLARE

Application keys in the TPM



CLOUDFLARE

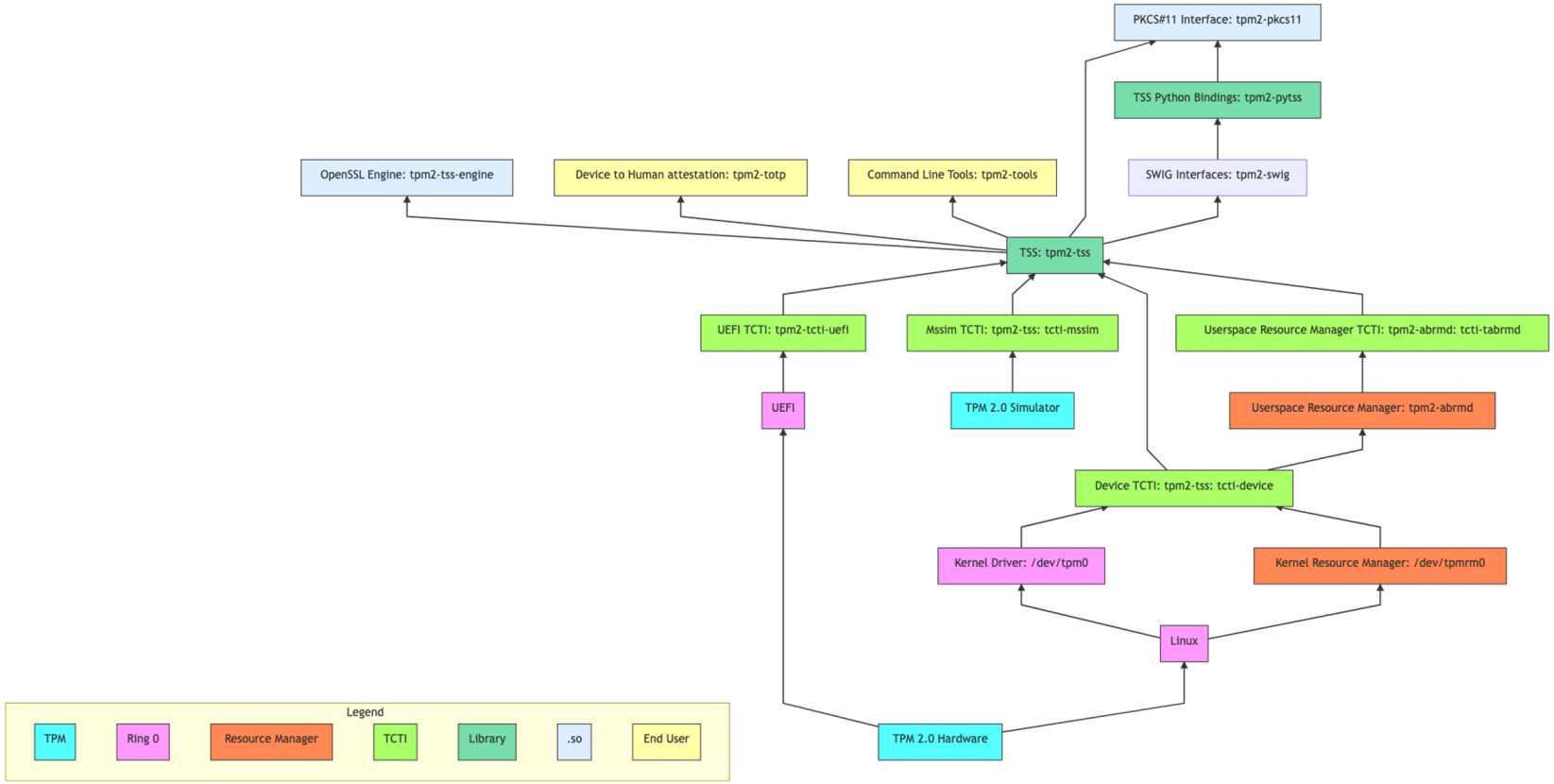
Application keys in the TPM



@ignatkn

CLOUDFLARE

TPM2 software stack



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

CLOUDFLARE

Application keys in the TPM

CLOUDFLARE

Access permissions for the TPM

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

CLOUDFLARE

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
```

CLOUDFLARE

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
```

CLOUDFLARE

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
...
```

CLOUDFLARE

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
```

CLOUDFLARE

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
```

@ignatkn

CLOUDFLARE

Linux Kernel key retention service

AKA keyrings or keystore

@ignatkn

CLOUDFLARE

Linux Kernel key retention service

Application

Application

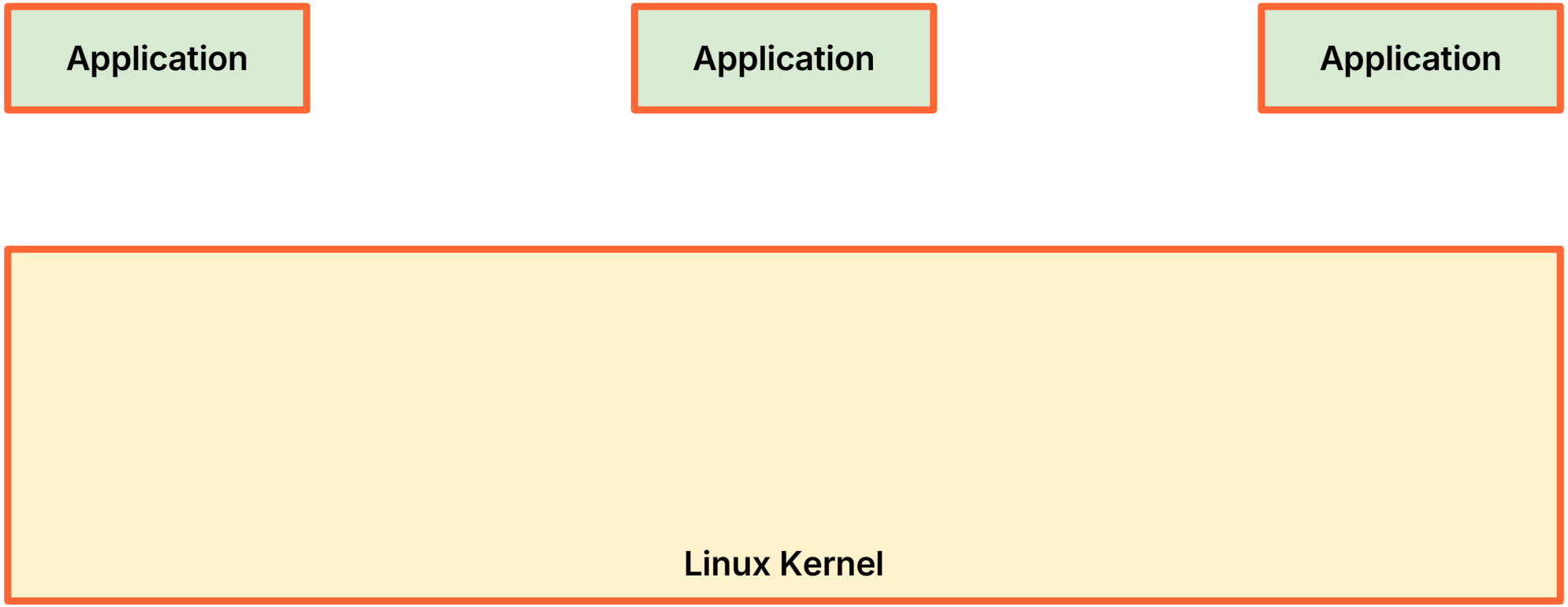
Application

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

@ignatkn

CLOUDFLARE

Linux Kernel key retention service

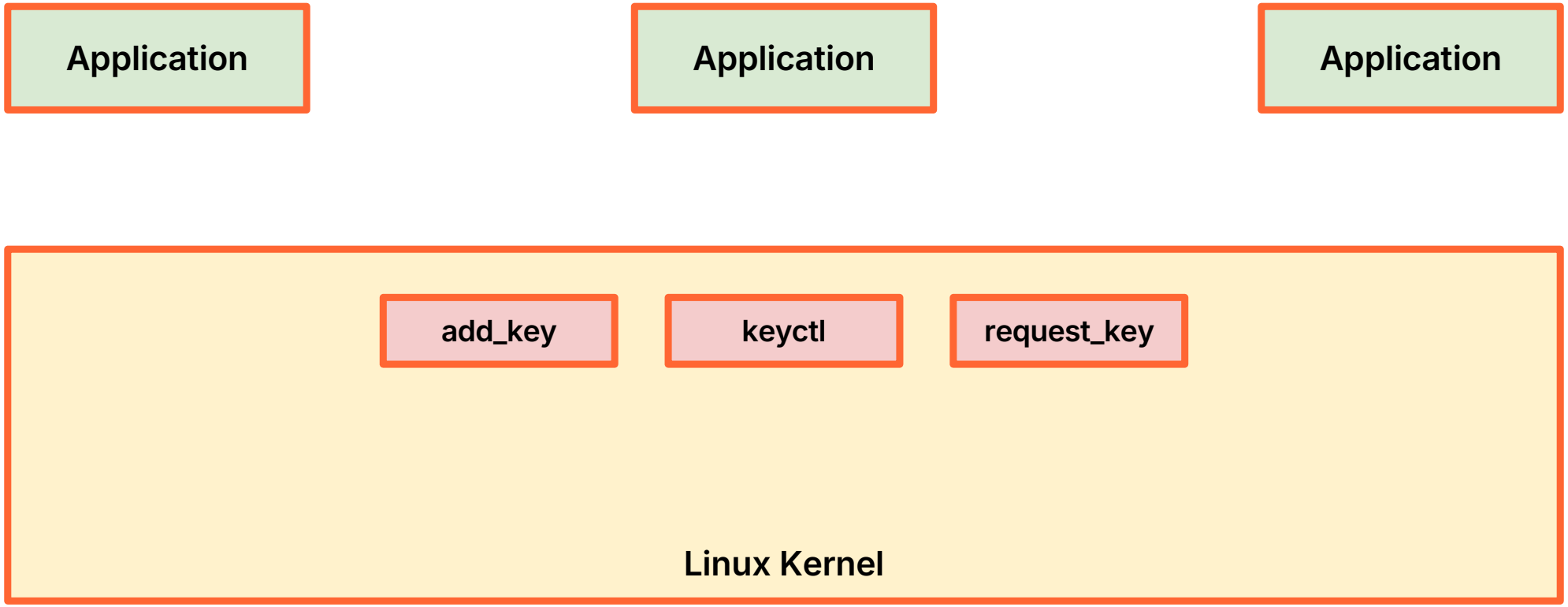


https://www.kernel.org/doc/html/latest/security/keys/core.html

@ignatkn

CLOUDFLARE

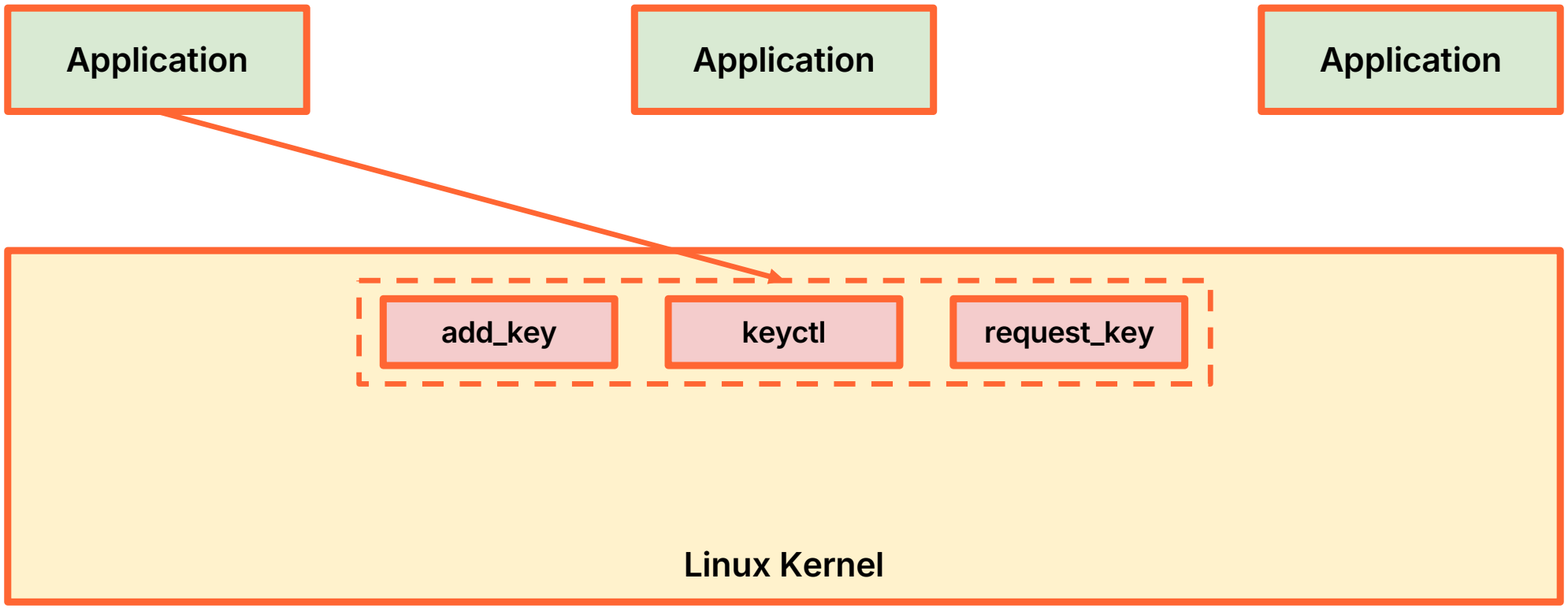
Linux Kernel key retention service



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

CLOUDFLARE

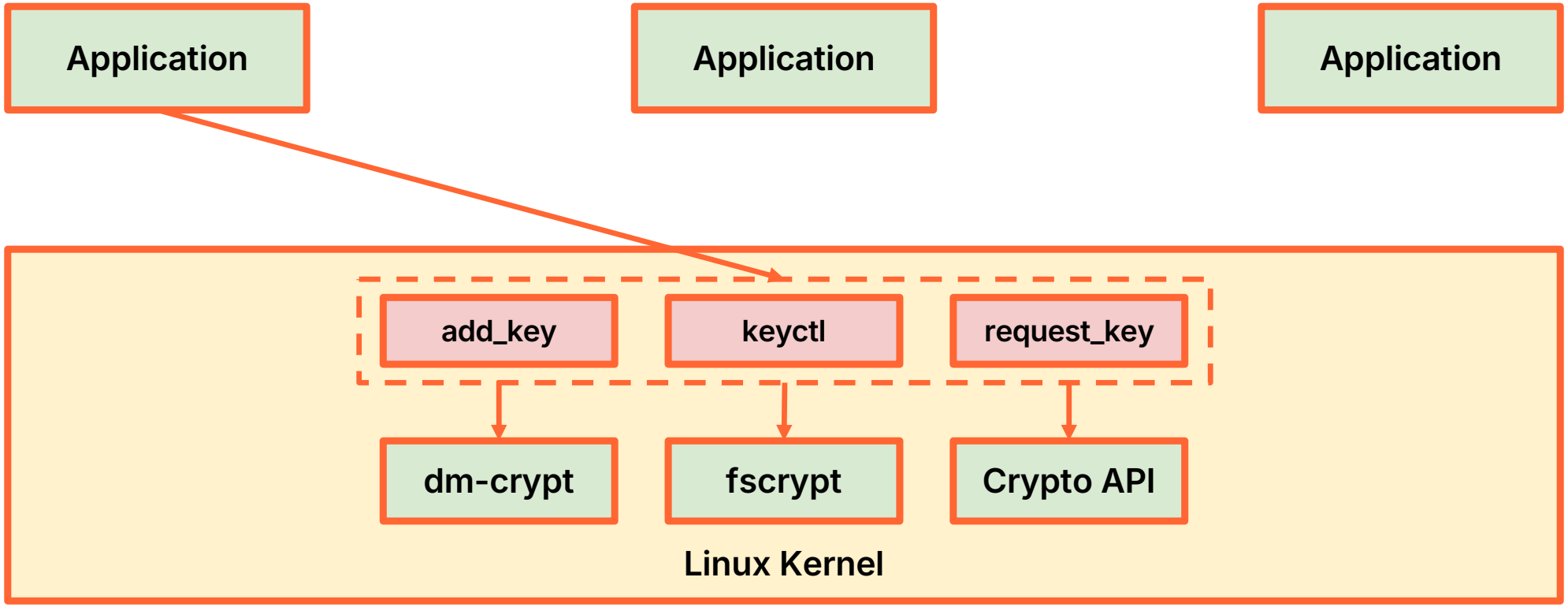
Linux Kernel key retention service



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

CLOUDFLARE

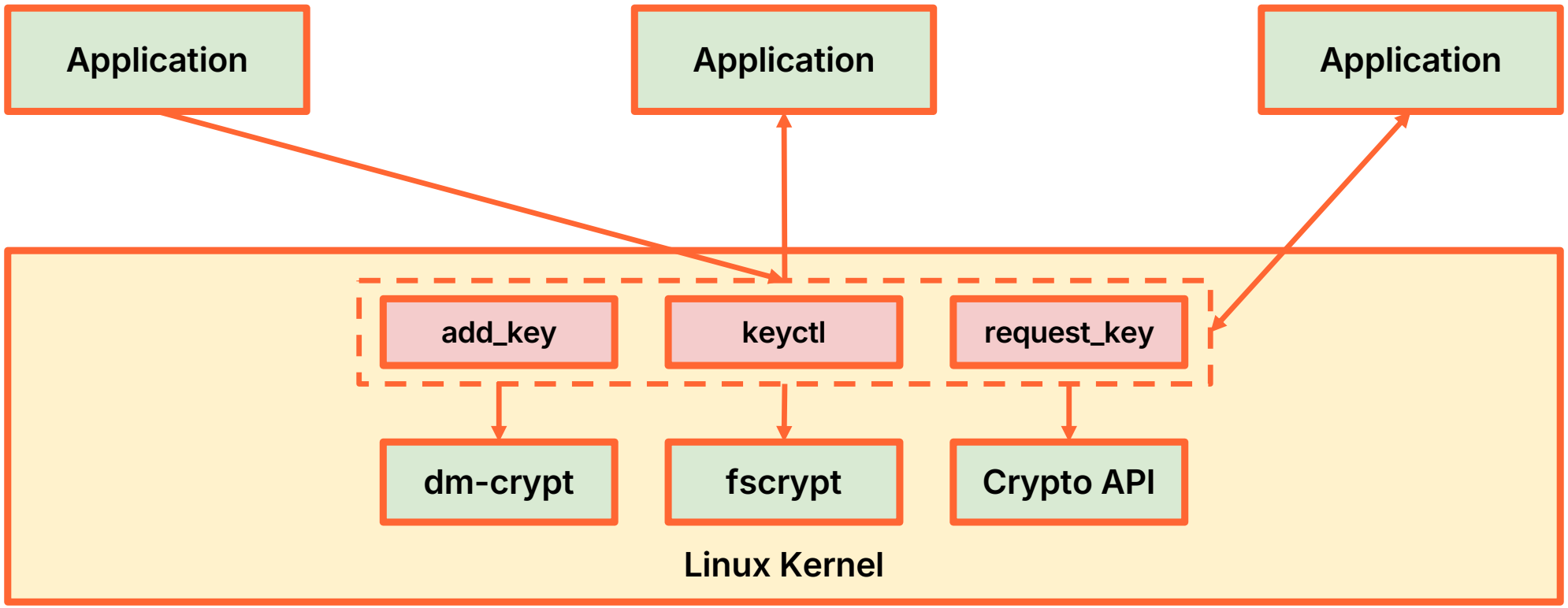
Linux Kernel key retention service



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

CLOUDFLARE

Linux Kernel key retention service



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

@ignatkn

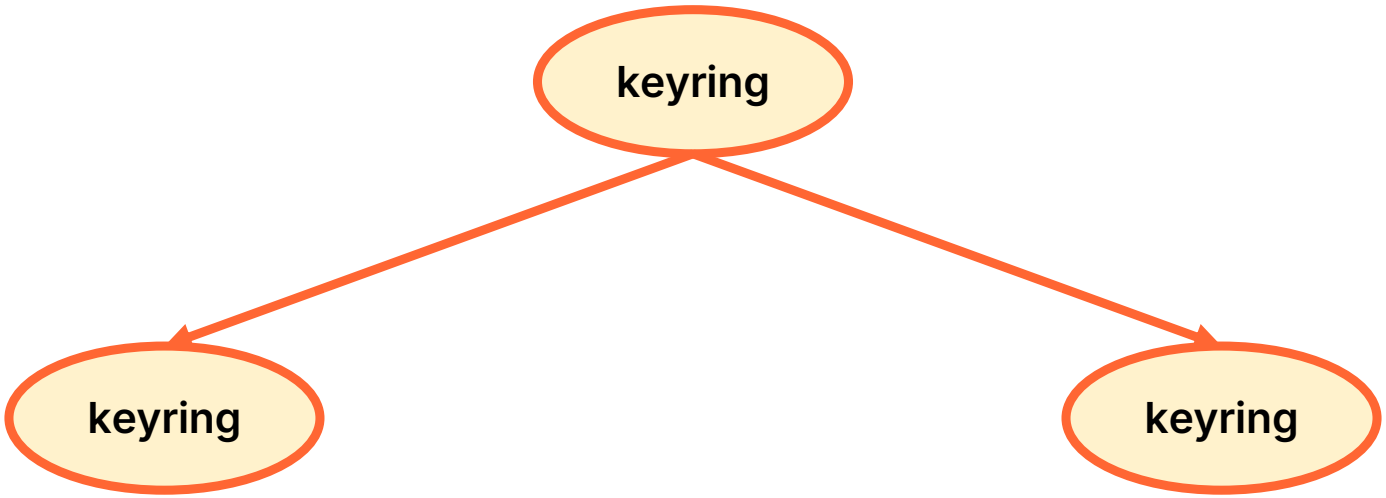
CLOUDFLARE

Keys and keyrings

@ignatkn

CLOUDFLARE

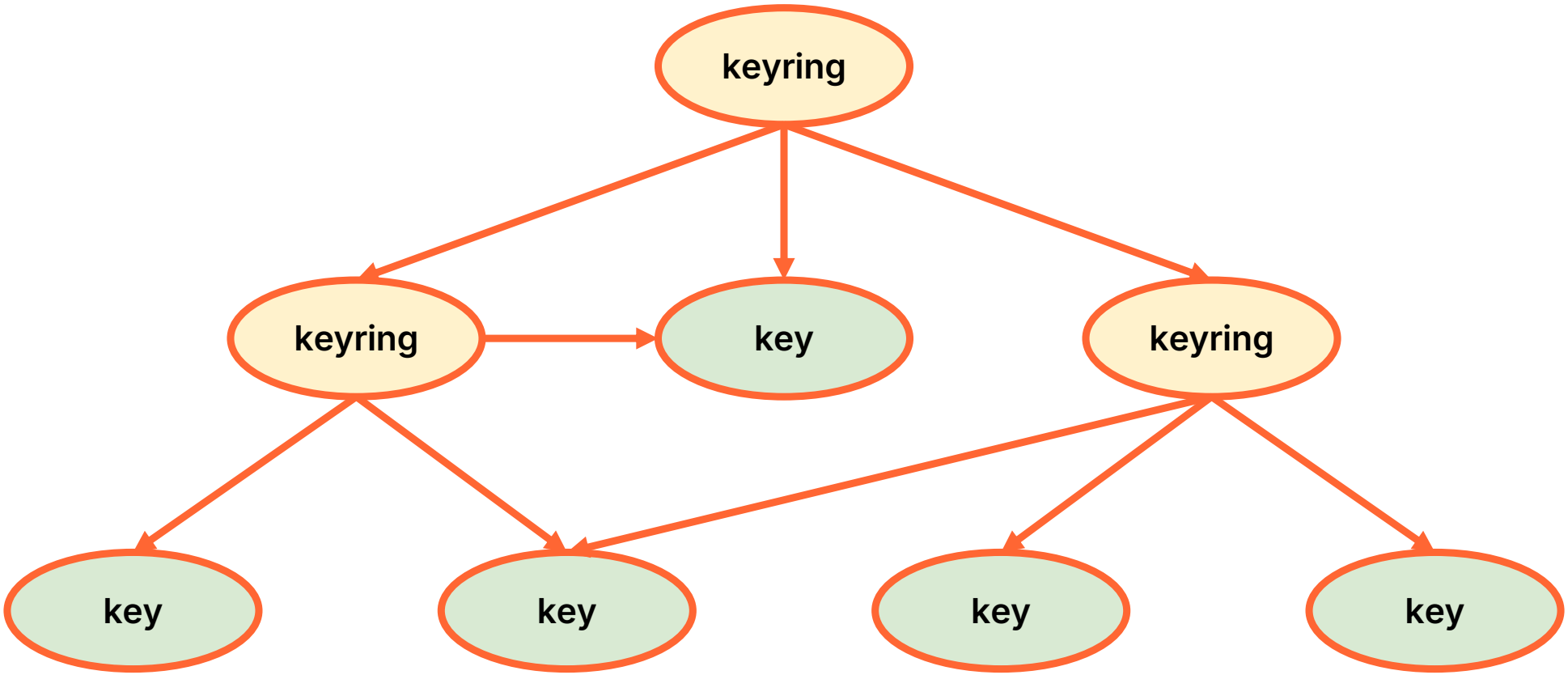
Keys and keyrings



@ignatkn

CLOUDFLARE

Keys and keyrings



CLOUDFLARE

Example: secret sharing

```
alice@dev:~$ id
uid=1001(alice) gid=1001(alice)
groups=1001(alice)
```

```
bob@dev:~$ id
uid=1002(bob) gid=1002(bob)
groups=1002(bob)
```

CLOUDFLARE

Example: secret sharing

```
alice@dev:~$ id
uid=1001(alice) gid=1001(alice)
groups=1001(alice)
alice@dev:~$ keyctl add user secret
hunter2 @u
791615806
```

```
bob@dev:~$ id
uid=1002(bob) gid=1002(bob)
groups=1002(bob)
```

CLOUDFLARE

Example: secret sharing

```
alice@dev:~$ id
uid=1001(alice) gid=1001(alice)
groups=1001(alice)
alice@dev:~$ keyctl add user secret
hunter2 @u
791615806
```

```
bob@dev:~$ id
uid=1002(bob) gid=1002(bob)
groups=1002(bob)
bob@dev:~$ keyctl newring from-others @u
966722684
```

CLOUDFLARE

Example: secret sharing

```
alice@dev:~$ id
uid=1001(alice) gid=1001(alice)
groups=1001(alice)
alice@dev:~$ keyctl add user secret
hunter2 @u
791615806
```

```
bob@dev:~$ id
uid=1002(bob) gid=1002(bob)
groups=1002(bob)
bob@dev:~$ keyctl newring from-others @u
966722684
bob@dev:~$ keyctl setperm %:from-others
0x3f010004
```

CLOUDFLARE

Example: secret sharing

```
alice@dev:~$ id
uid=1001(alice) gid=1001(alice)
groups=1001(alice)
alice@dev:~$ keyctl add user secret
hunter2 @u
791615806
alice@dev:~$ keyctl move %user:secret
@u 966722684
```

```
bob@dev:~$ id
uid=1002(bob) gid=1002(bob)
groups=1002(bob)
bob@dev:~$ keyctl newring from-others @u
966722684
bob@dev:~$ keyctl setperm %:from-others
0x3f010004
```

CLOUDFLARE

Example: secret sharing

```
alice@dev:~$ id
uid=1001(alice) gid=1001(alice)
groups=1001(alice)
alice@dev:~$ keyctl add user secret
hunter2 @u
791615806
alice@dev:~$ keyctl move %user:secret
@u 966722684
```

```
bob@dev:~$ id
uid=1002(bob) gid=1002(bob)
groups=1002(bob)
bob@dev:~$ keyctl newring from-others @u
966722684
bob@dev:~$ keyctl setperm %:from-others
0x3f010004
bob@dev:~$ keyctl print %user:secret
hunter2
```

CLOUDFLARE

Example: secret sharing

```
alice@dev:~$ id
uid=1001(alice) gid=1001(alice)
groups=1001(alice)
alice@dev:~$ keyctl add user secret
hunter2 @u
791615806
alice@dev:~$ keyctl move %user:secret
@u 966722684
```

```
bob@dev:~$ id
uid=1002(bob) gid=1002(bob)
groups=1002(bob)
bob@dev:~$ keyctl newring from-others @u
966722684
bob@dev:~$ keyctl setperm %:from-others
0x3f010004
bob@dev:~$ keyctl print %user:secret
hunter2
bob@dev:~$ keyctl show @u
Keyring
 812825228 --alswrv    1002 65534
keyring: _uid.1002
 966722684 --alswrv    1002  1002    \_
keyring: from-others
 791615806 --alswrv    1001  1001
\_ user: secret
```

CLOUDFLARE

Example: secret sharing

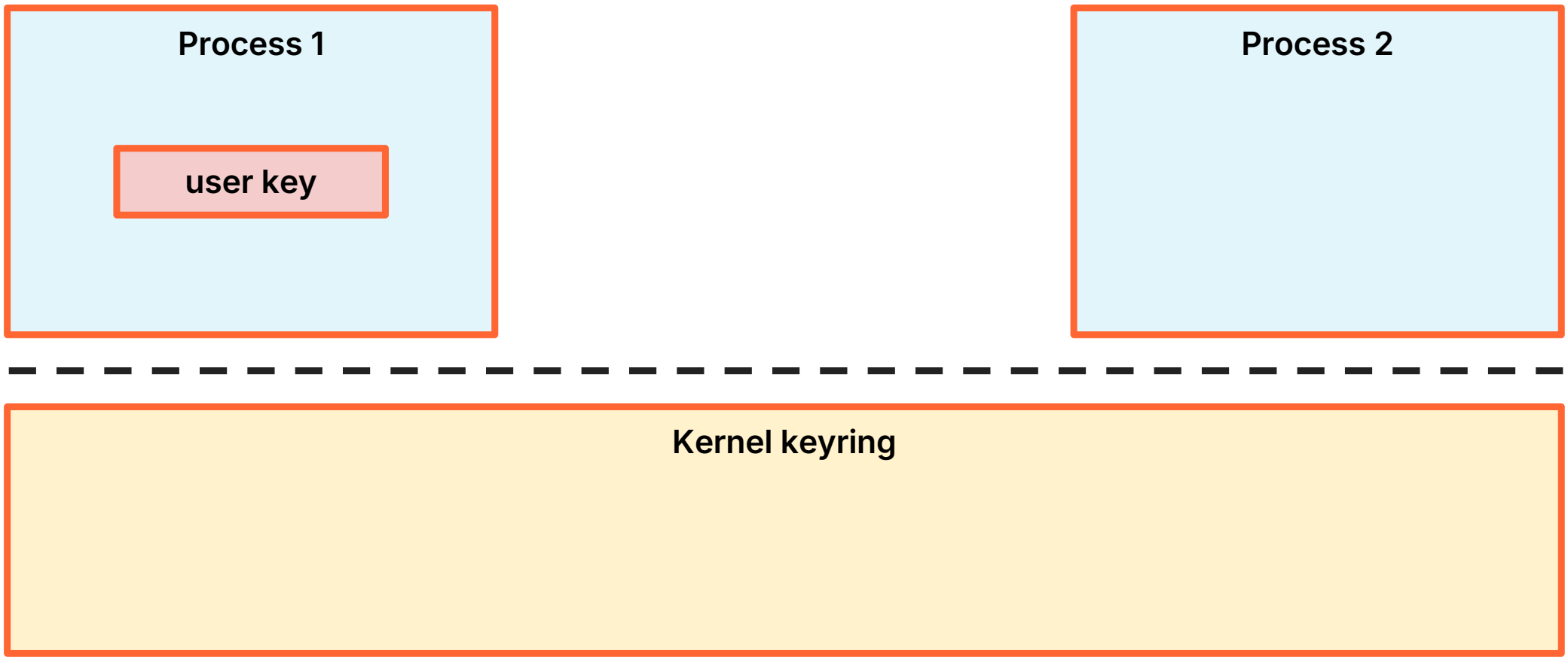
```
alice@dev:~$ id
uid=1001(alice) gid=1001(alice)
groups=1001(alice)
alice@dev:~$ keyctl add user secret
hunter2 @u
791615806
alice@dev:~$ keyctl move %user:secret
@u 966722684
alice@dev:~$ keyctl show
Session Keyring
 931561702 --alswrv   1001  1001
keyring: _ses
 107607516 --alswrv   1001 65534   \_
keyring: _uid.1001
```

```
bob@dev:~$ id
uid=1002(bob) gid=1002(bob)
groups=1002(bob)
bob@dev:~$ keyctl newring from-others @u
966722684
bob@dev:~$ keyctl setperm %:from-others
0x3f010004
bob@dev:~$ keyctl print %user:secret
hunter2
bob@dev:~$ keyctl show @u
Keyring
 812825228 --alswrv   1002 65534
keyring: _uid.1002
 966722684 --alswrv   1002  1002   \_
keyring: from-others
 791615806 --alswrv   1001  1001
\_ user: secret
```

@ignatkn

CLOUDFLARE

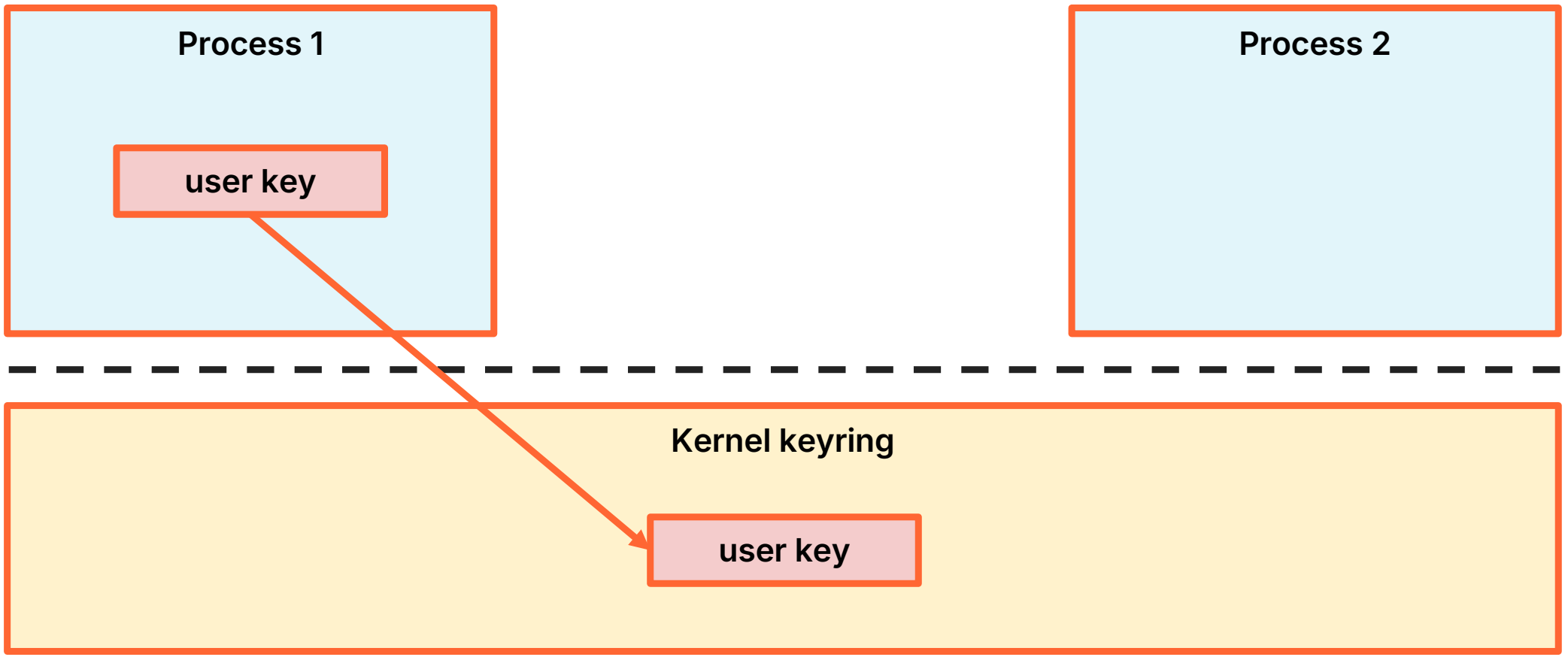
User keys



@ignatkn

CLOUDFLARE

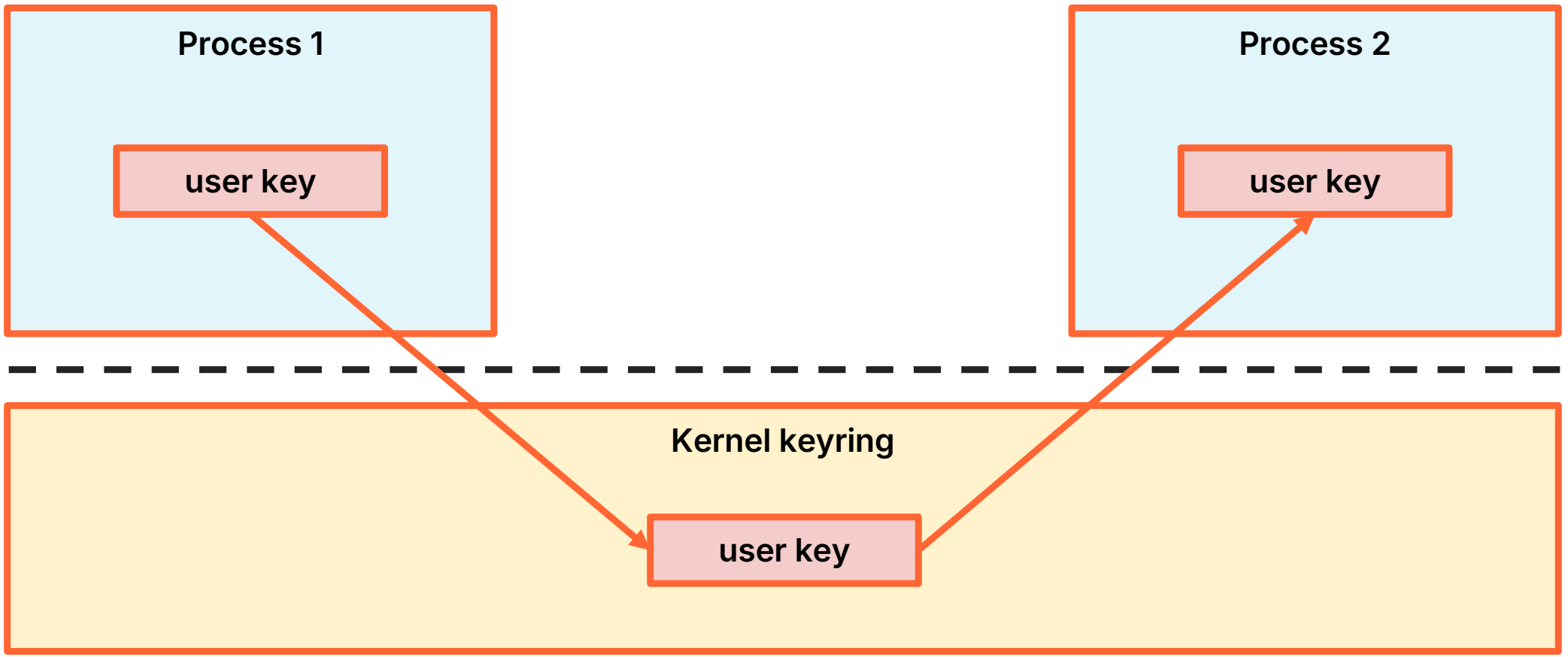
User keys



@ignatkn

CLOUDFLARE

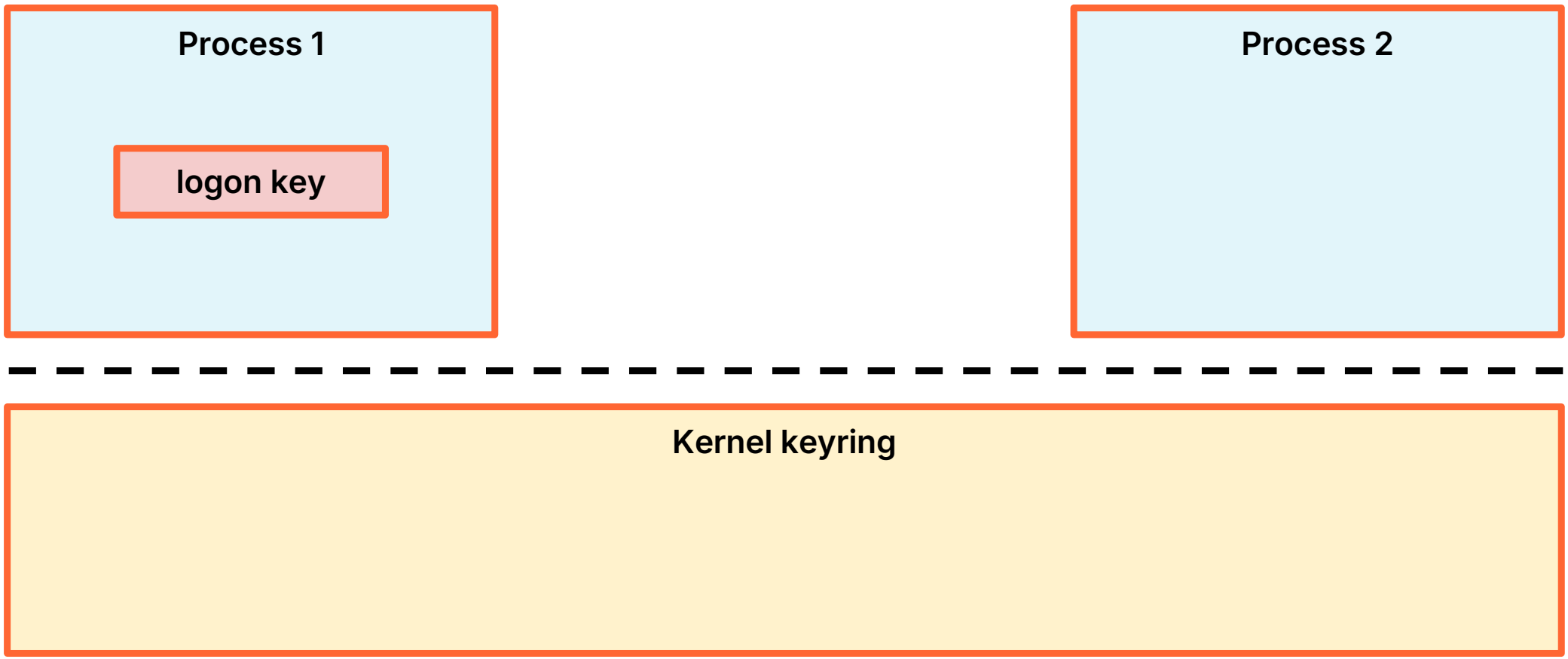
User keys



@ignatkn

CLOUDFLARE

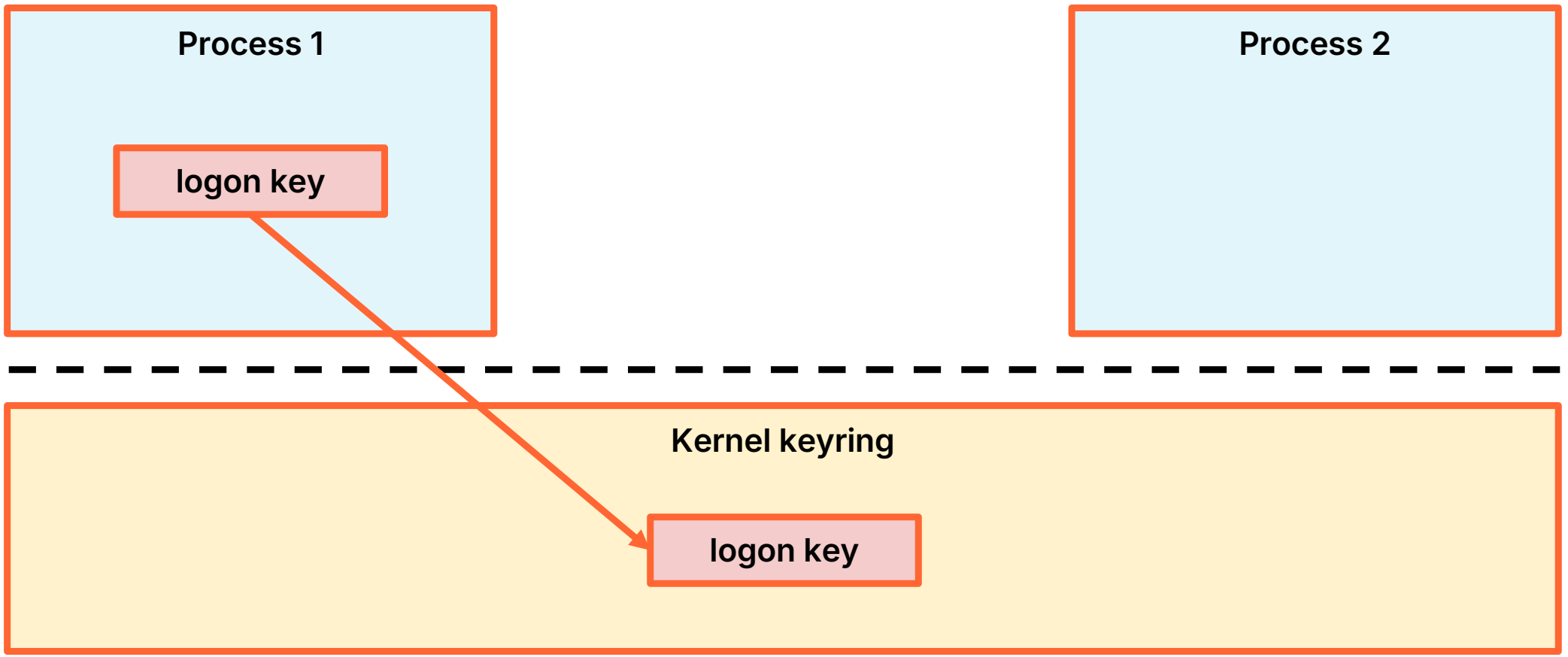
Logon keys



@ignatkn

CLOUDFLARE

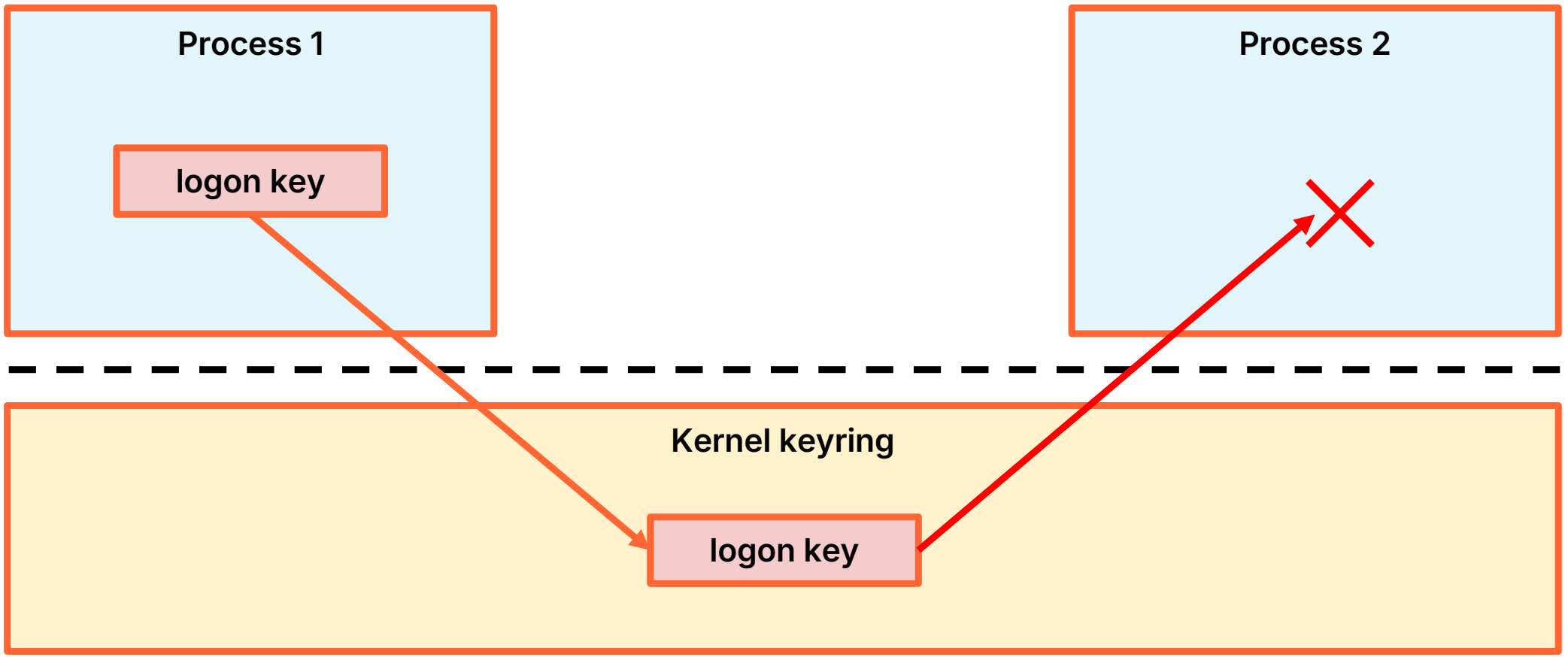
Logon keys



@ignatkn

CLOUDFLARE

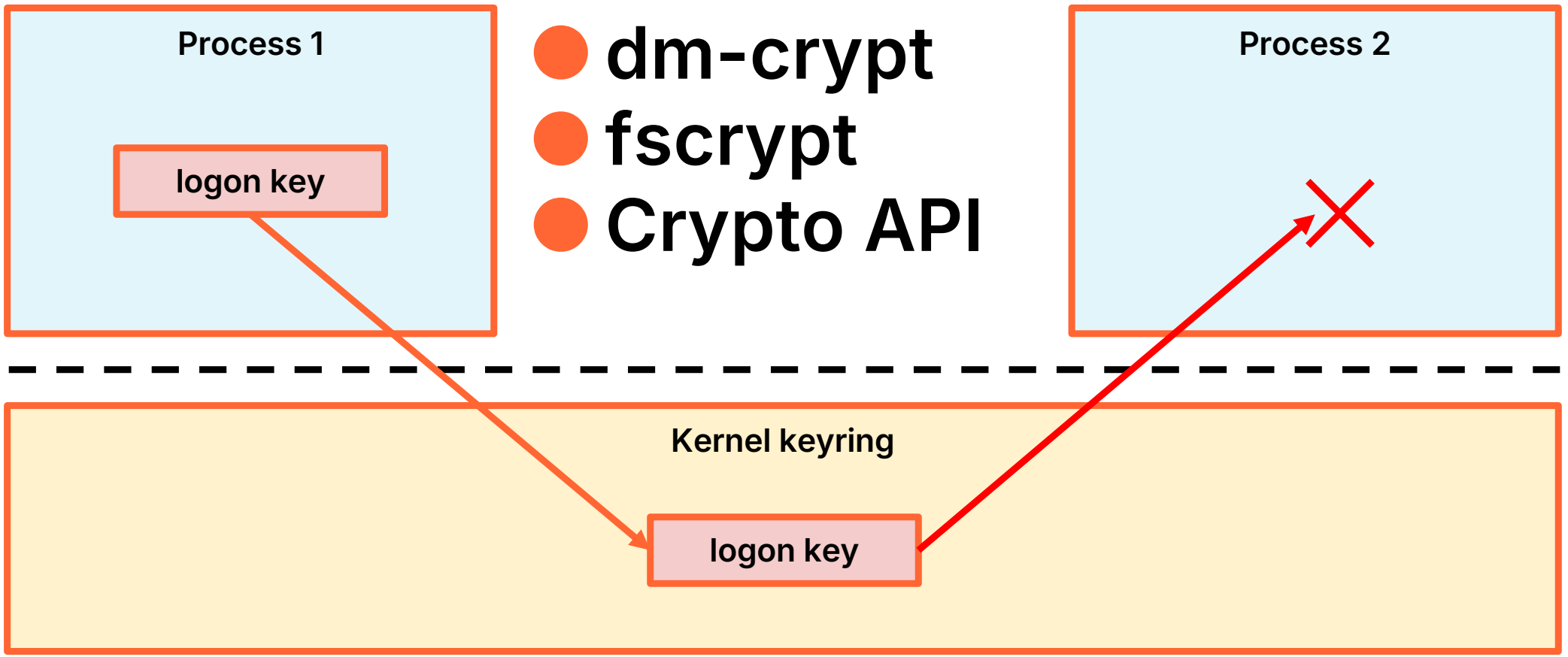
Logon keys



@ignatkn

CLOUDFLARE

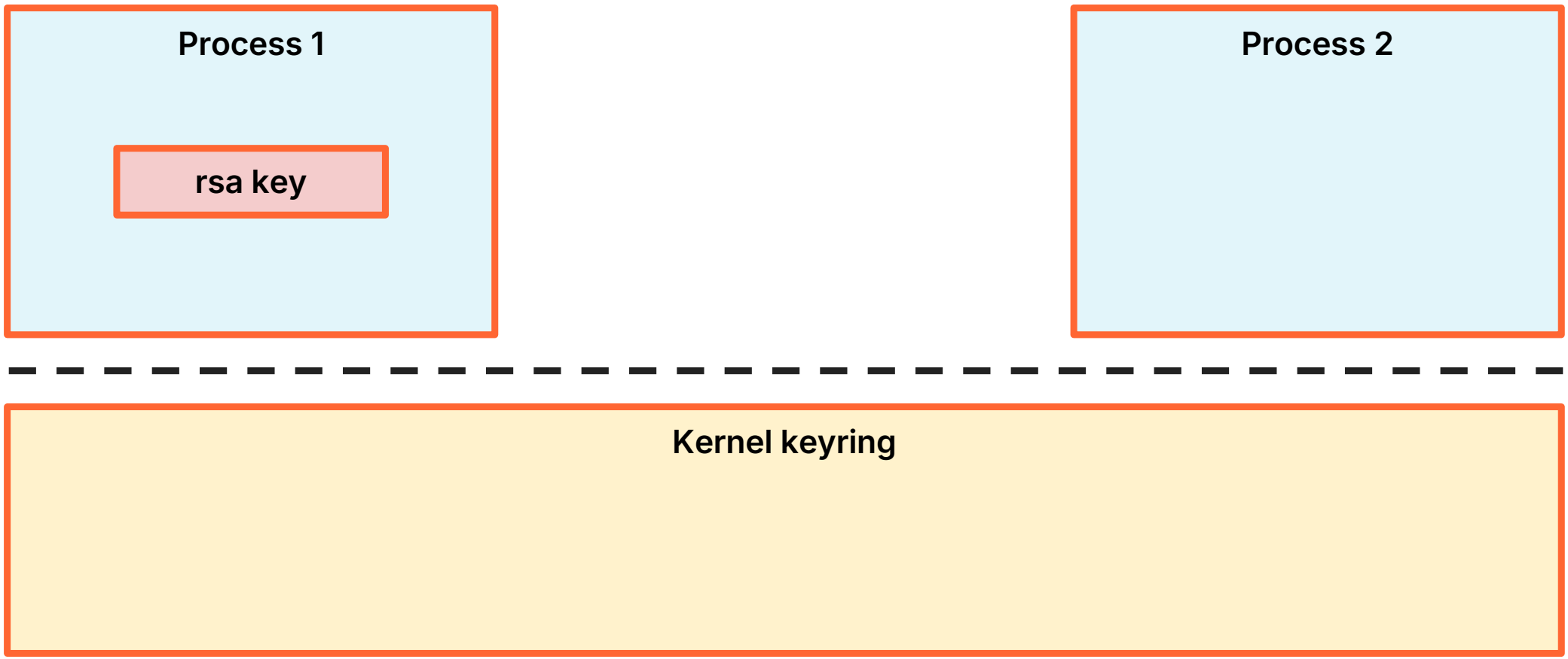
Logon keys



@ignatkn

CLOUDFLARE

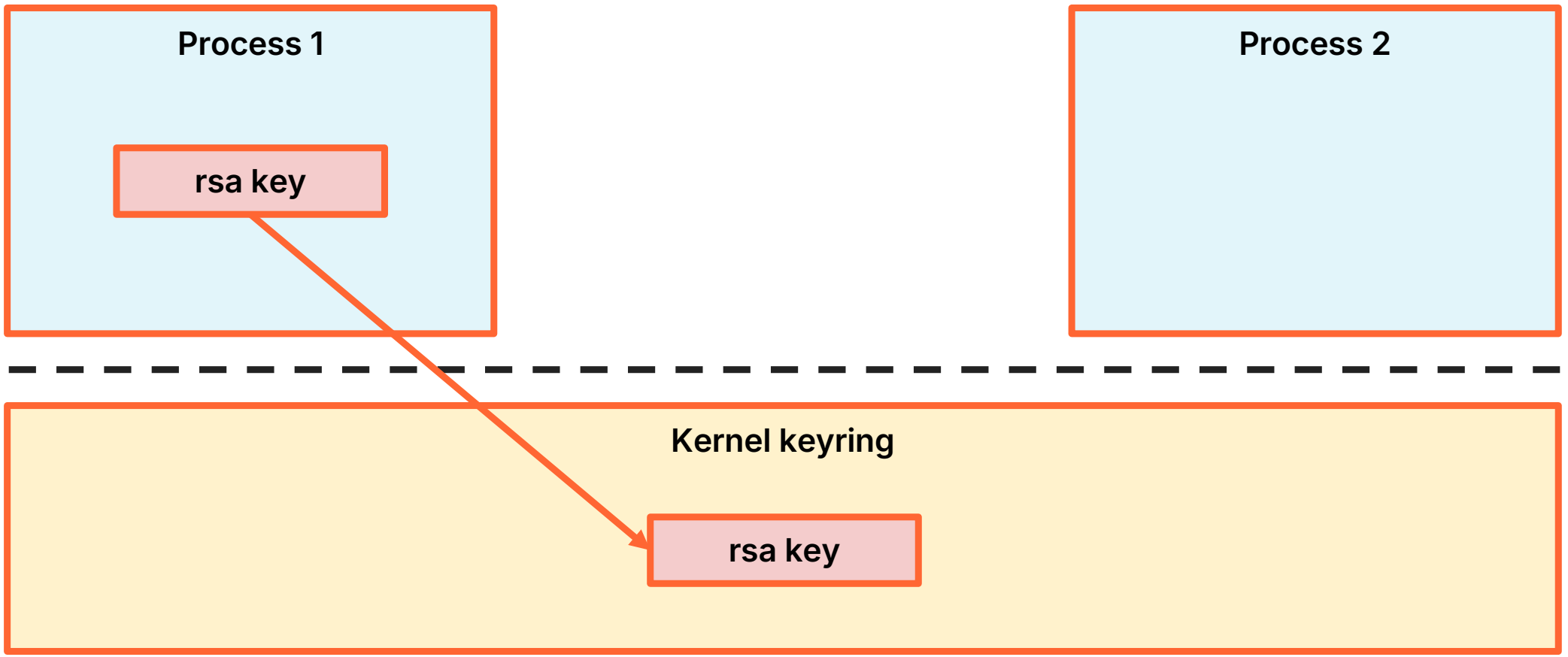
Asymmetric keys



@ignatkn

CLOUDFLARE

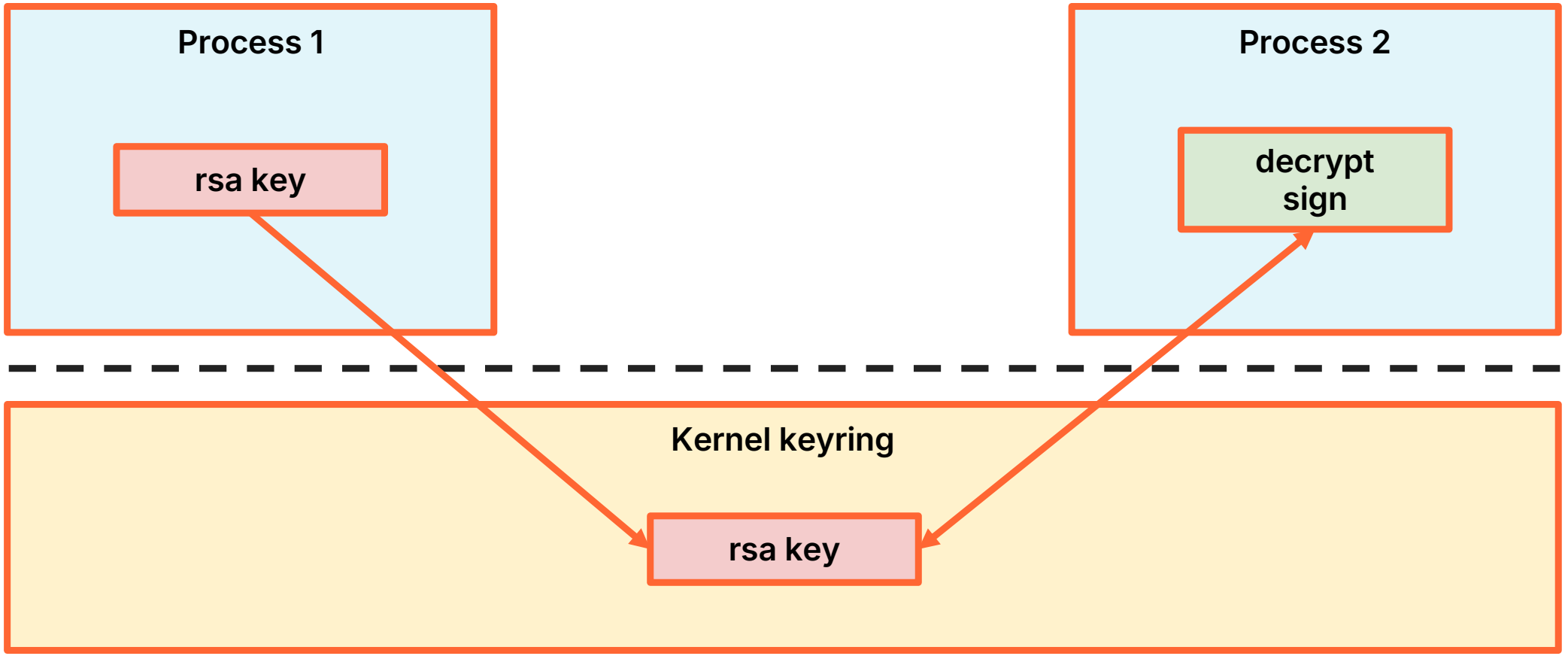
Asymmetric keys



@ignatkn

CLOUDFLARE

Asymmetric keys



@ignatkn

CLOUDFLARE

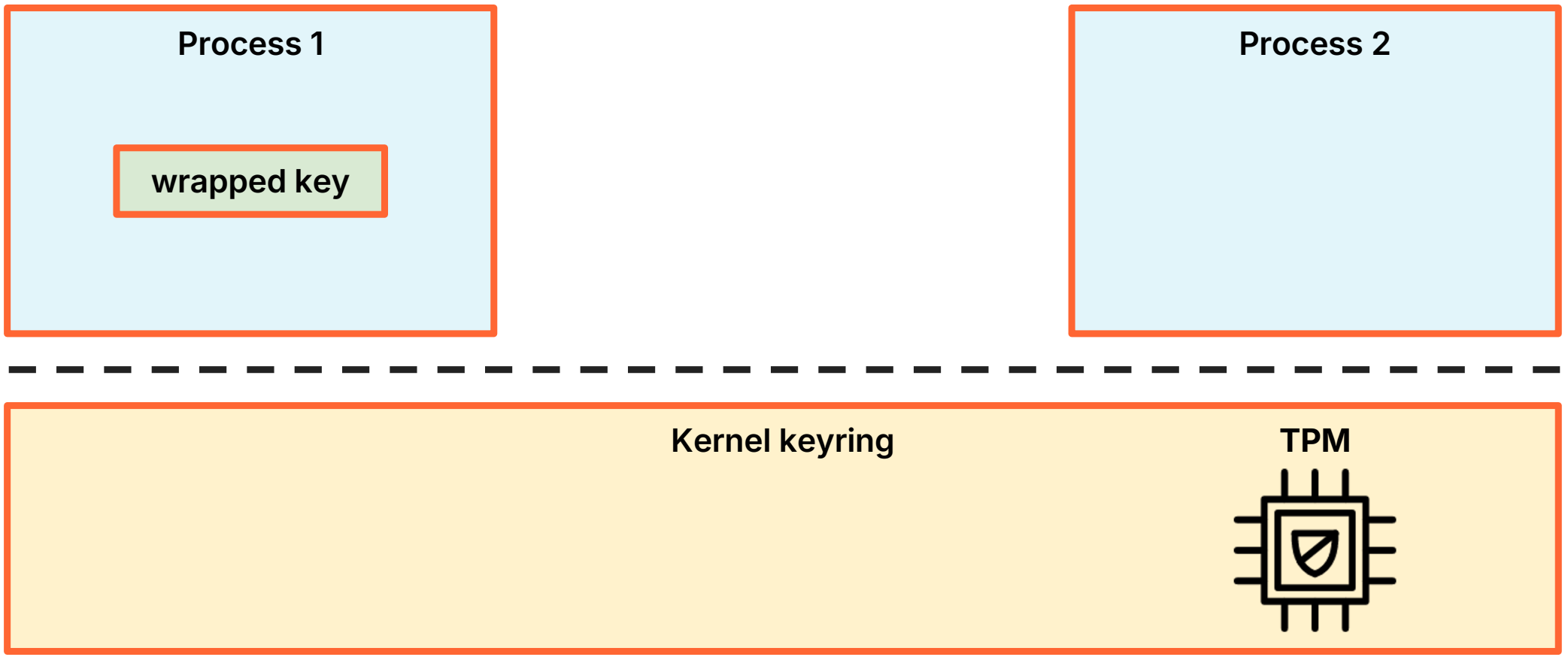
Linux keystore and TPMs

Better together?

@ignatkn

CLOUDFLARE

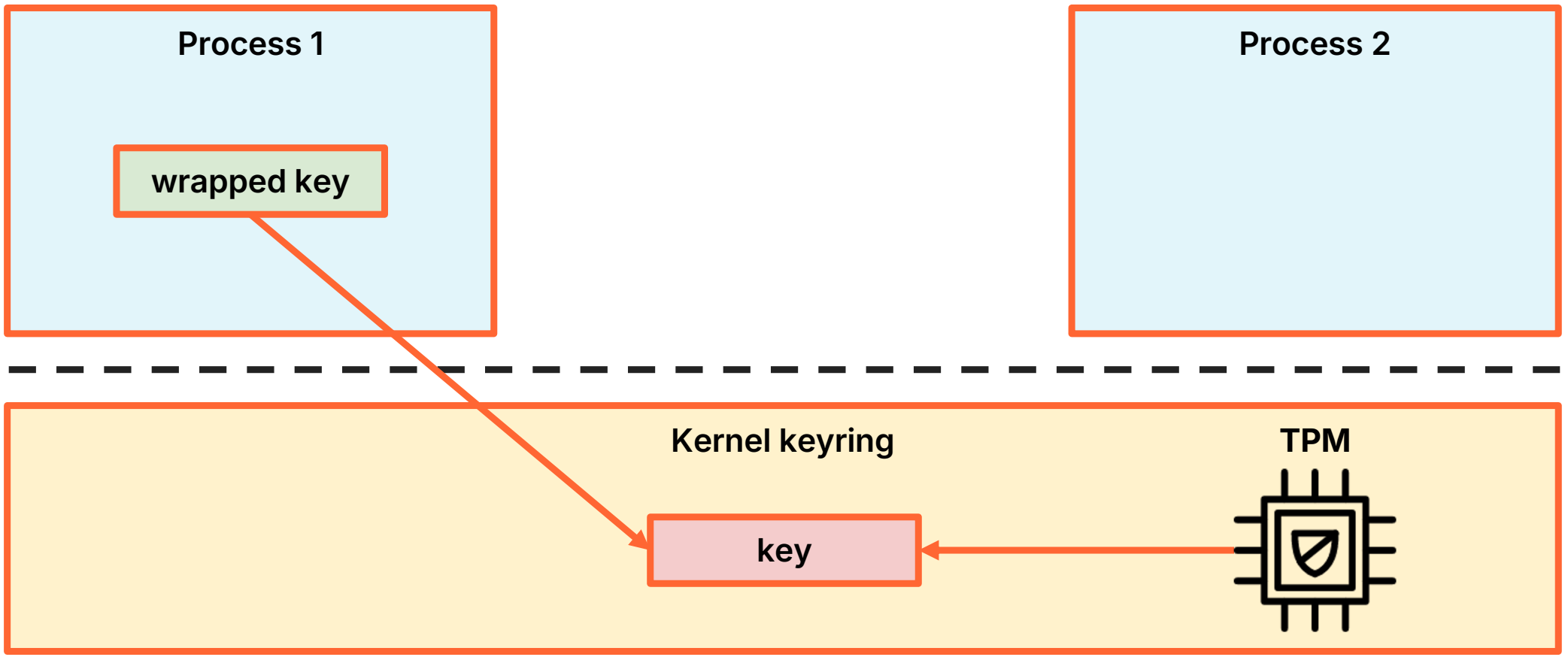
Trusted keys



@ignatkn

CLOUDFLARE

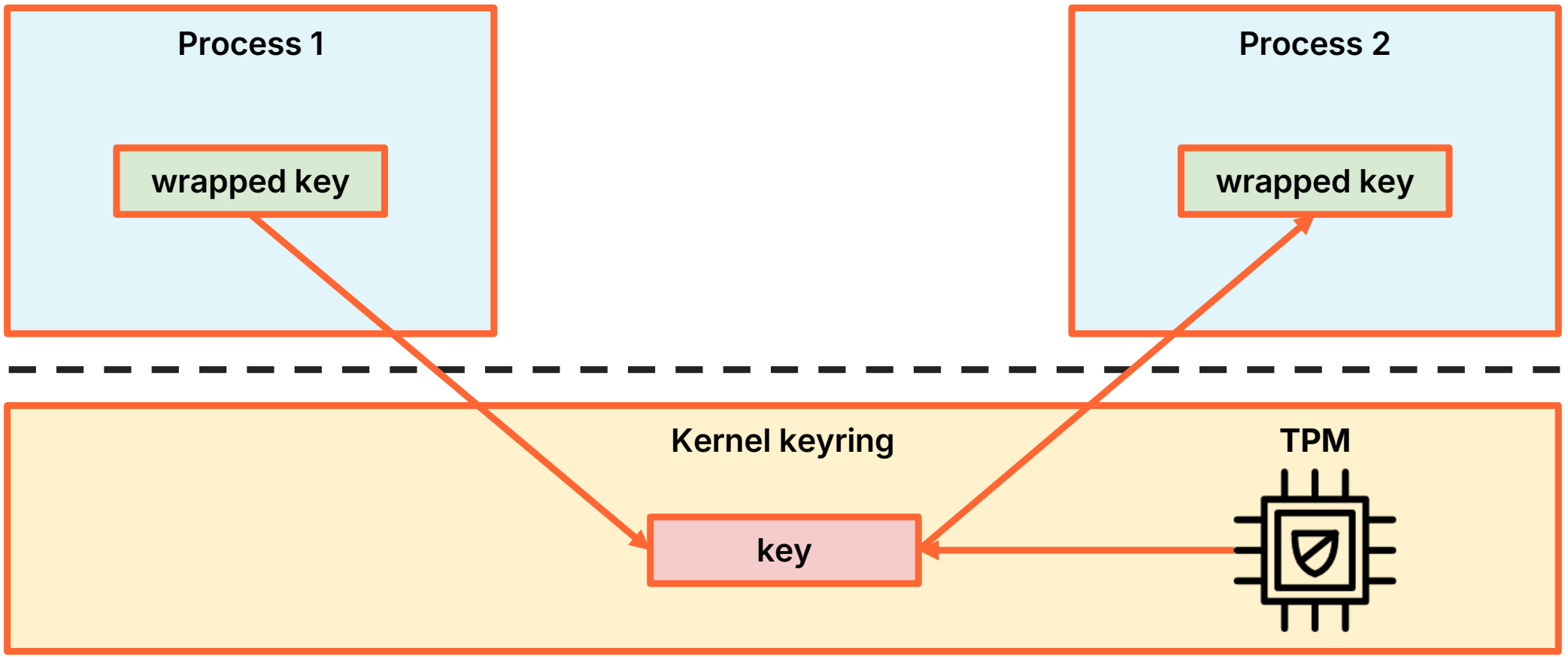
Trusted keys



@ignatkn

CLOUDFLARE

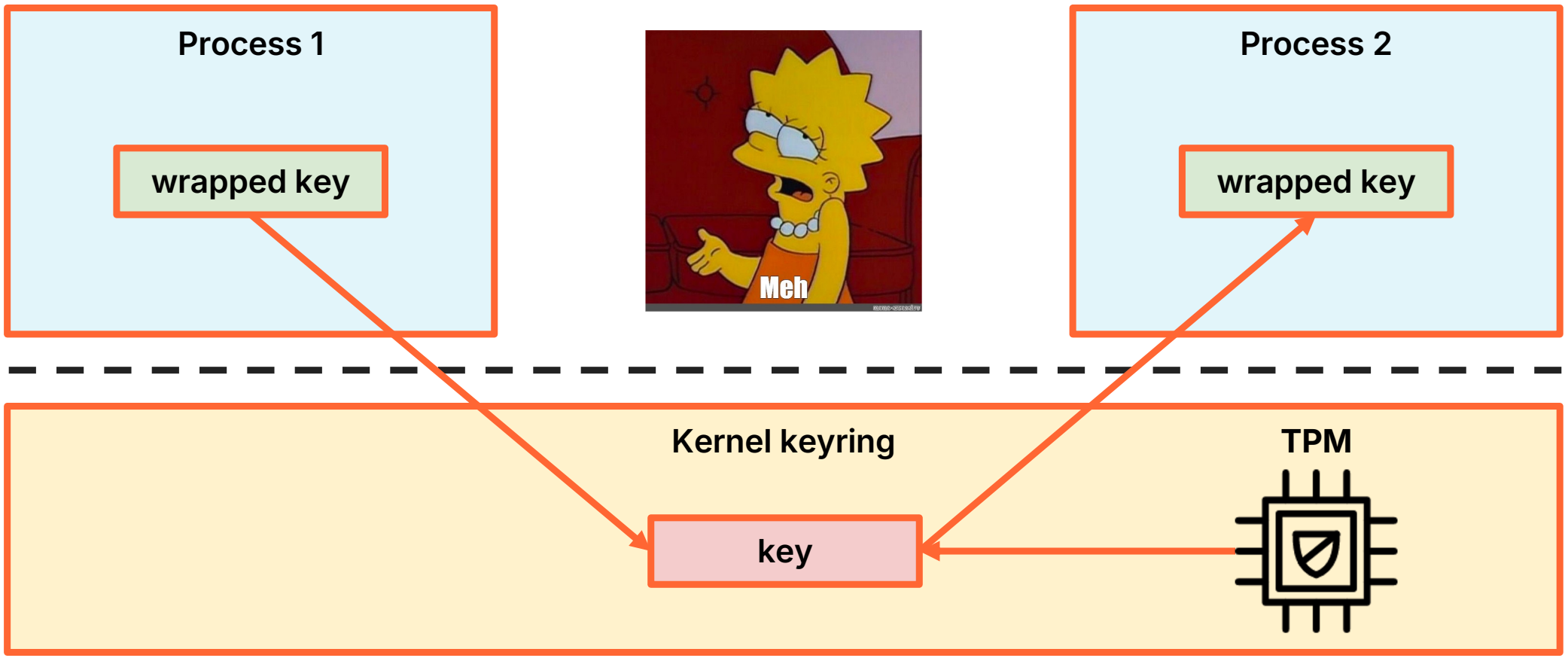
Trusted keys



@ignatkn

CLOUDFLARE

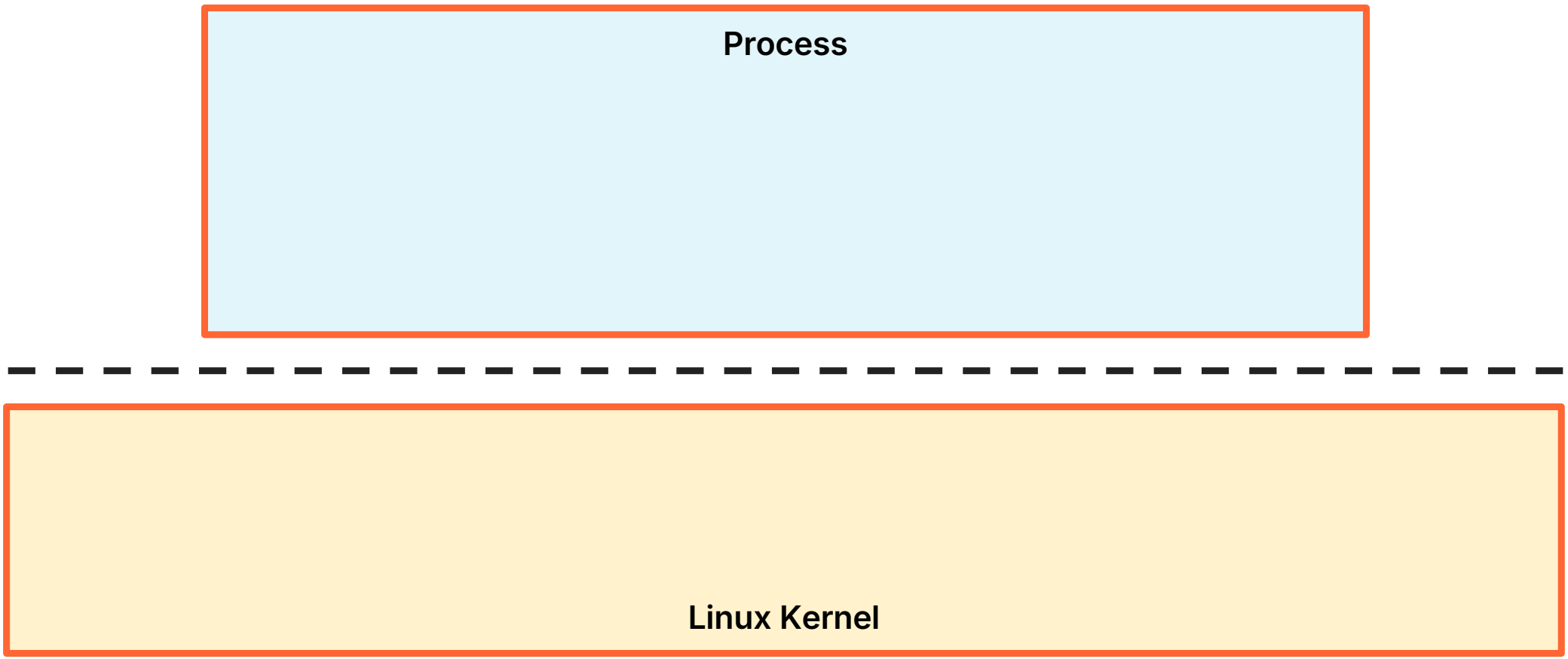
Trusted keys



@ignatkn

CLOUDFLARE

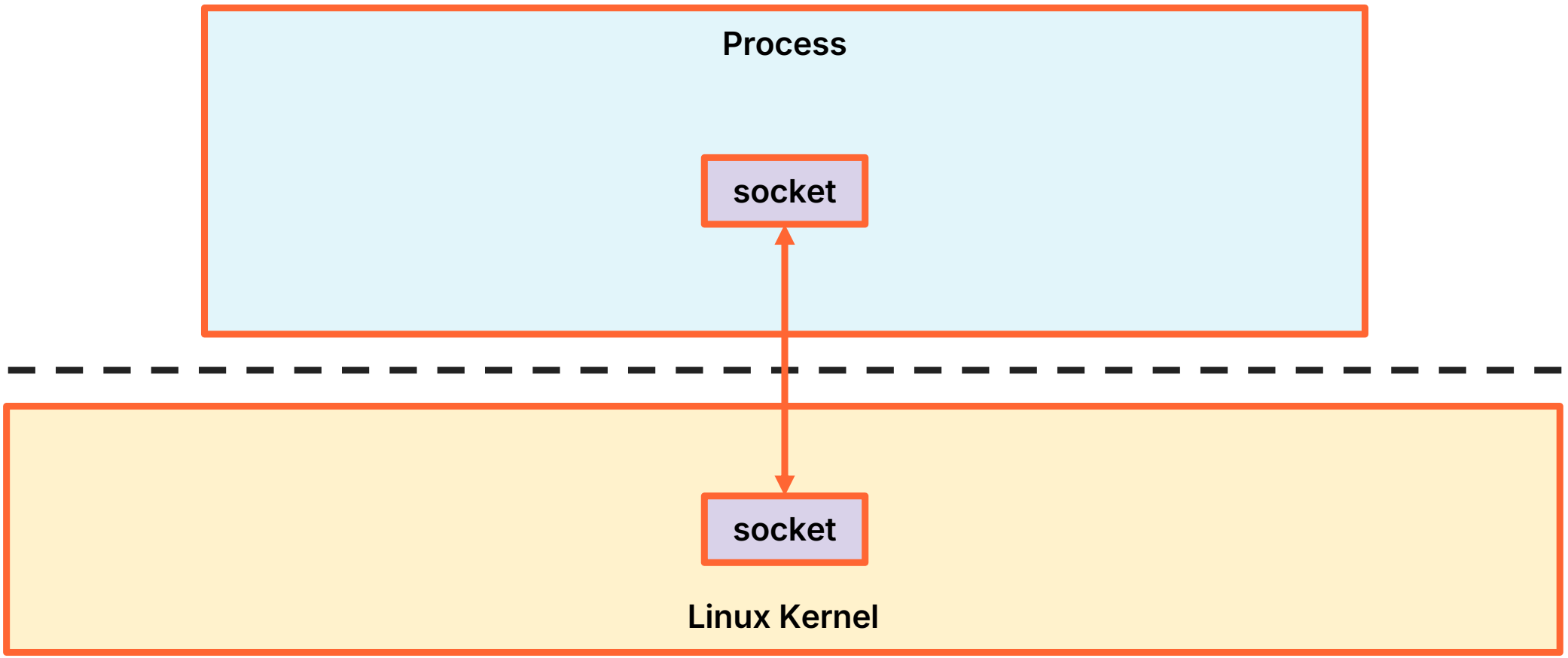
Linux Crypto API



@ignatkn

CLOUDFLARE

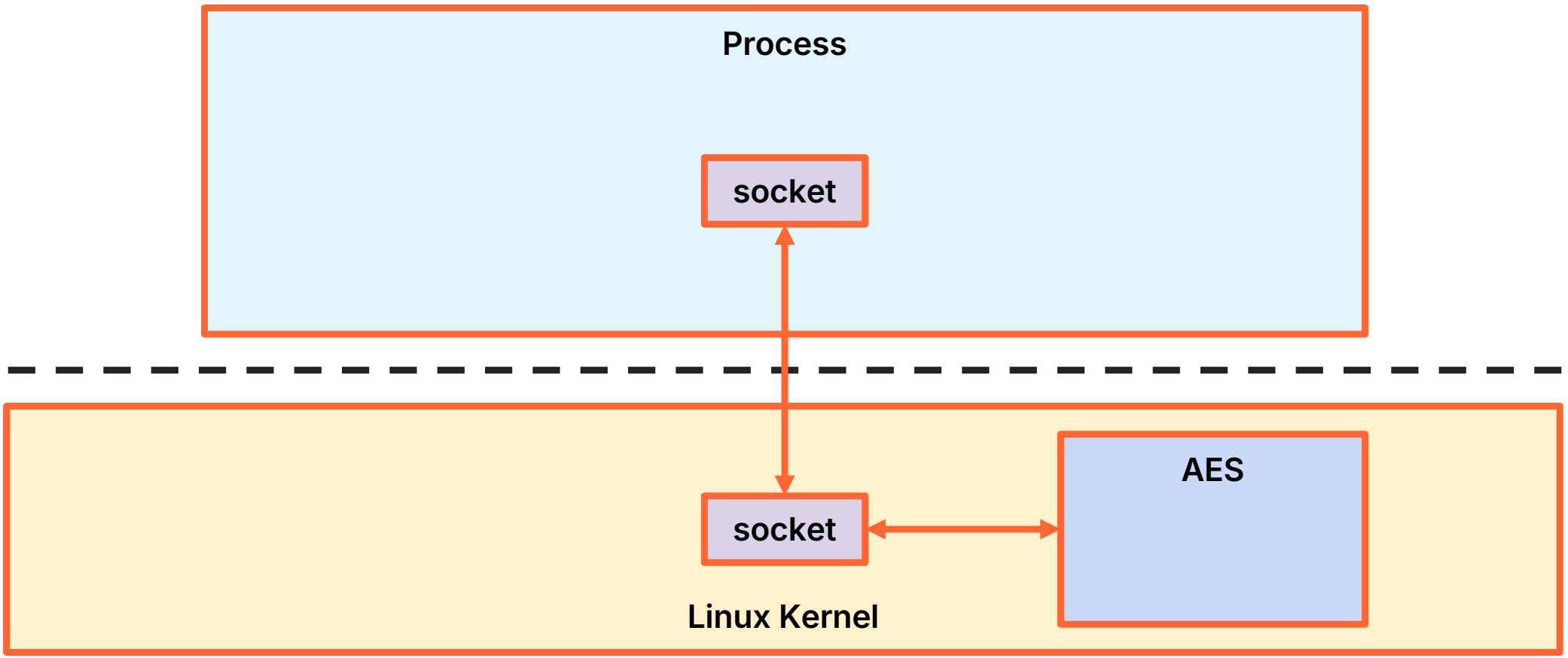
Linux Crypto API



@ignatkn

CLOUDFLARE

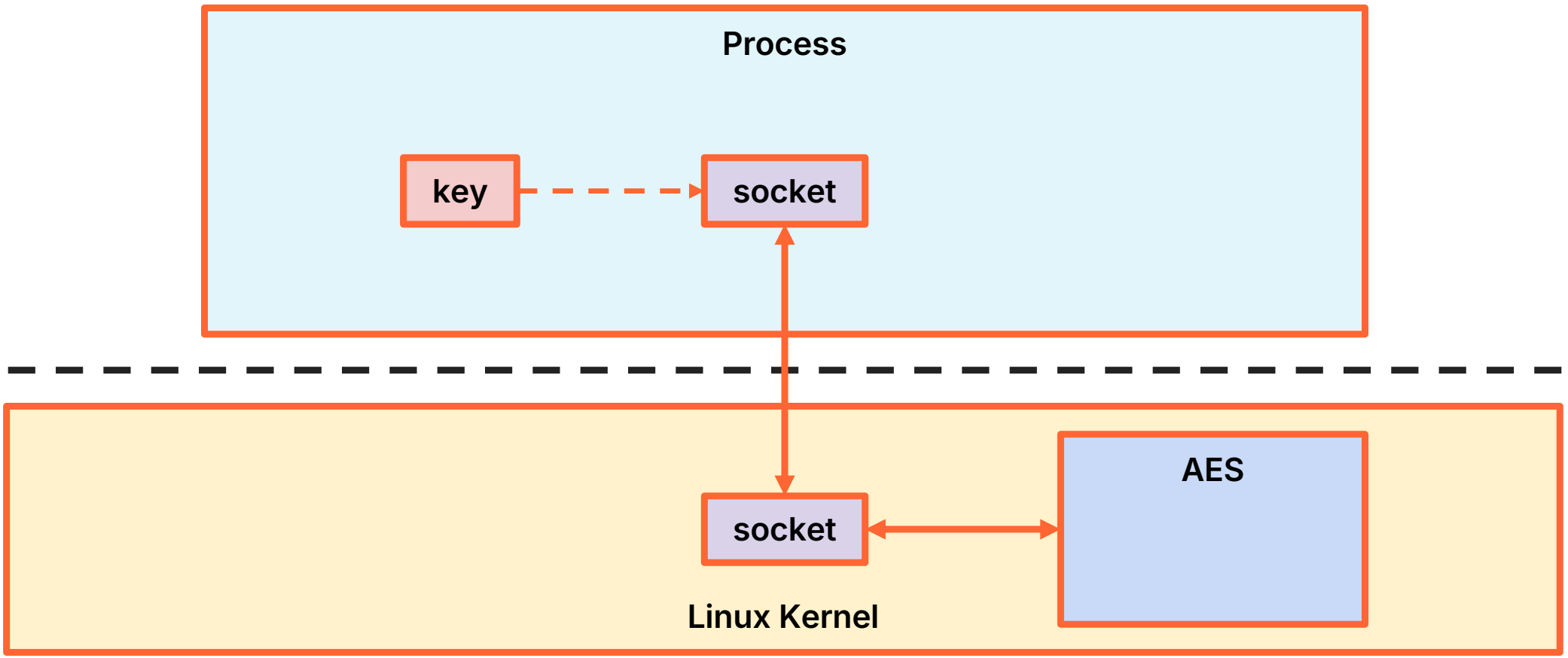
Linux Crypto API



@ignatkn

CLOUDFLARE

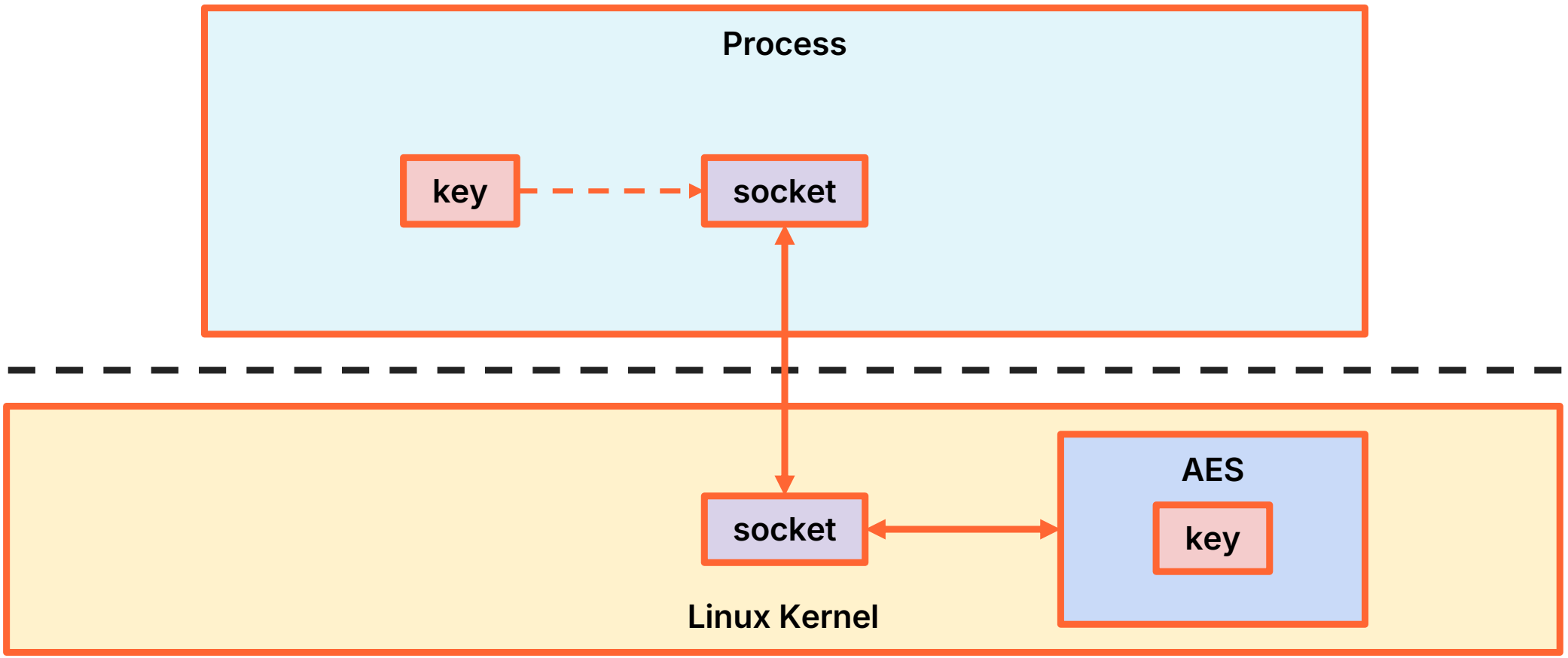
Linux Crypto API



@ignatkn

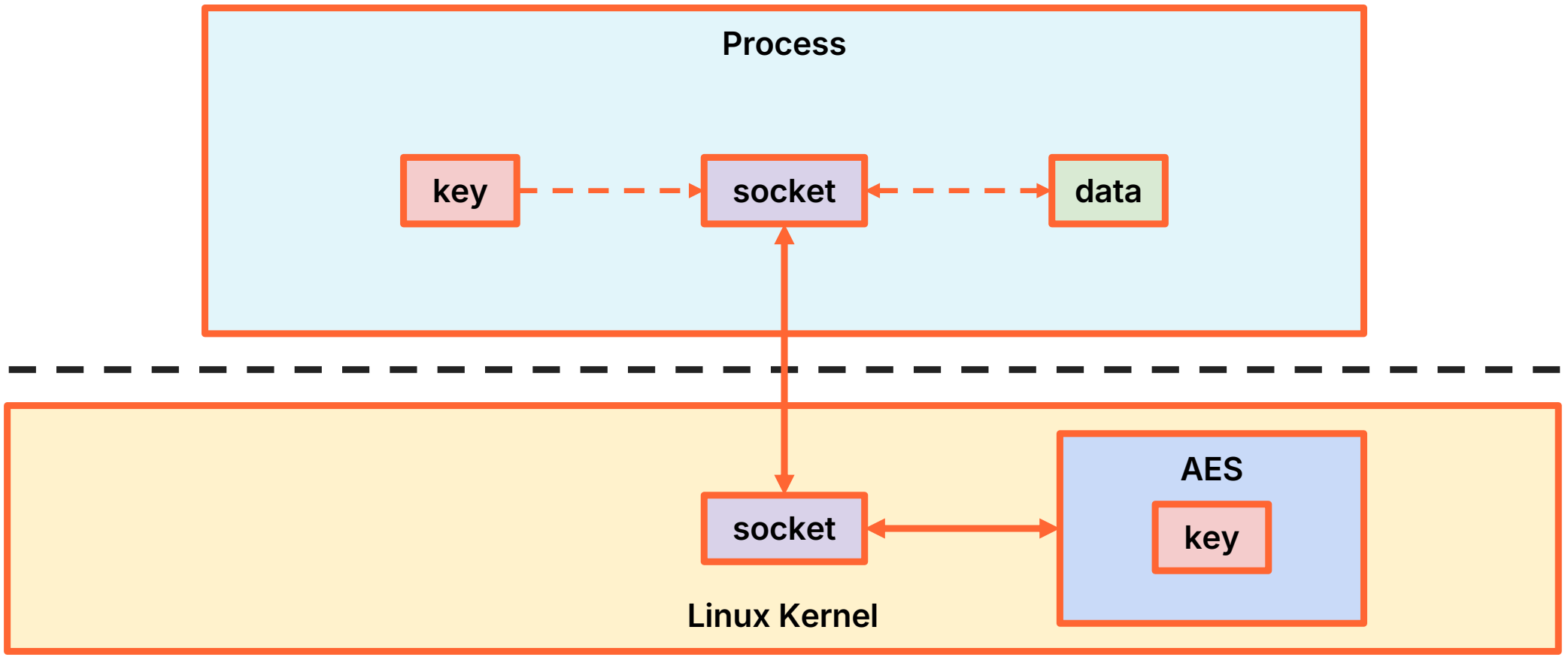
CLOUDFLARE

Linux Crypto API



CLOUDFLARE

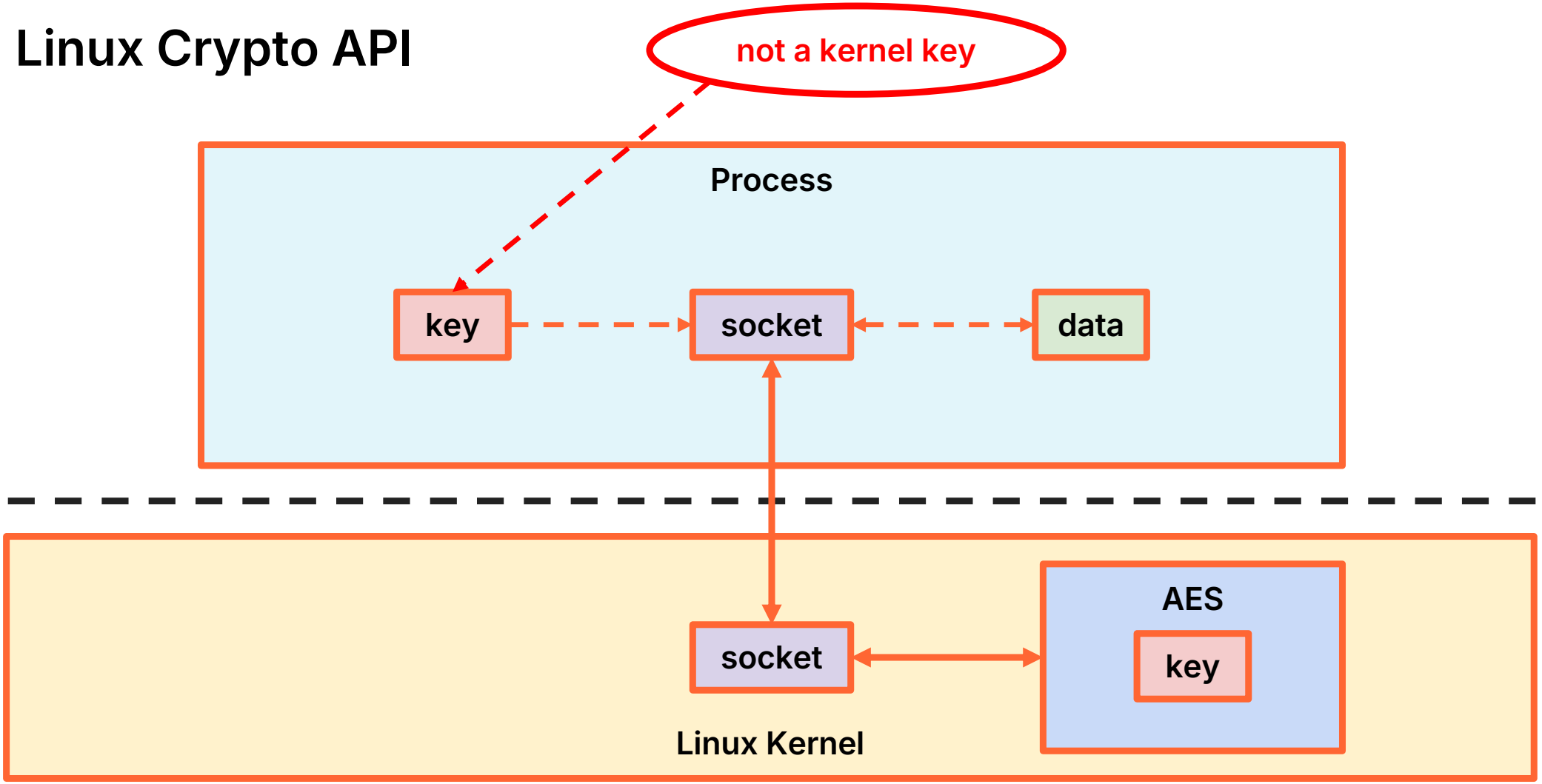
Linux Crypto API



@ignatkn

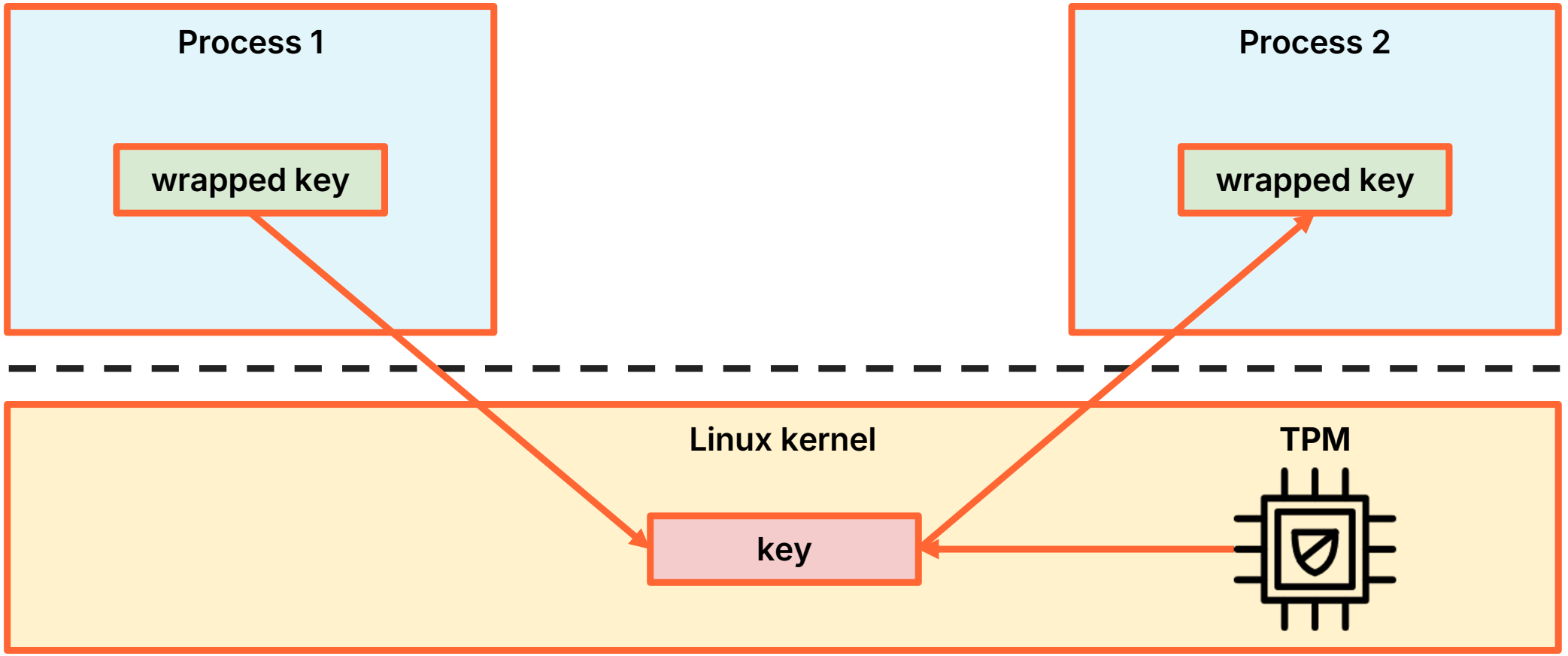
CLOUDFLARE

Linux Crypto API



CLOUDFLARE

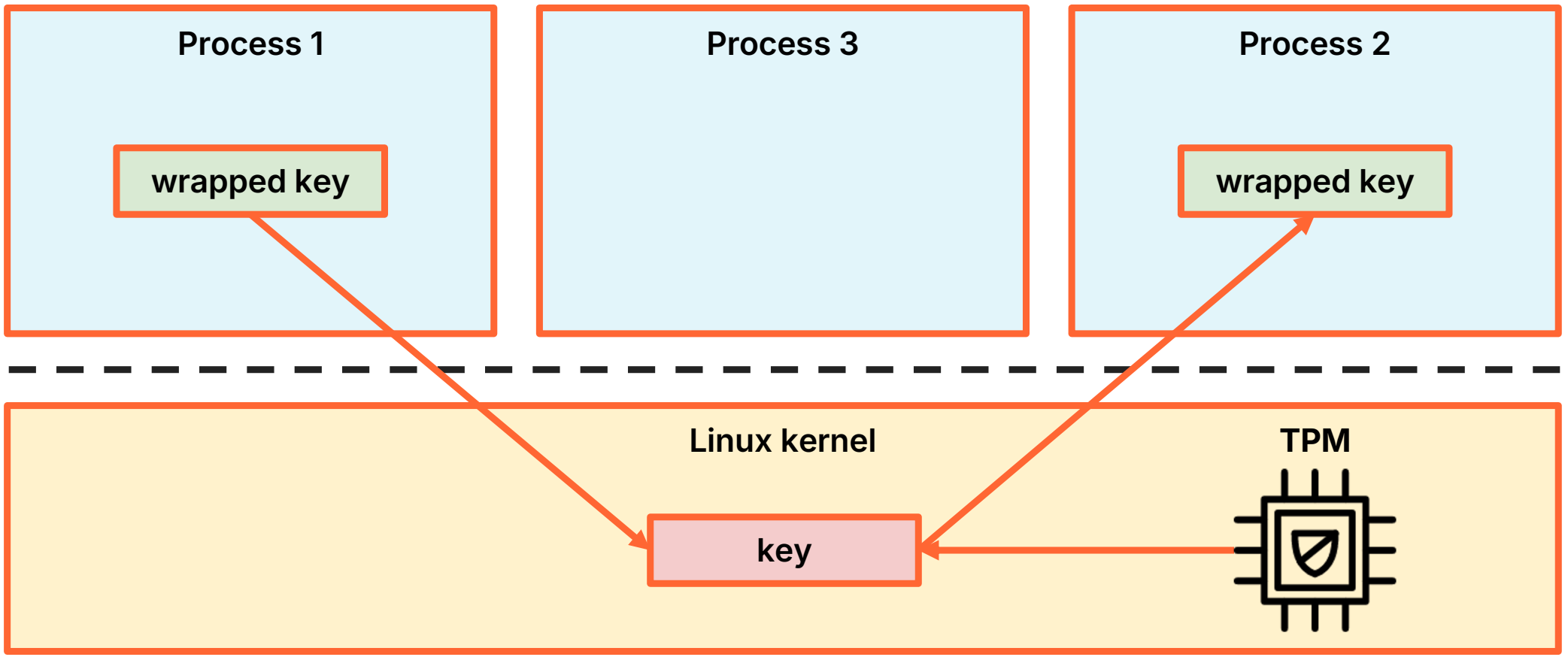
Key usage from applications



@ignatkn

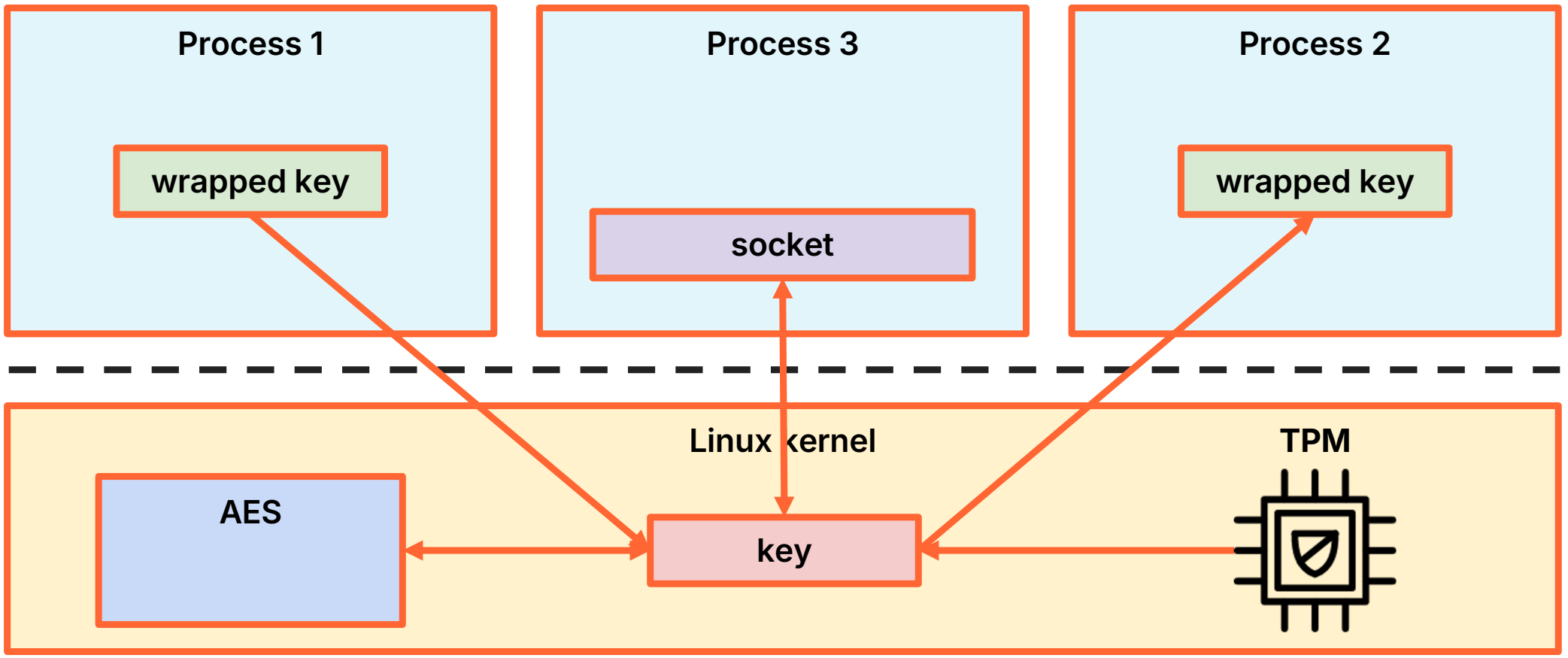
CLOUDFLARE

Key usage from applications



CLOUDFLARE

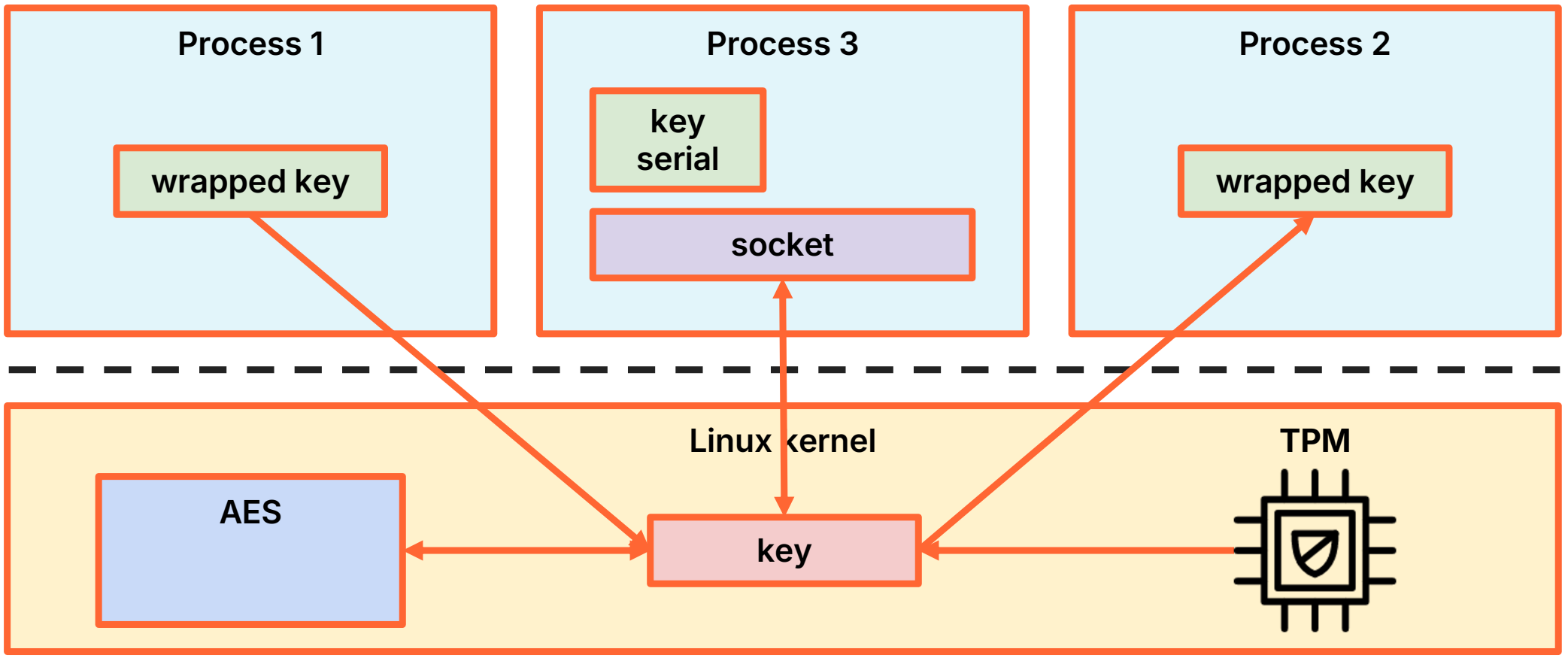
Key usage from applications



@ignatkn

CLOUDFLARE

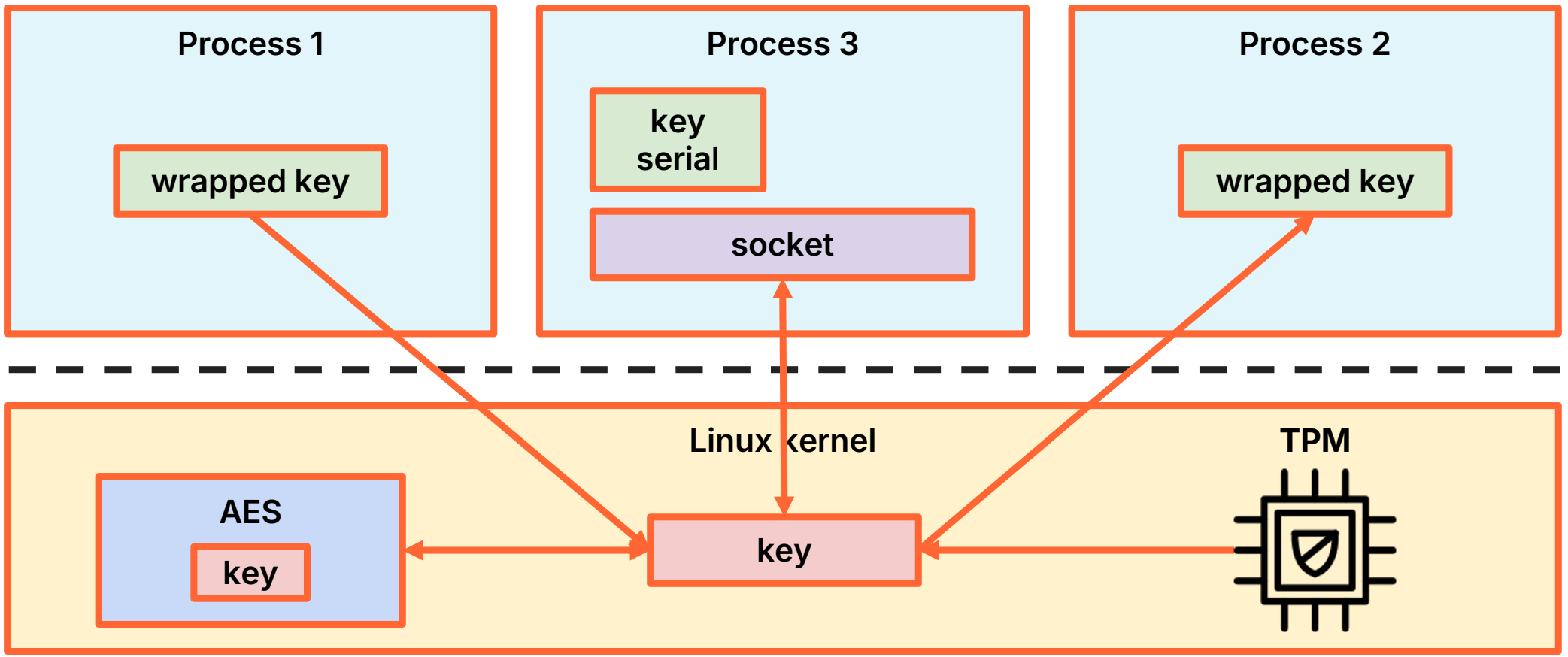
Key usage from applications



@ignatkn

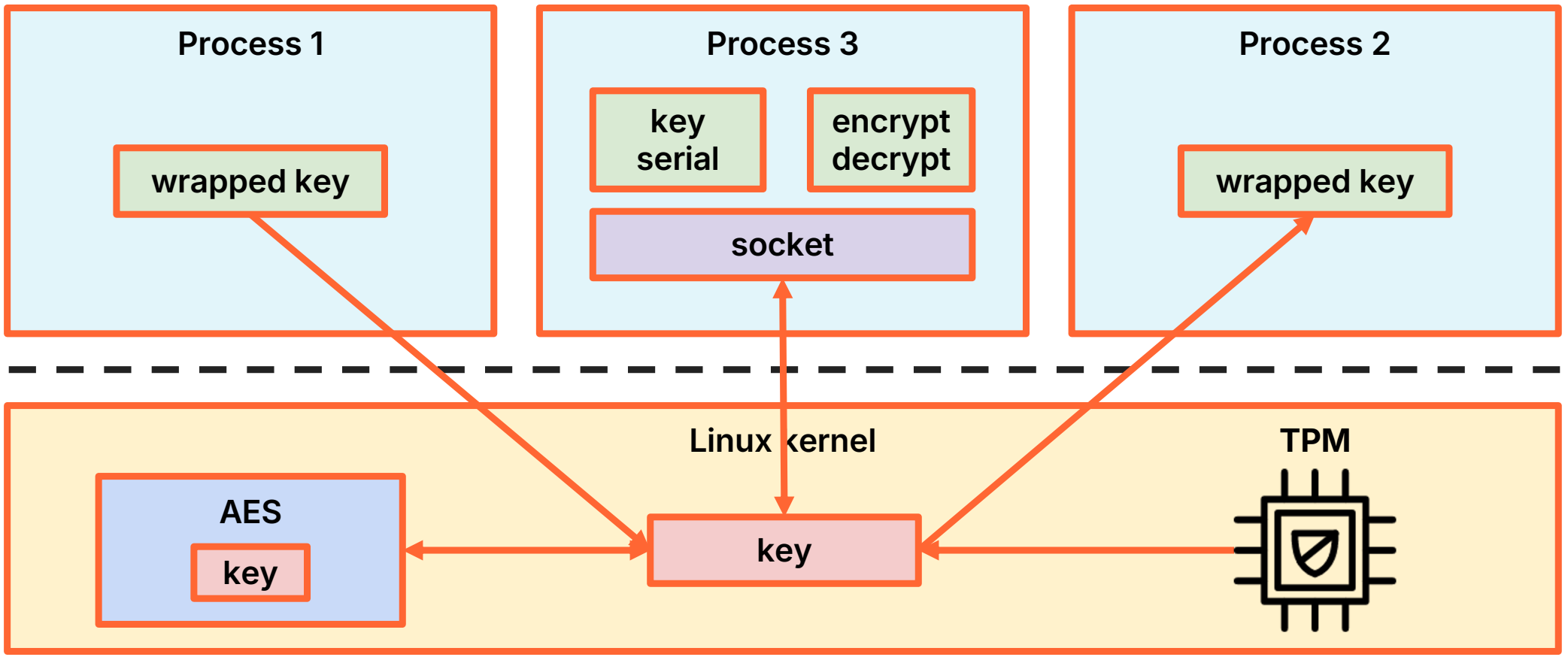
CLOUDFLARE

Key usage from applications



CLOUDFLARE

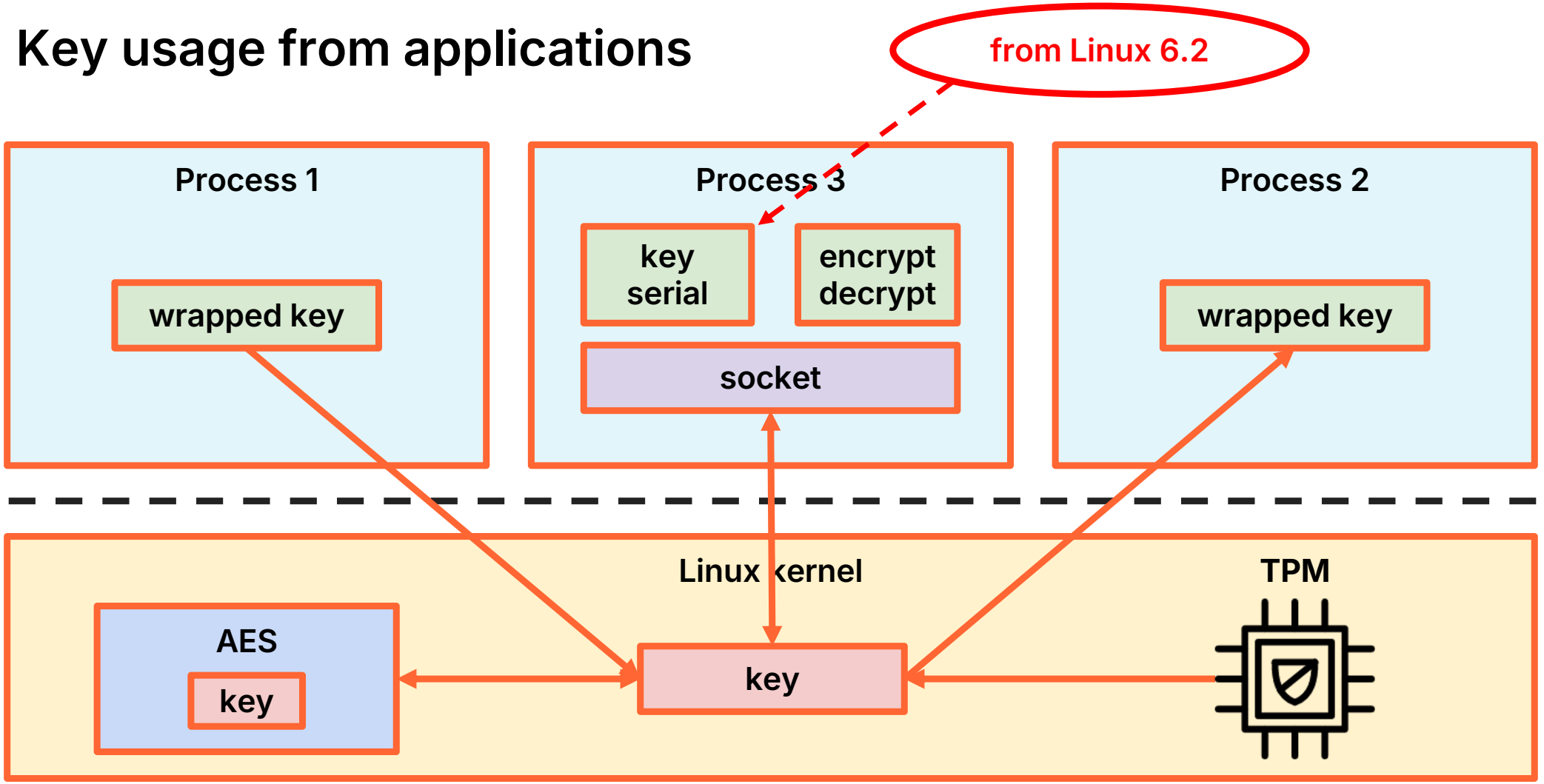
Key usage from applications



@ignatkn

CLOUDFLARE

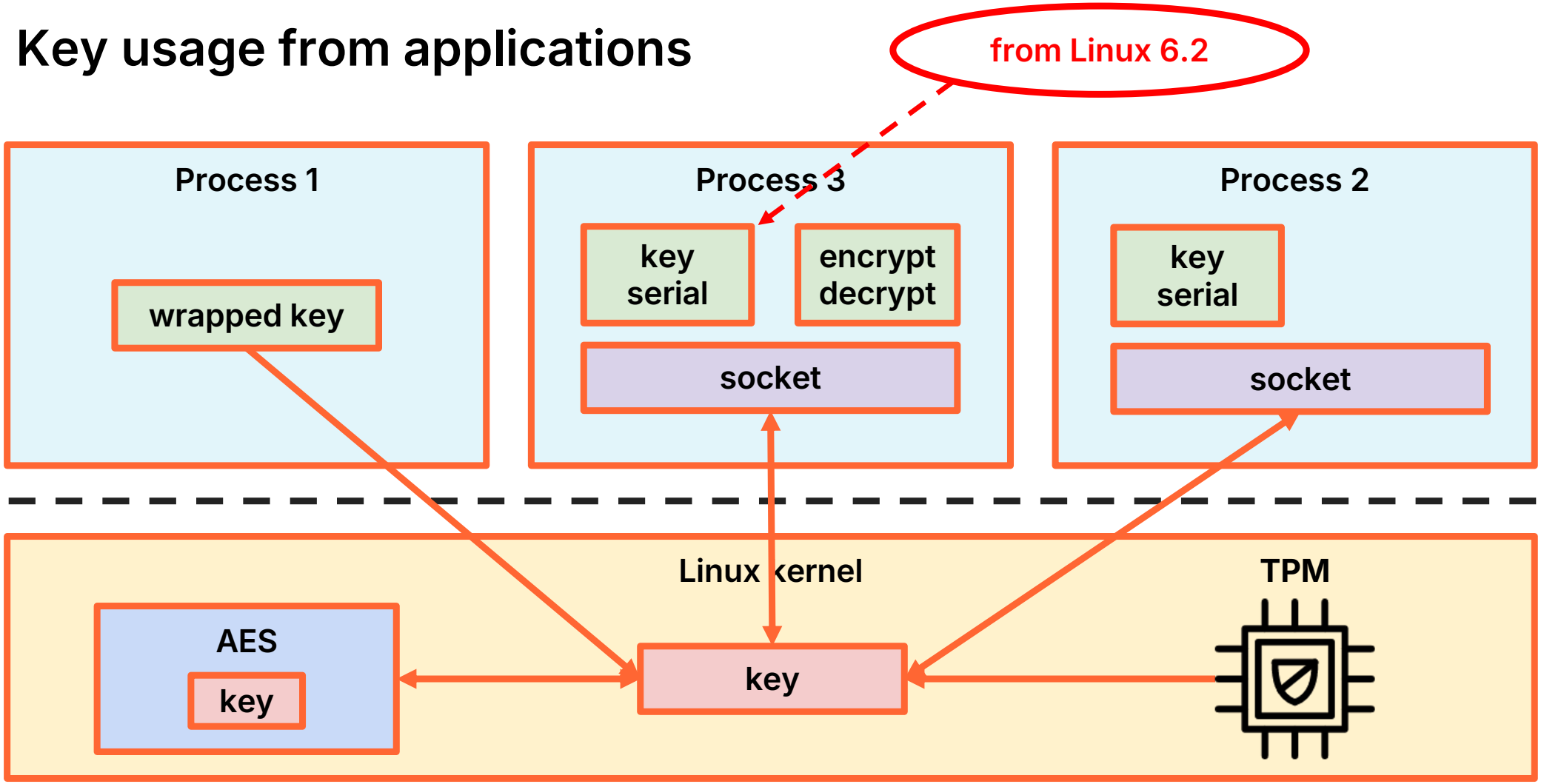
Key usage from applications



@ignatkn

CLOUDFLARE

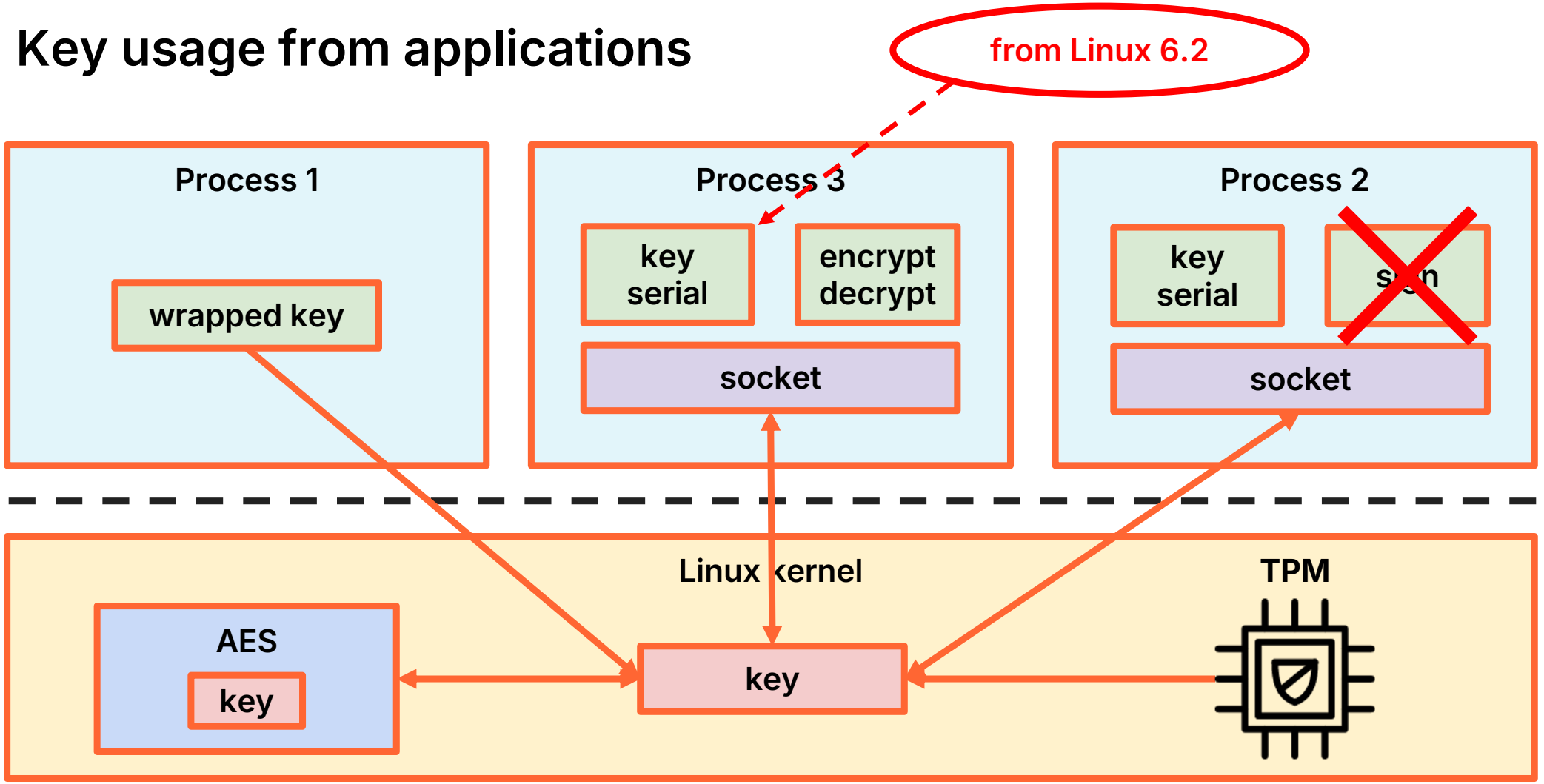
Key usage from applications



@ignatkn

CLOUDFLARE

Key usage from applications



CLOUDFLARE

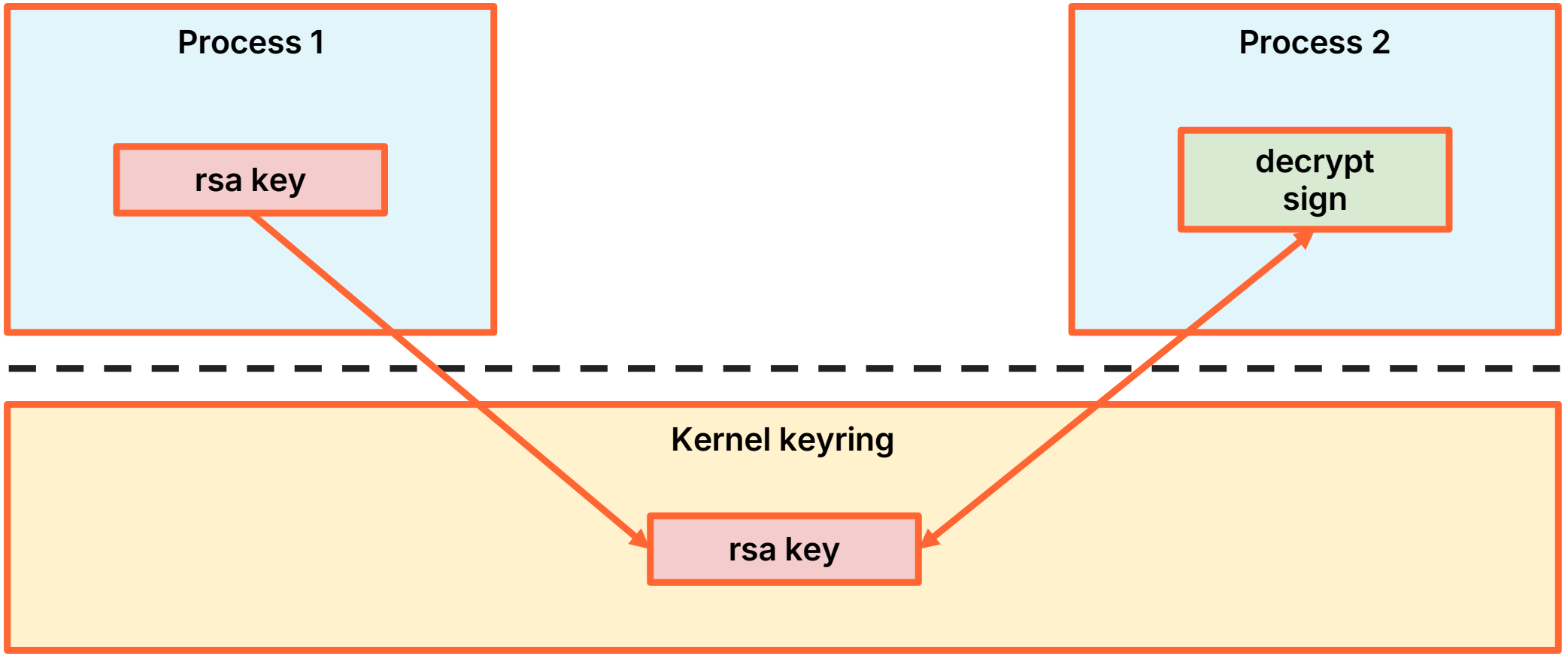
Asymmetric TPM keys

https://lore.kernel.org/lkml/20240528210823.28798-2-jarkko@kernel.org/T/

@ignatkn

CLOUDFLARE

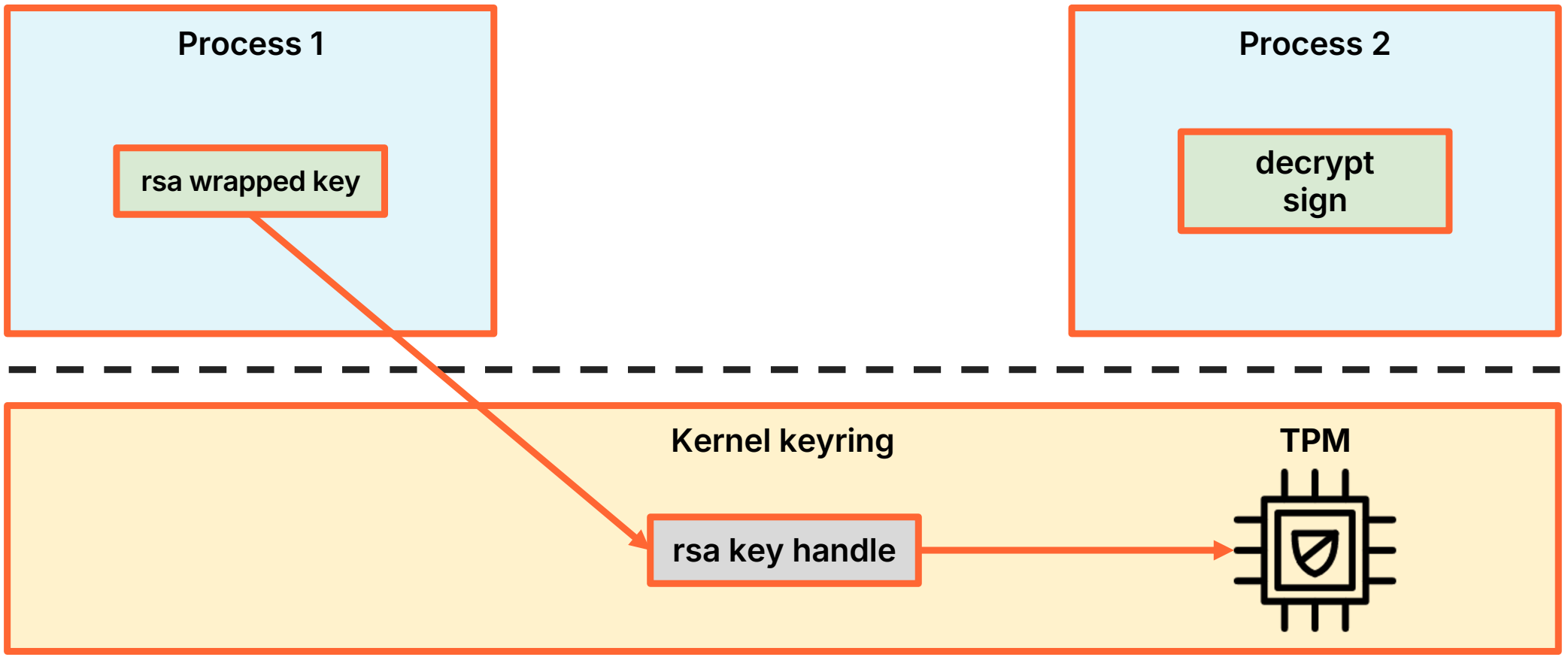
Asymmetric TPM keys



@ignatkn

CLOUDFLARE

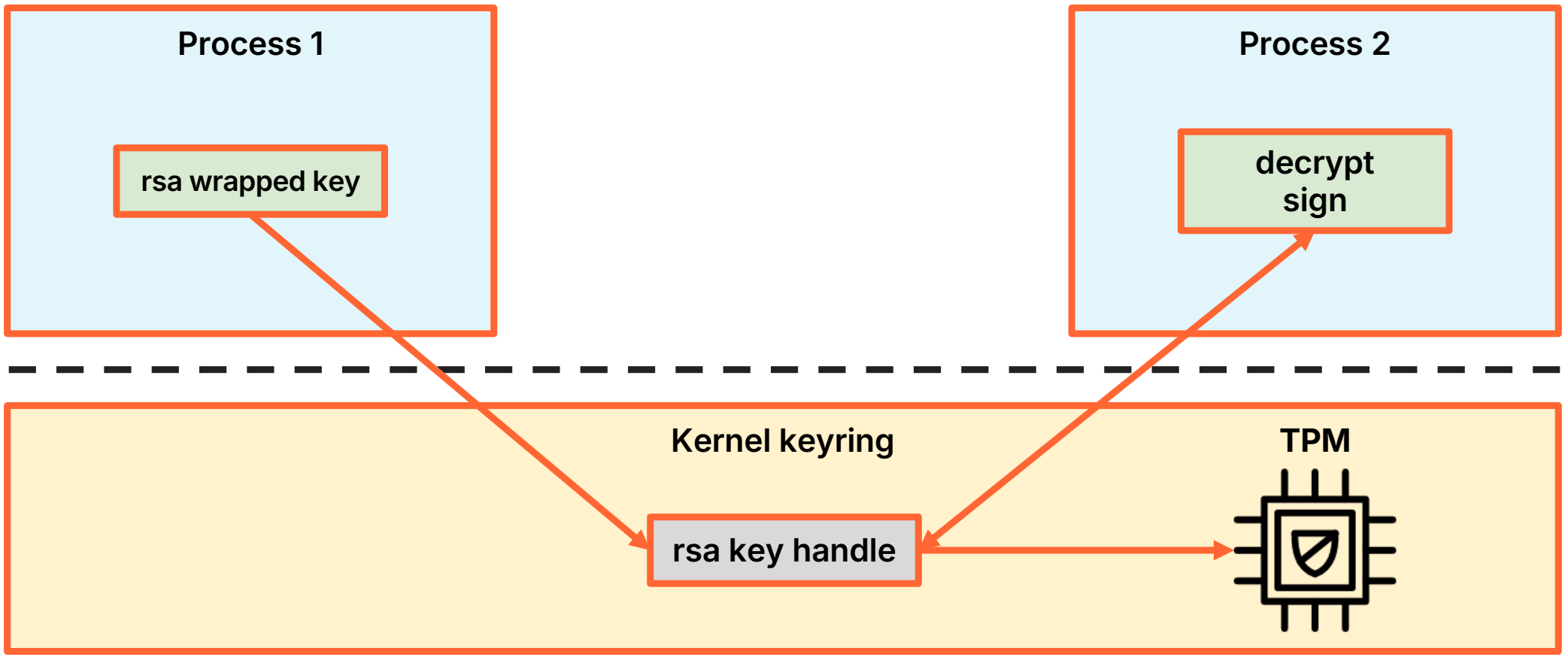
Asymmetric TPM keys



@ignatkn

CLOUDFLARE

Asymmetric TPM keys

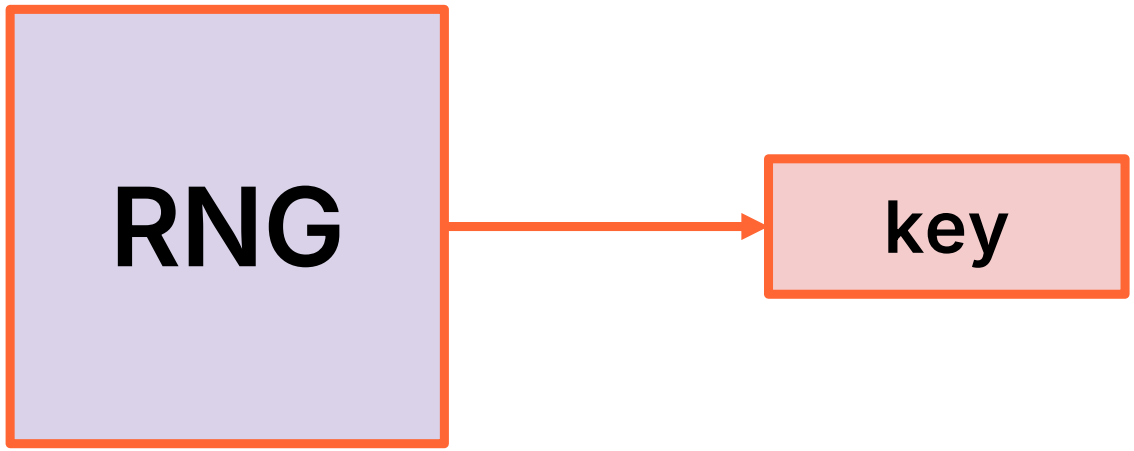


CLOUDFLARE

Wrapped keys

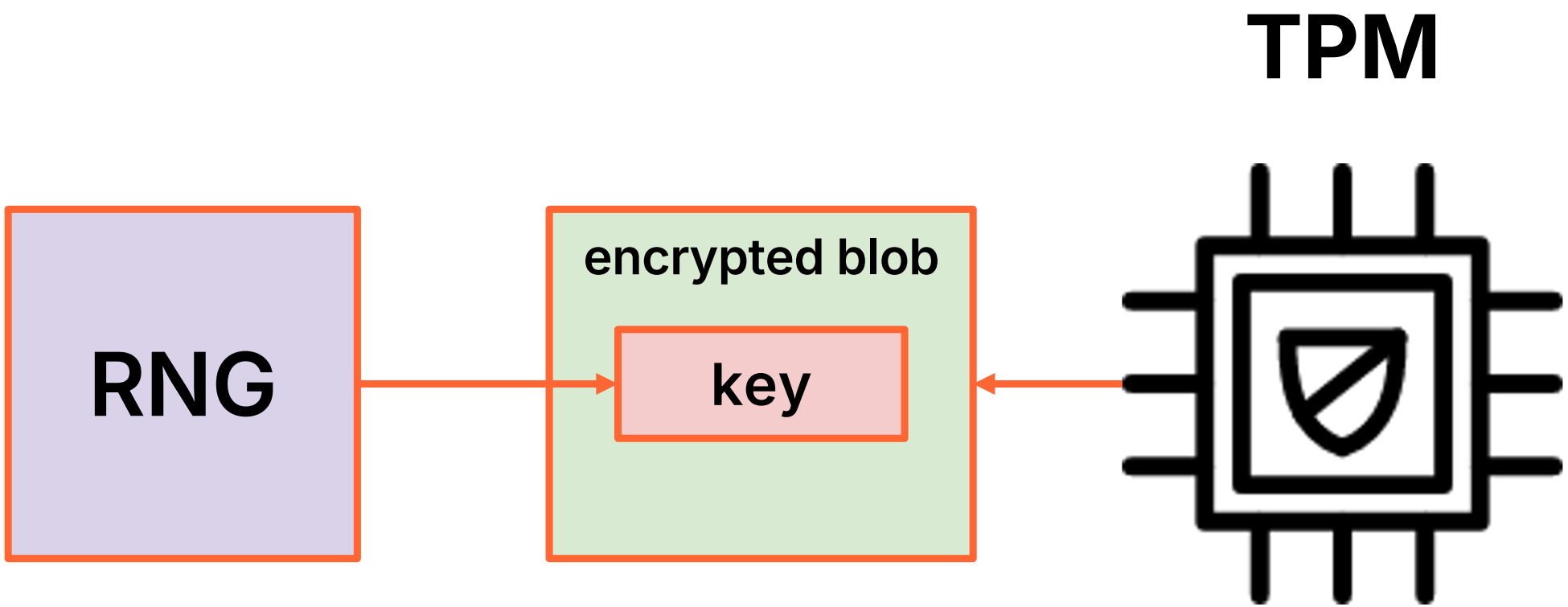
CLOUDFLARE

Wrapped keys



CLOUDFLARE

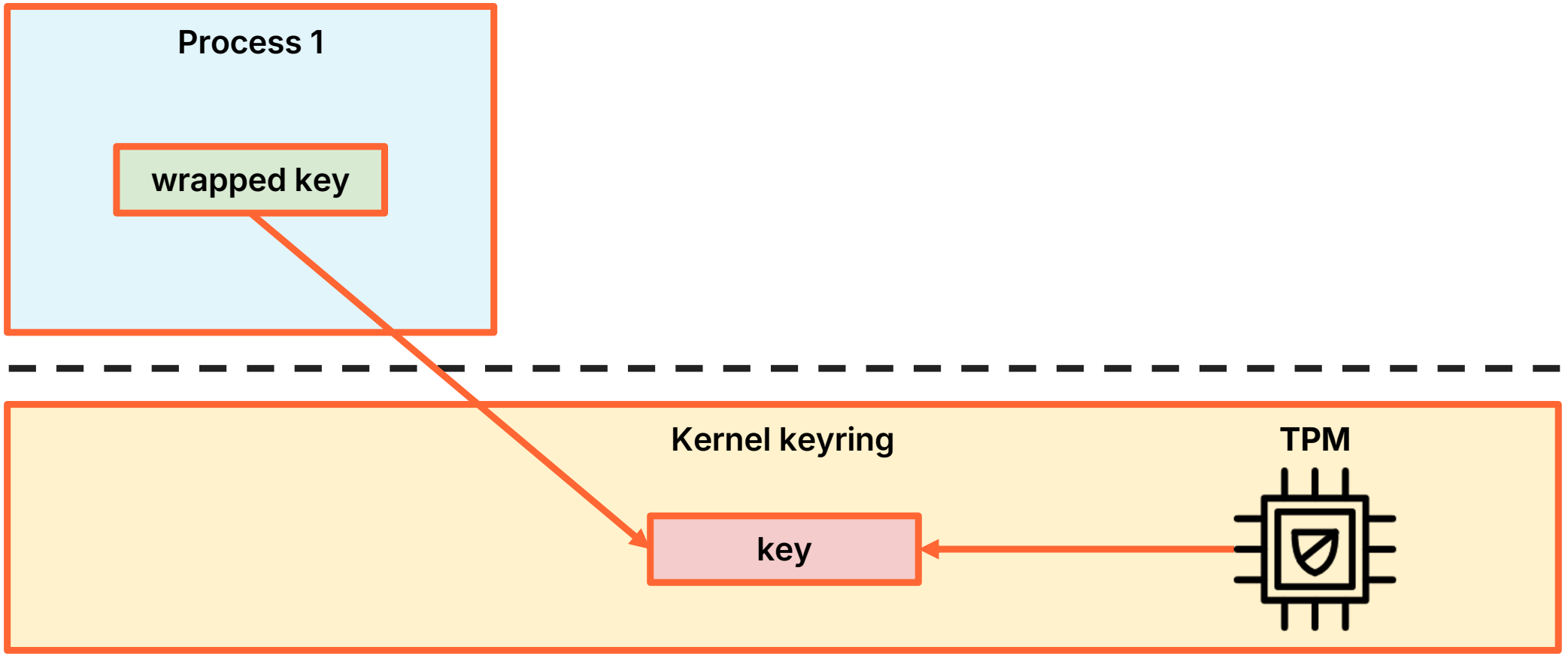
Wrapped keys



@ignatkn

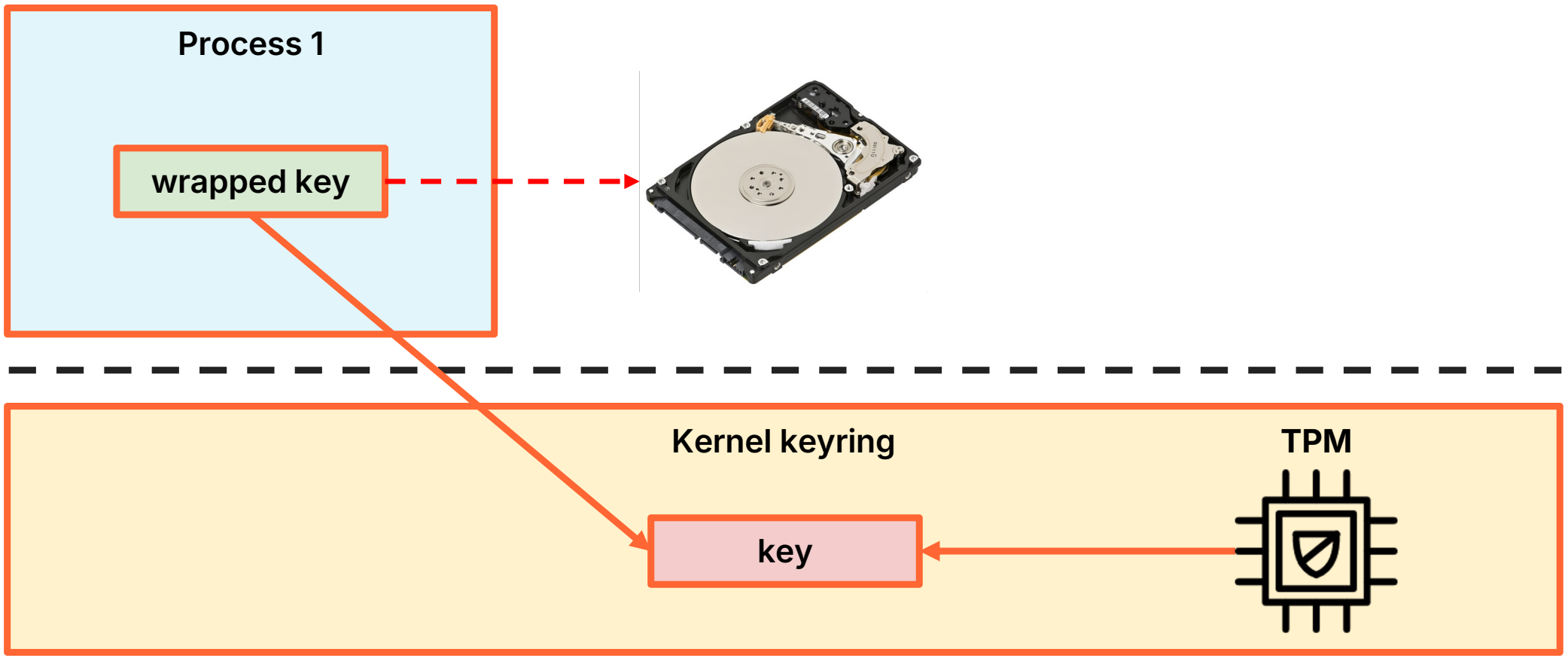
CLOUDFLARE

Trusted key management



CLOUDFLARE

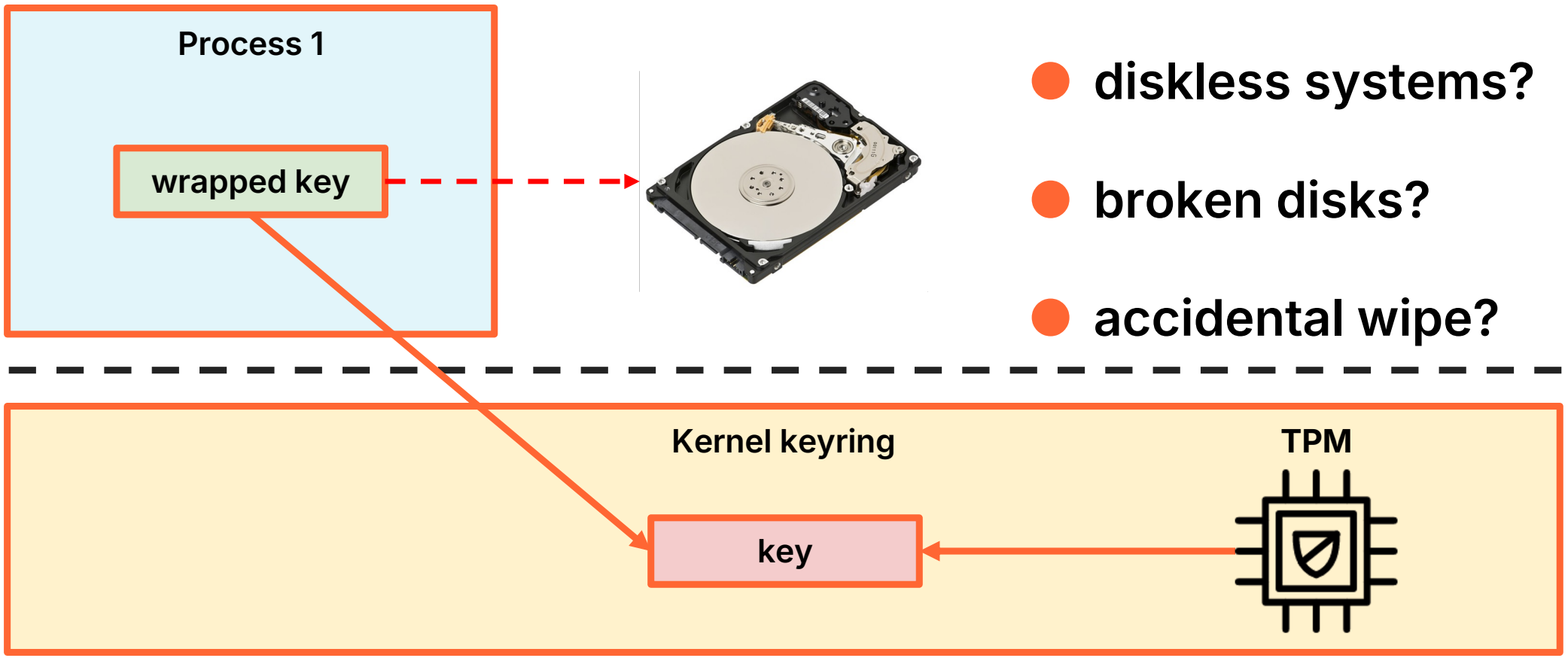
Trusted key management



@ignatkn

CLOUDFLARE

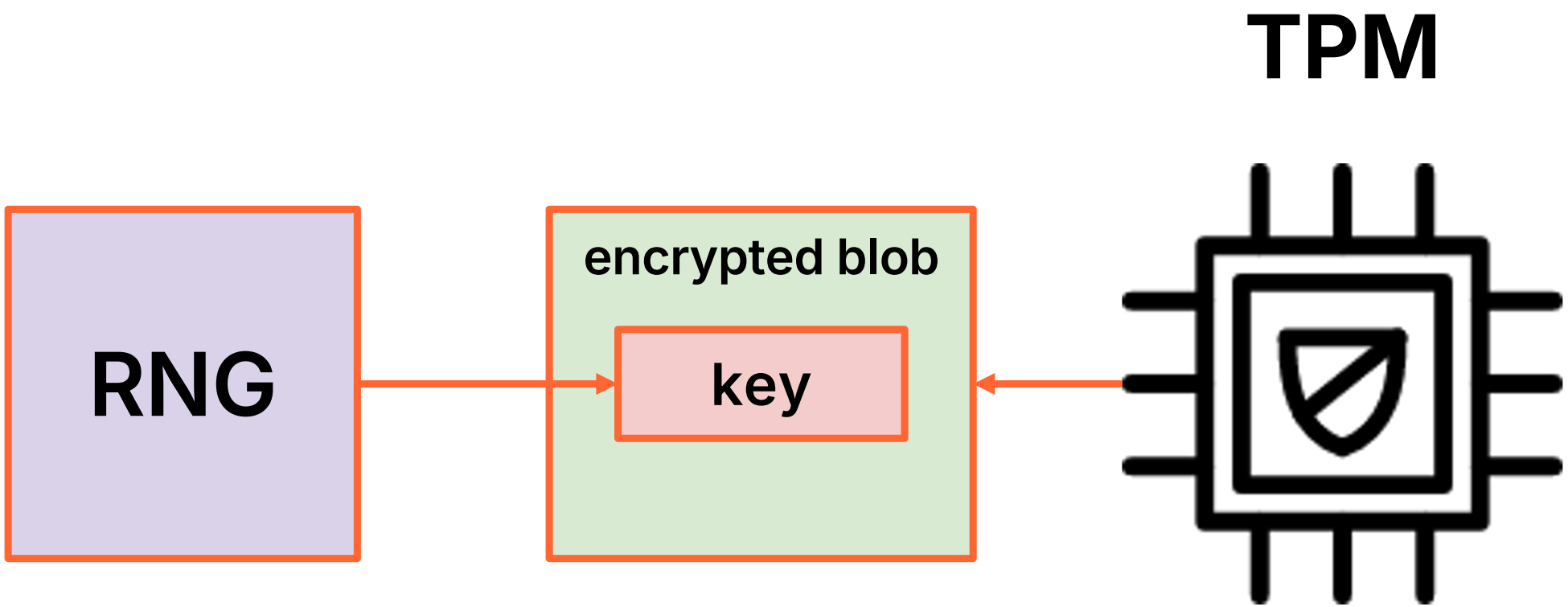
Trusted key management



- diskless systems?
- broken disks?
- accidental wipe?

CLOUDFLARE

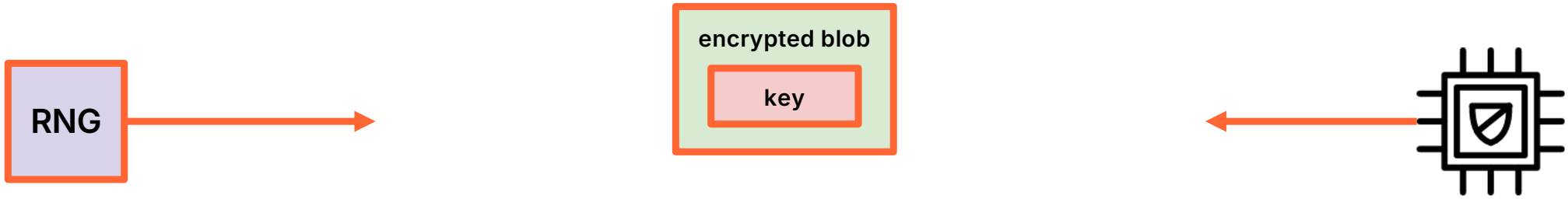
Wrapped keys



@ignatkn

CLOUDFLARE

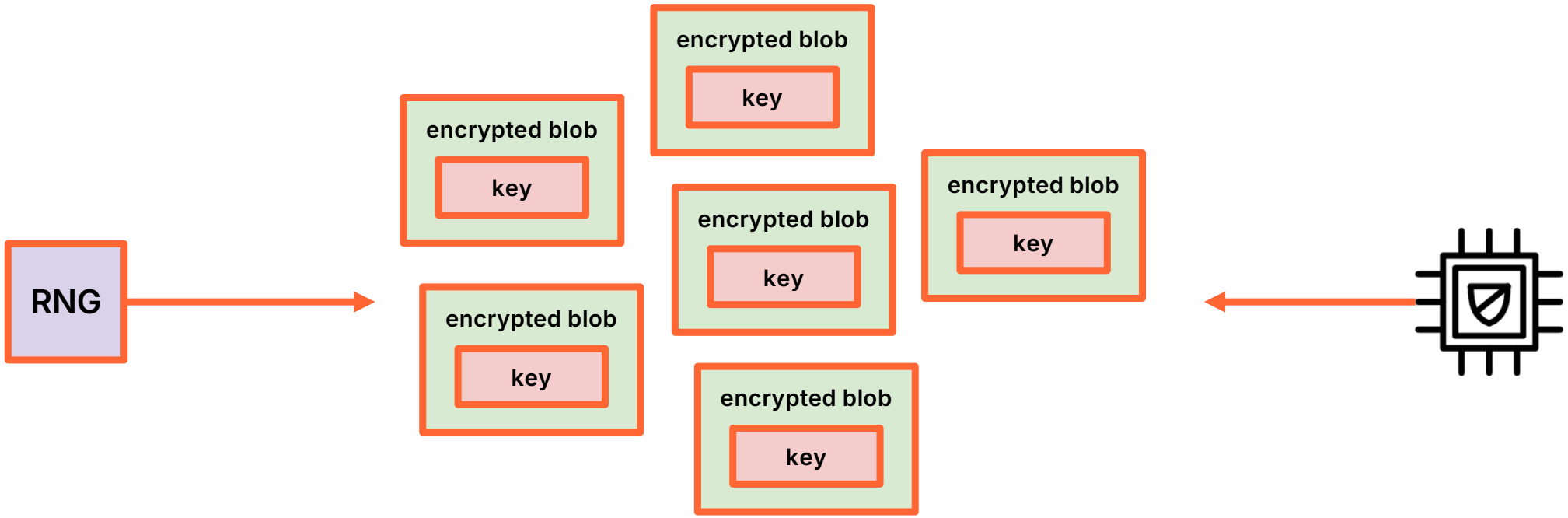
Wrapped keys



@ignatkn

CLOUDFLARE

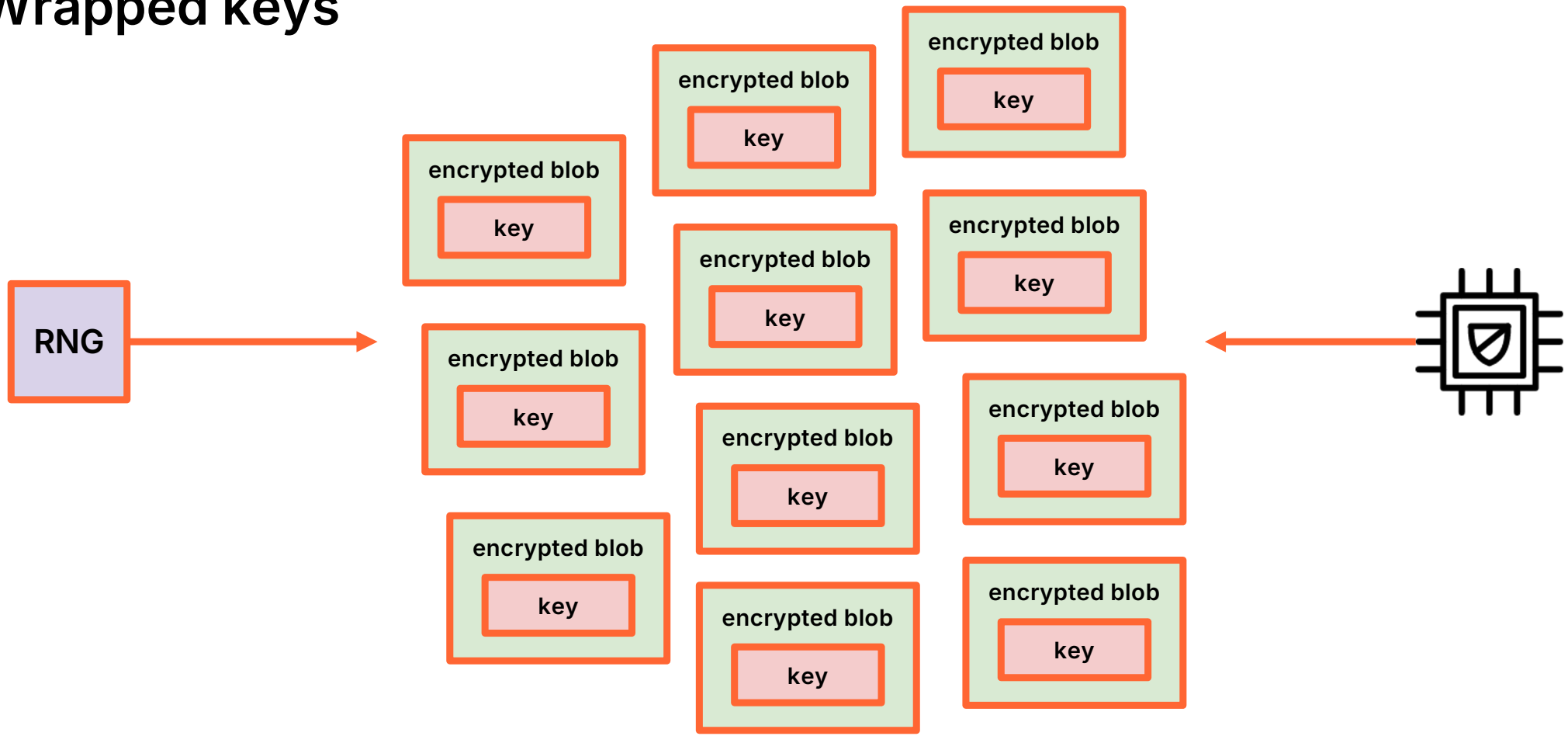
Wrapped keys



@ignatkn

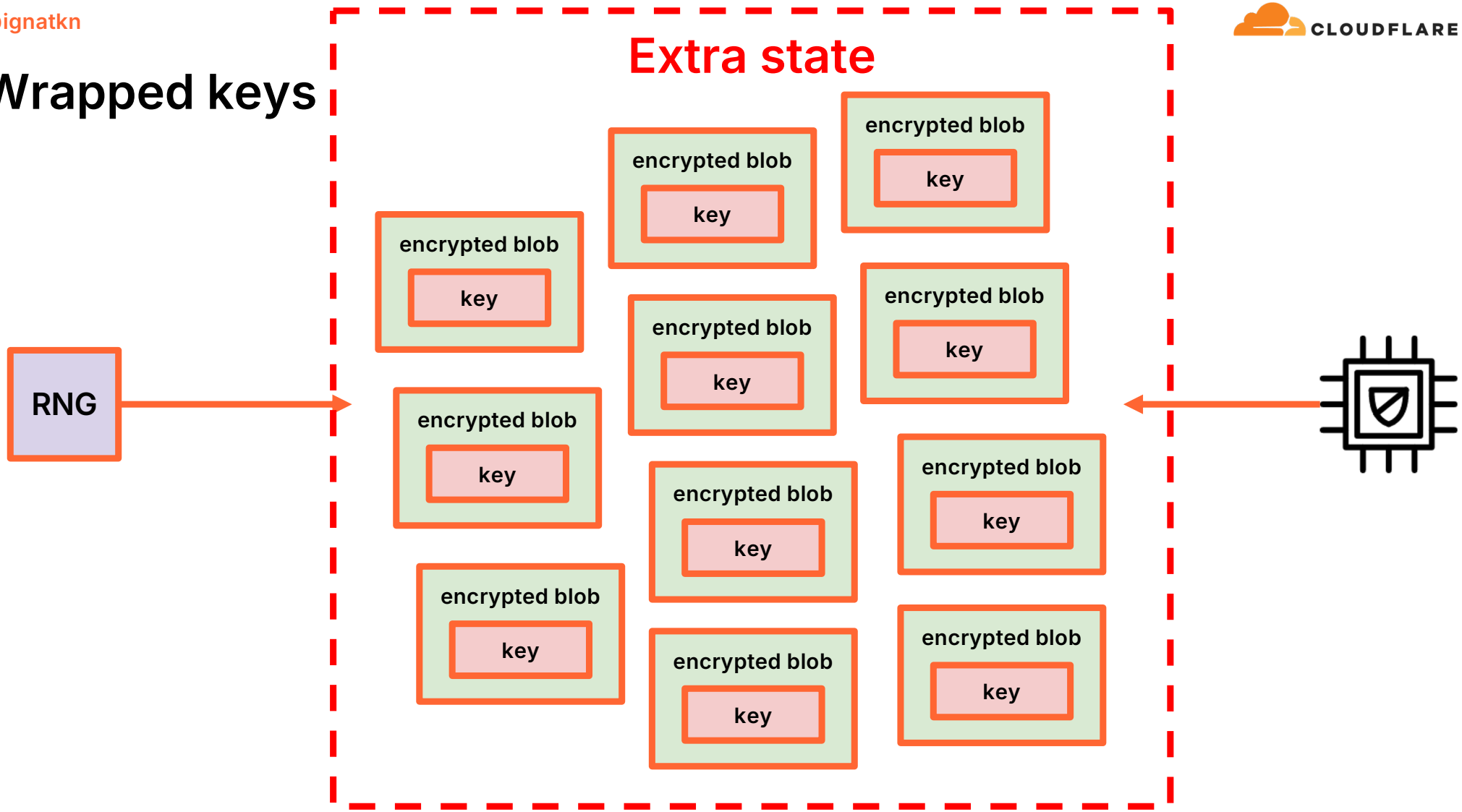
CLOUDFLARE

Wrapped keys



@ignatkn

Wrapped keys

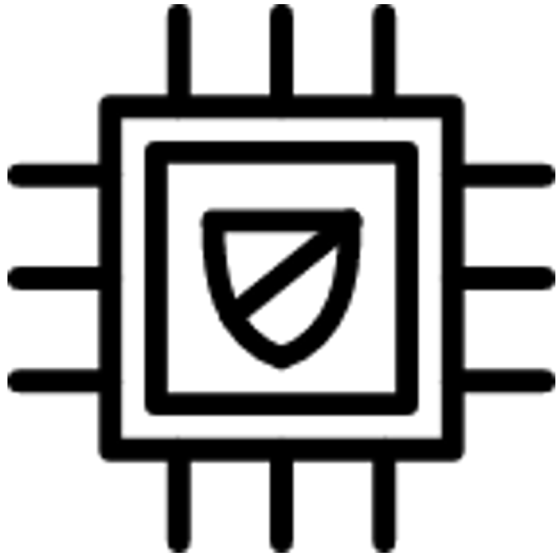


@ignatkn

CLOUDFLARE

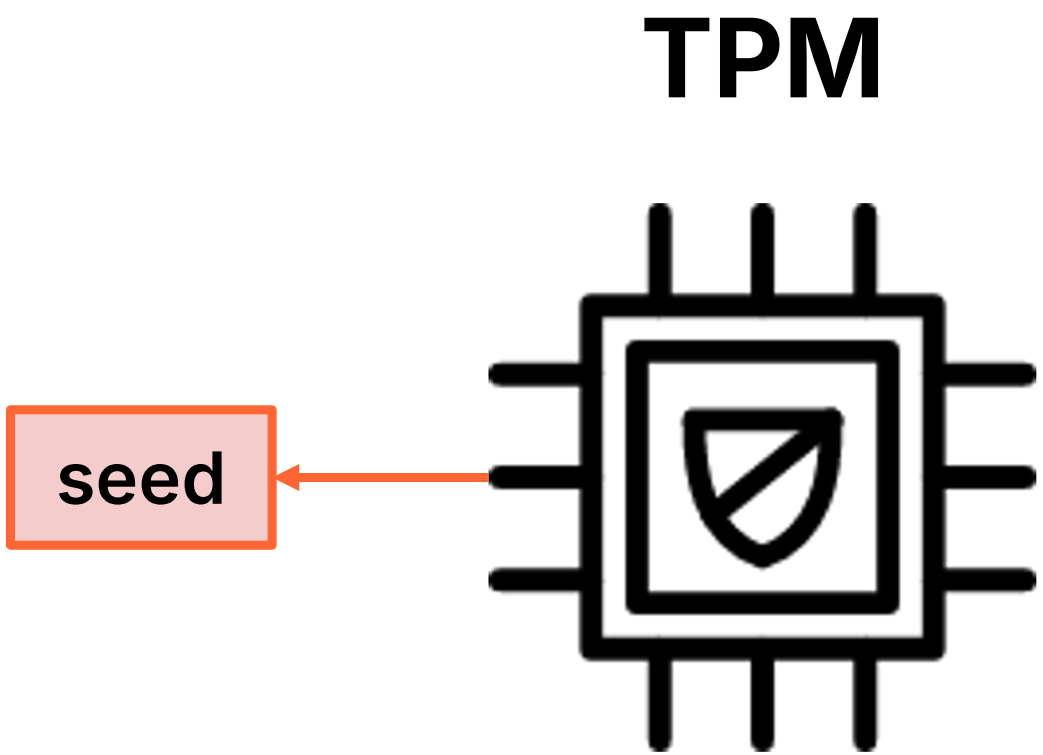
Derived keys

TPM



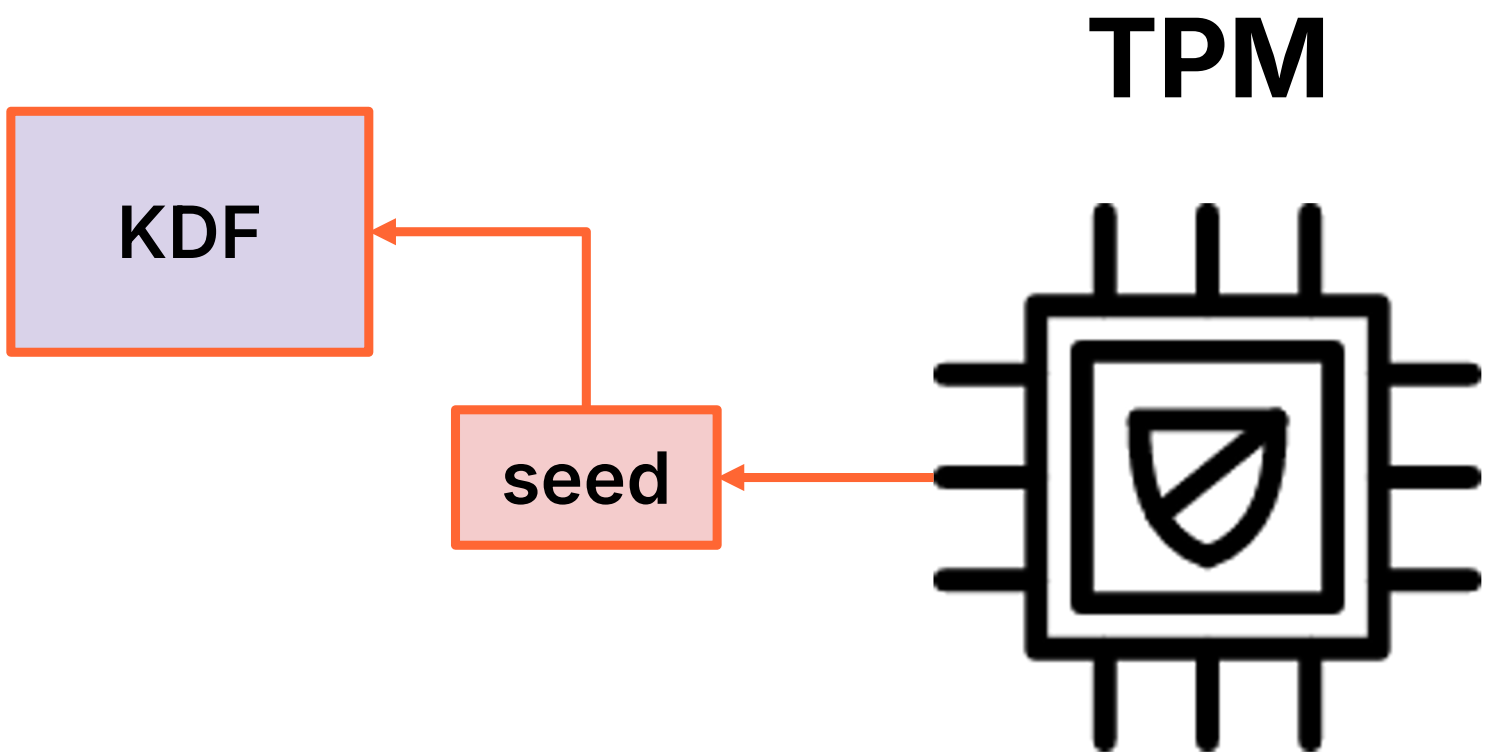
CLOUDFLARE

Derived keys



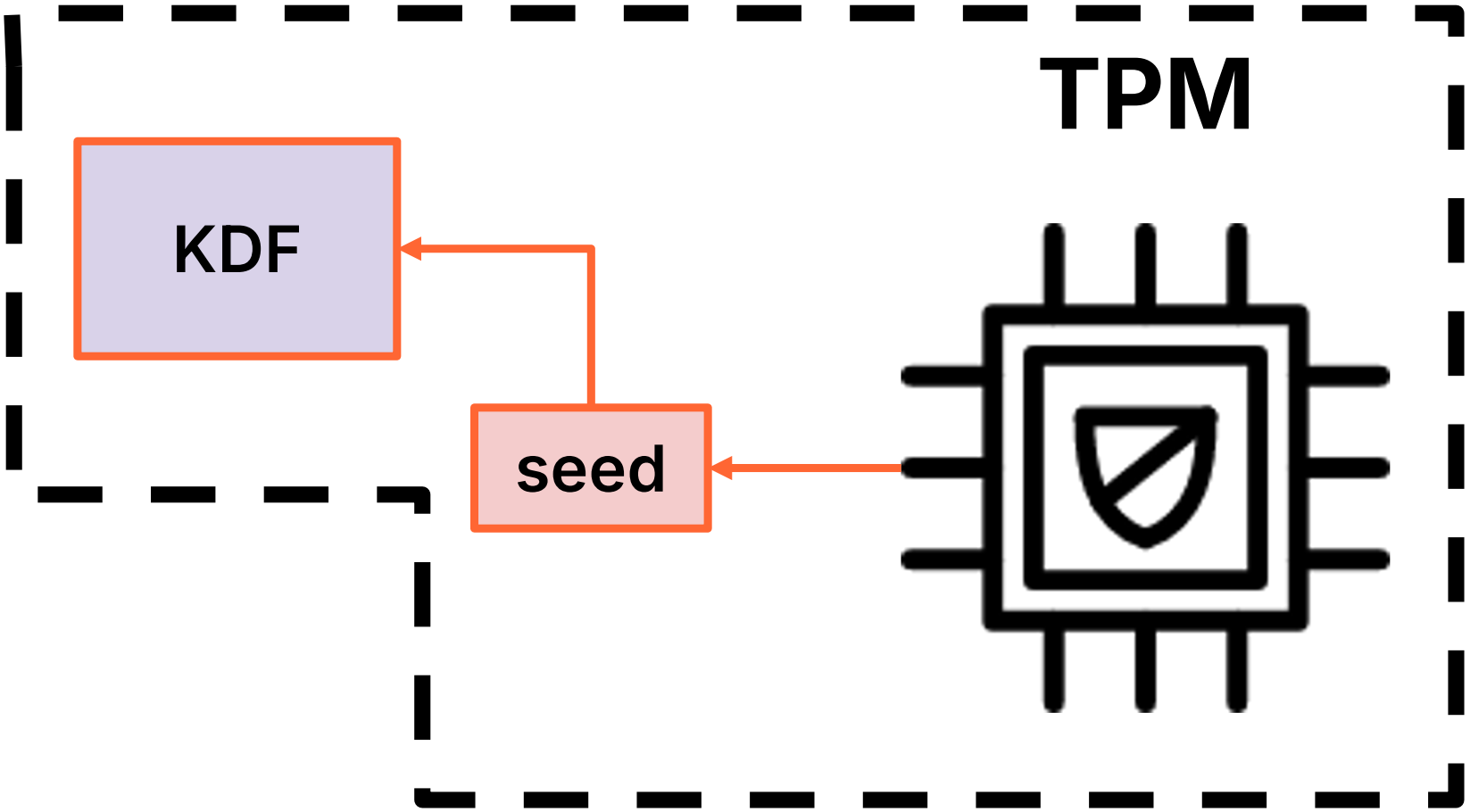
CLOUDFLARE

Derived keys



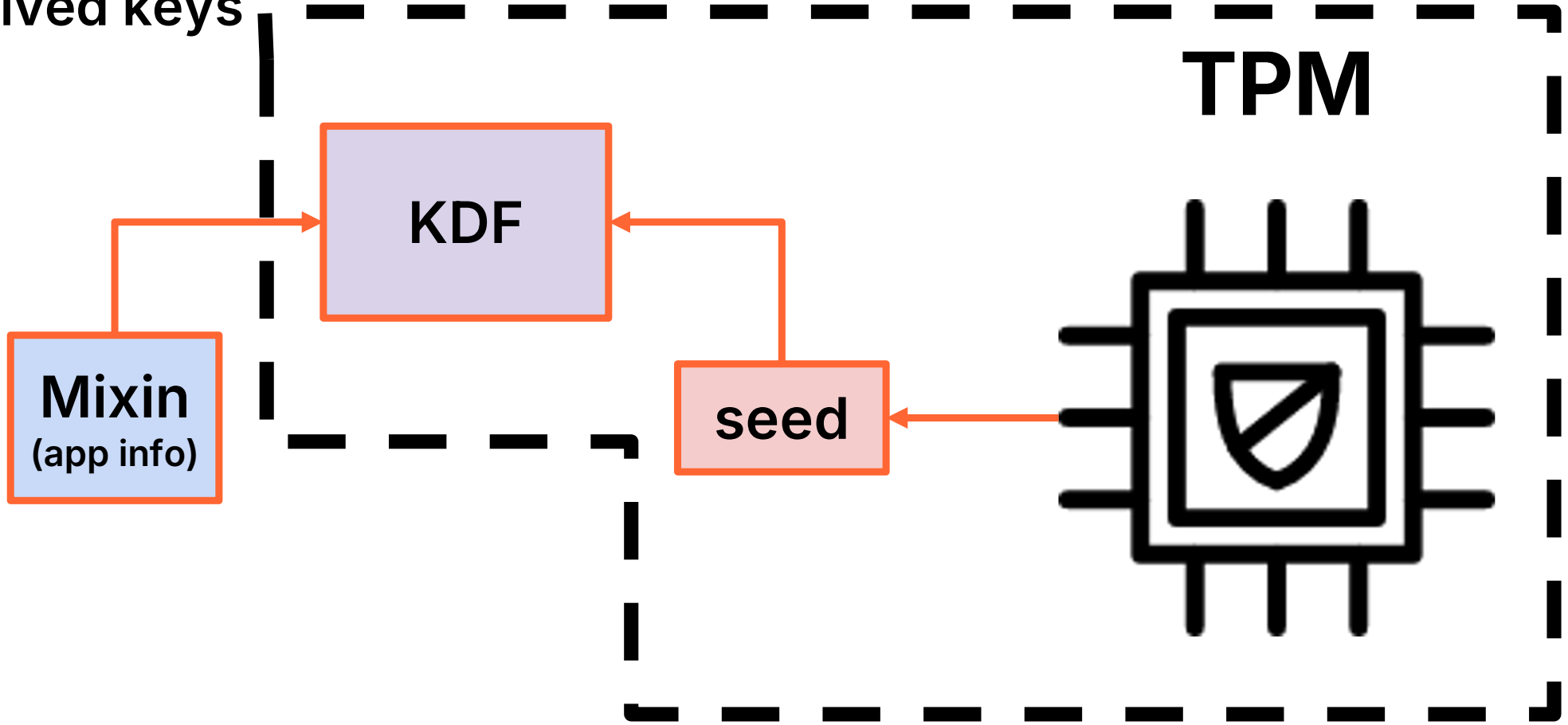
CLOUDFLARE

Derived keys



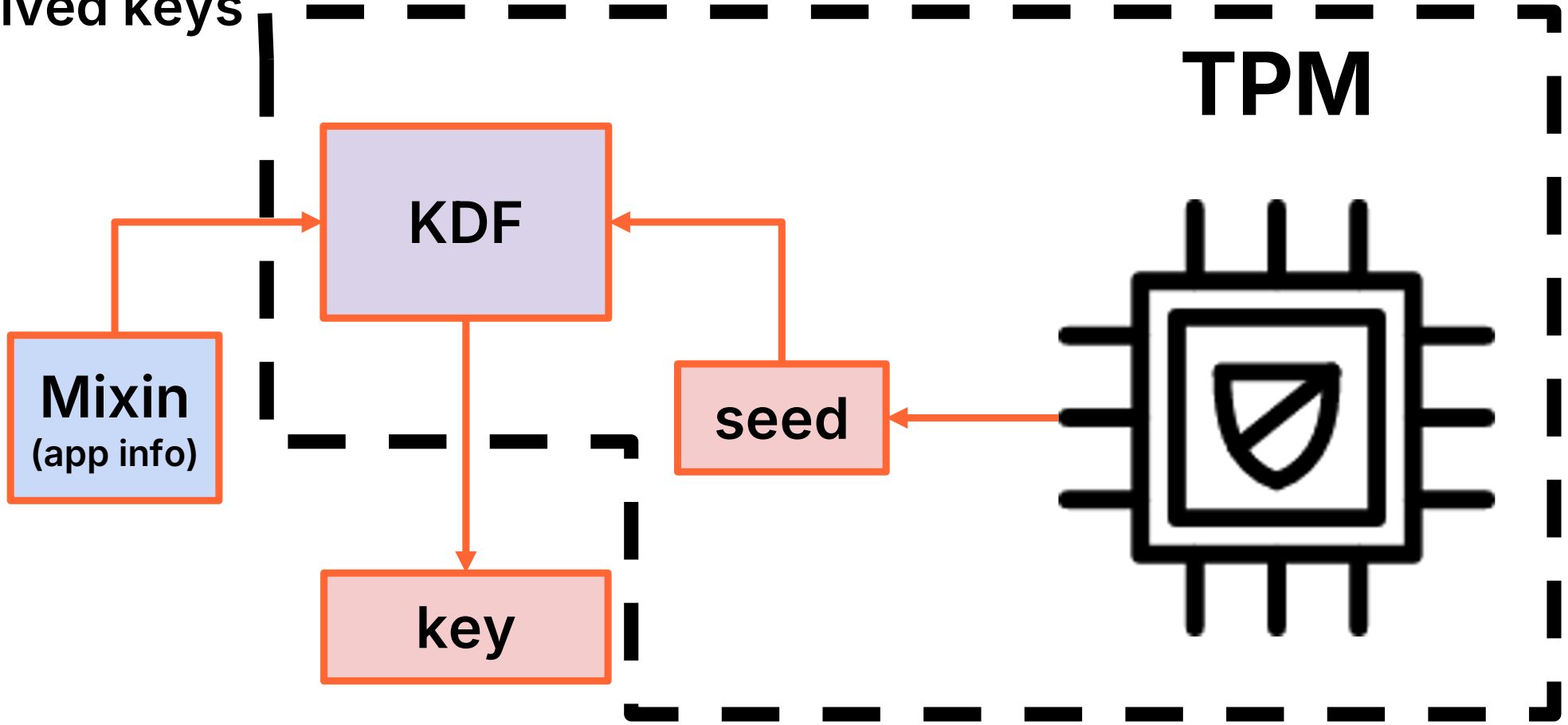
CLOUDFLARE

Derived keys



CLOUDFLARE

Derived keys



@ignatkn

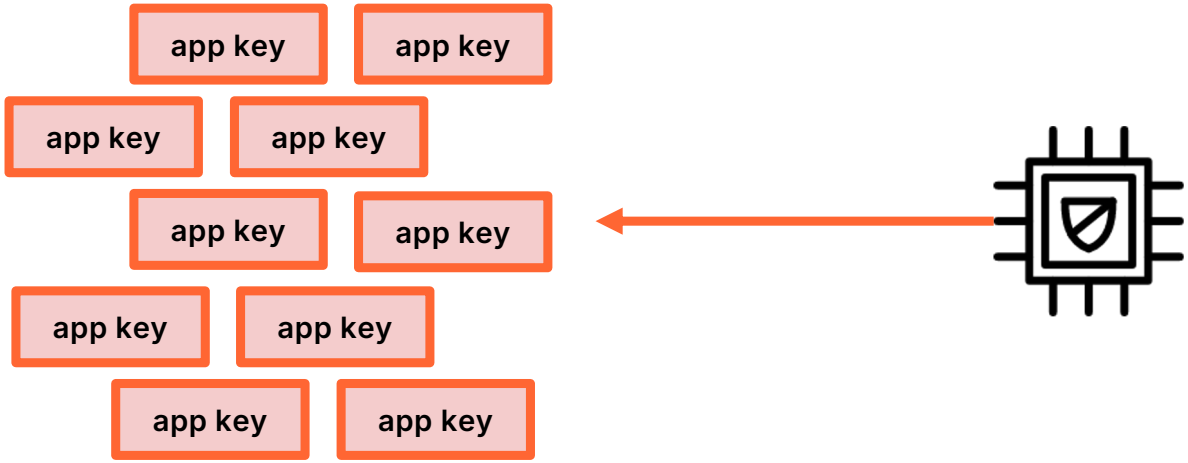
CLOUDFLARE

Derived keys

@ignatkn

CLOUDFLARE

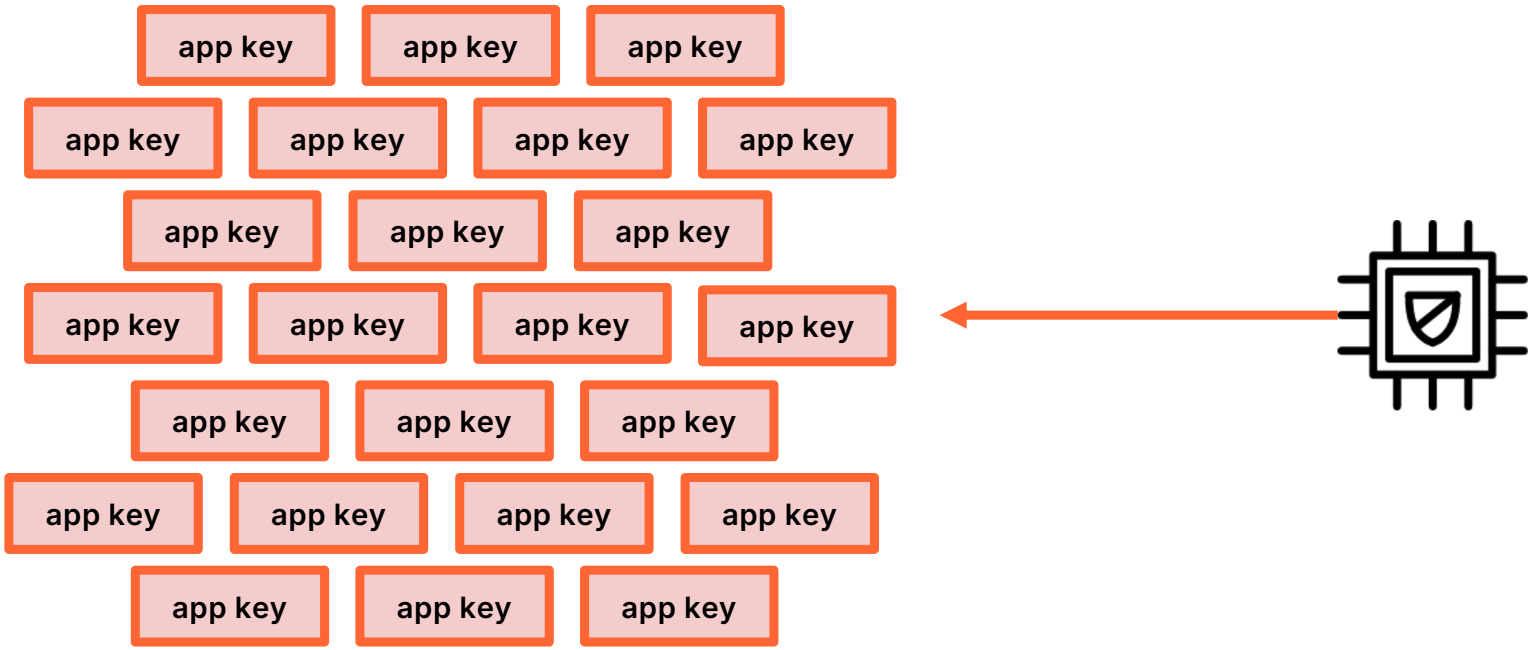
Derived keys



@ignatkn

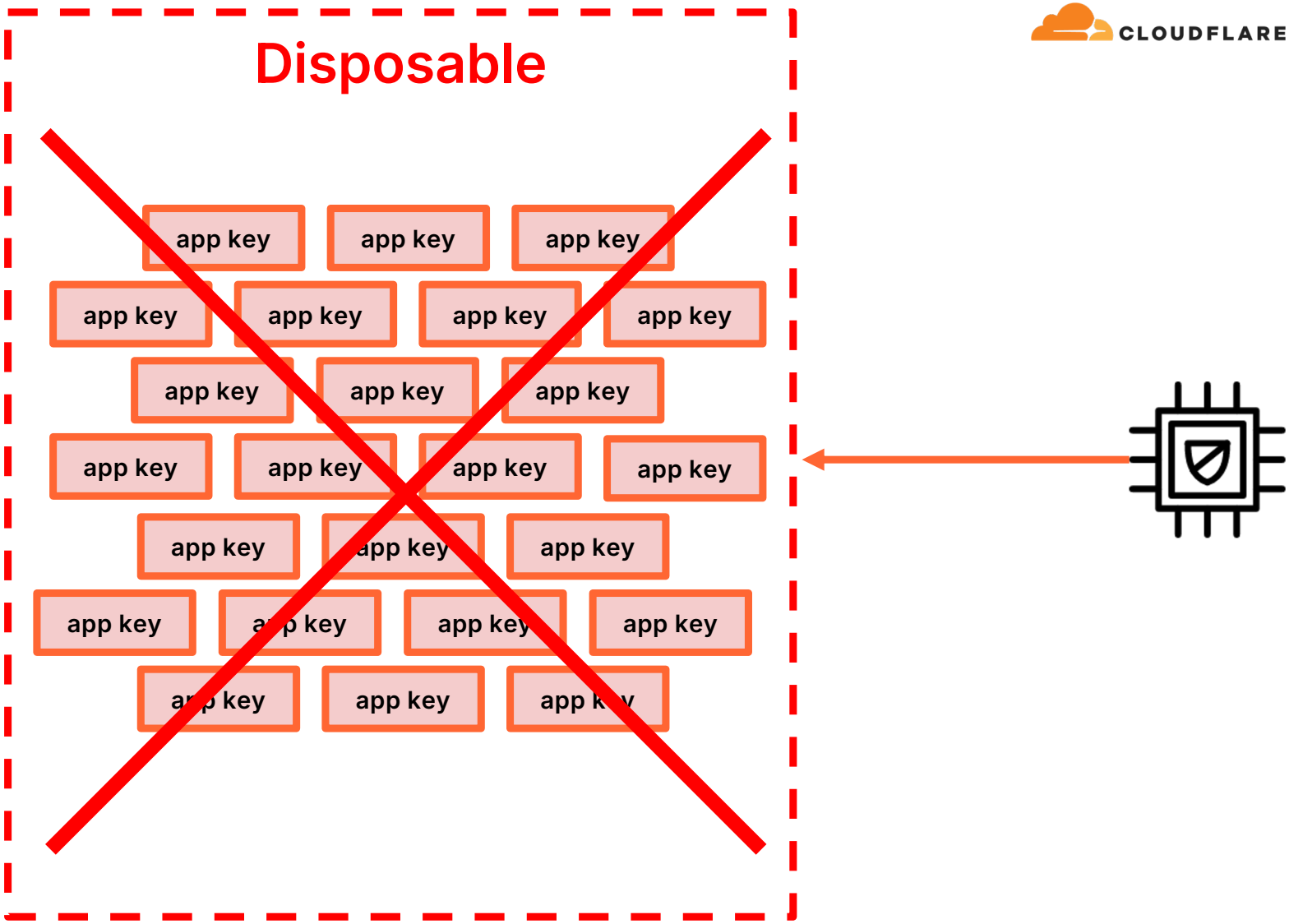
CLOUDFLARE

Derived keys

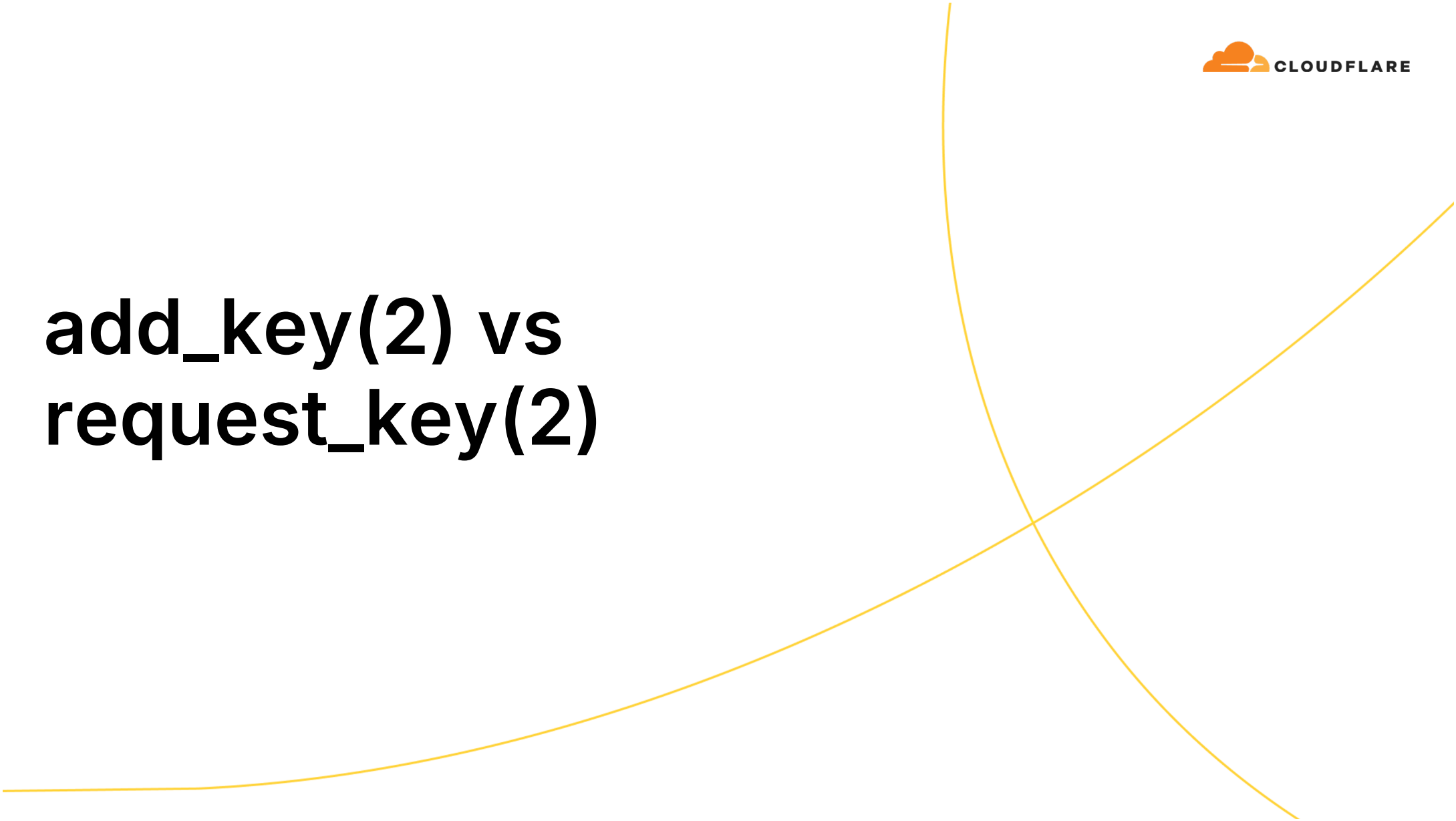


@ignatkn

Derived keys

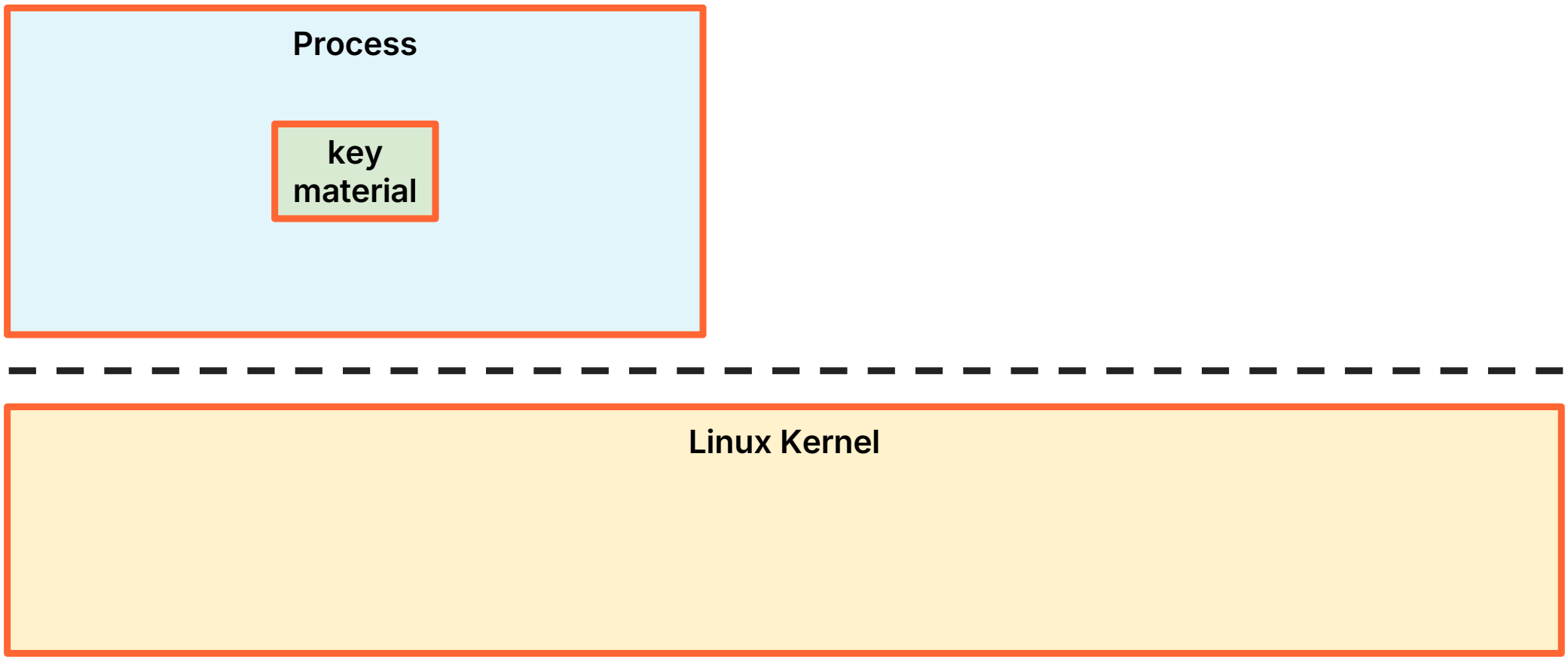


add_key(2) vs request_key(2)



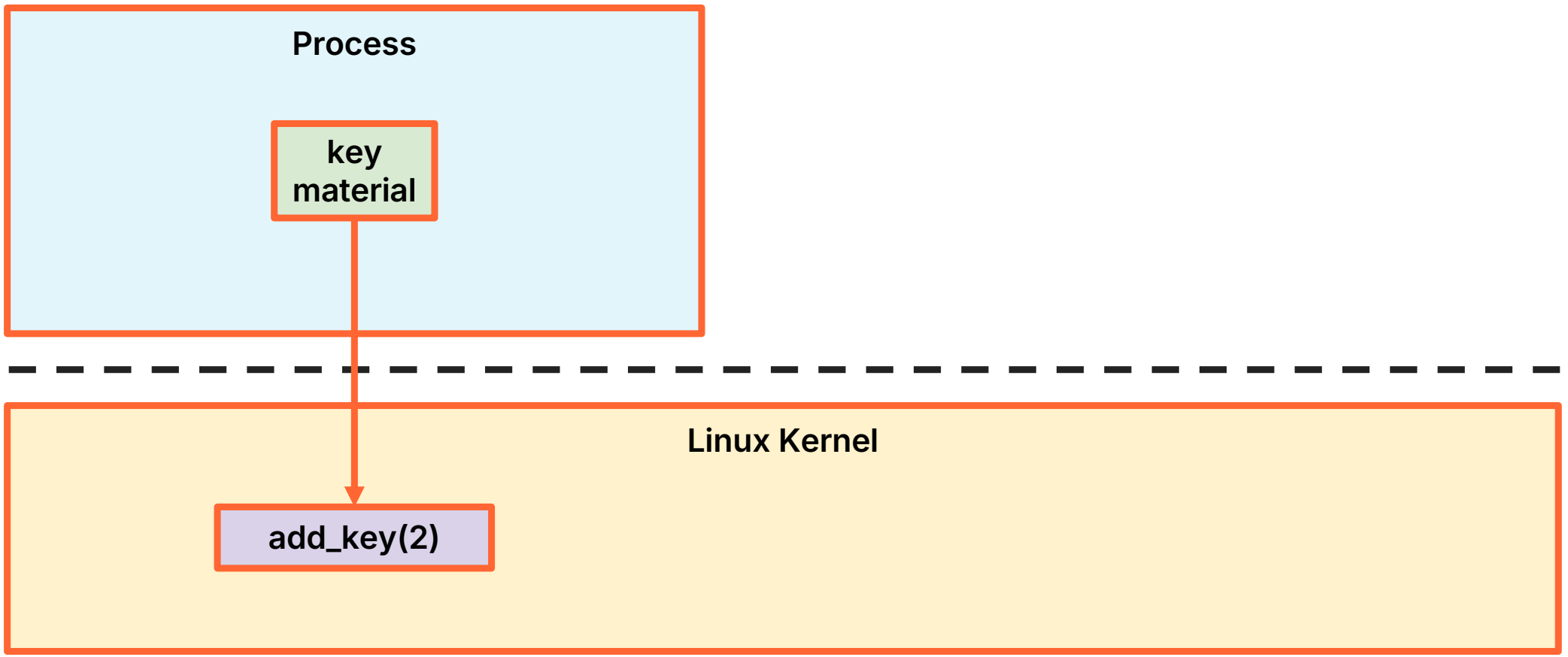
CLOUDFLARE

add_key(2)



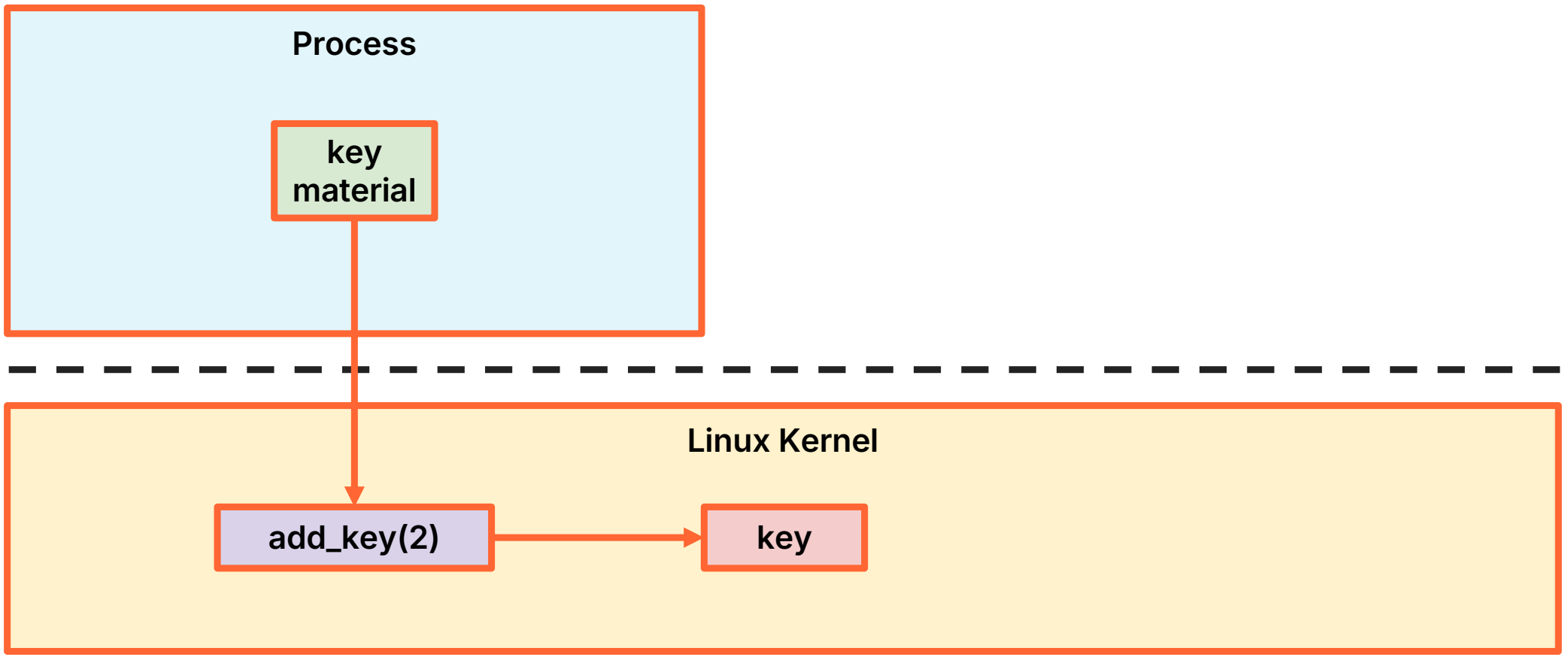
CLOUDFLARE

add_key(2)



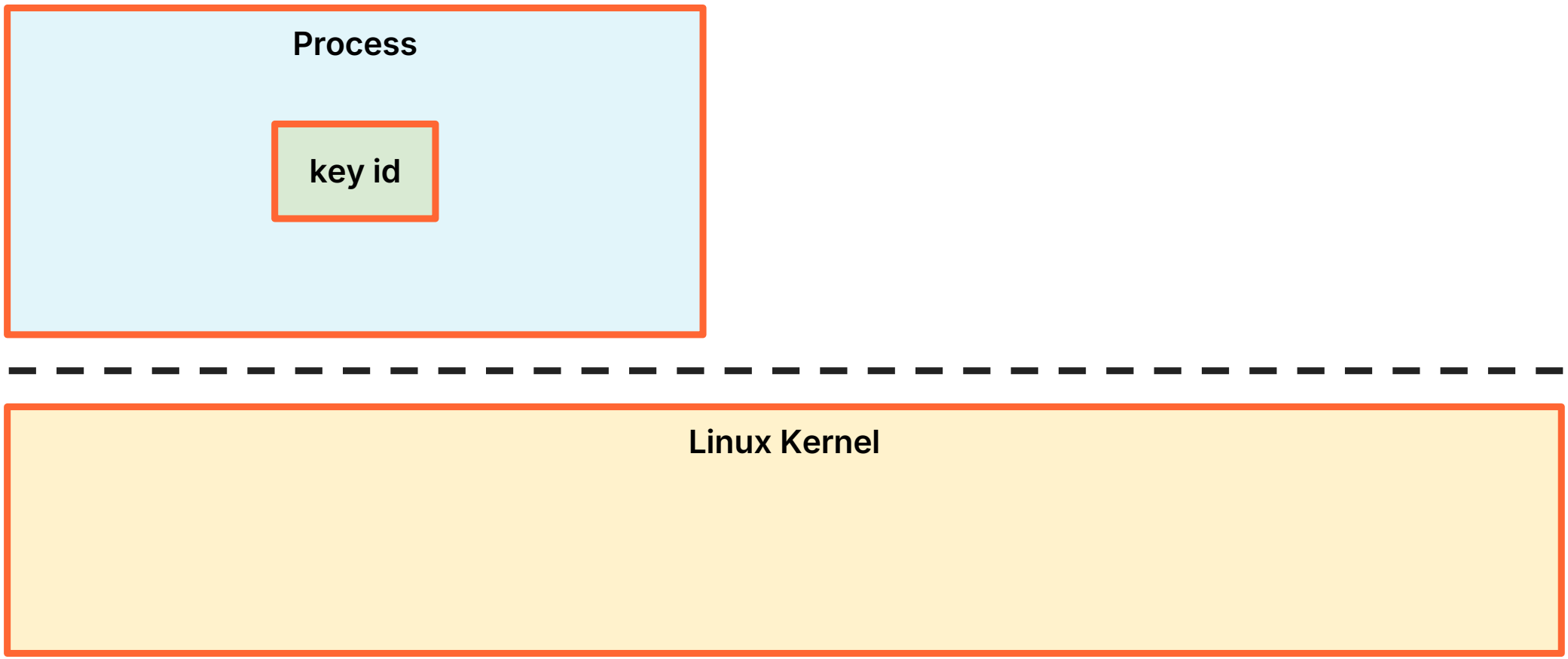
CLOUDFLARE

add_key(2)



CLOUDFLARE

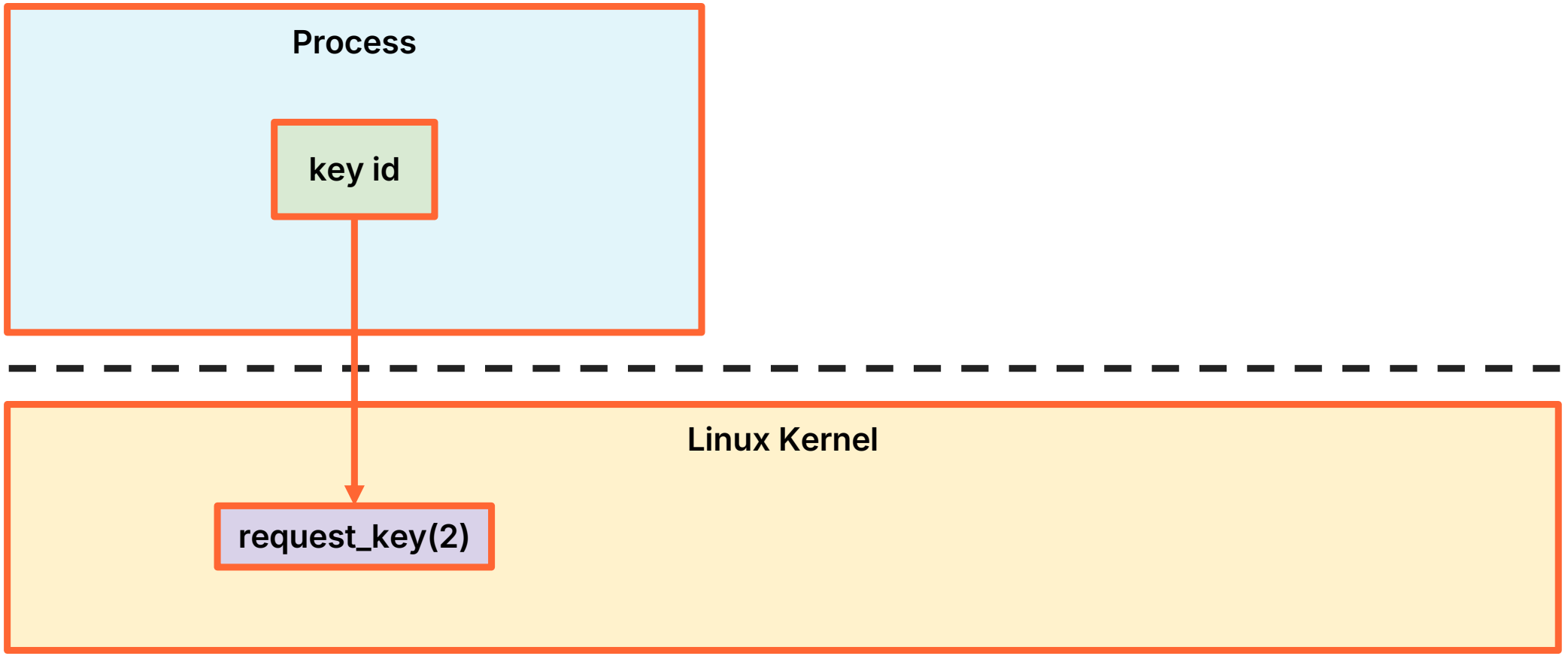
request_key(2)



@ignatkn

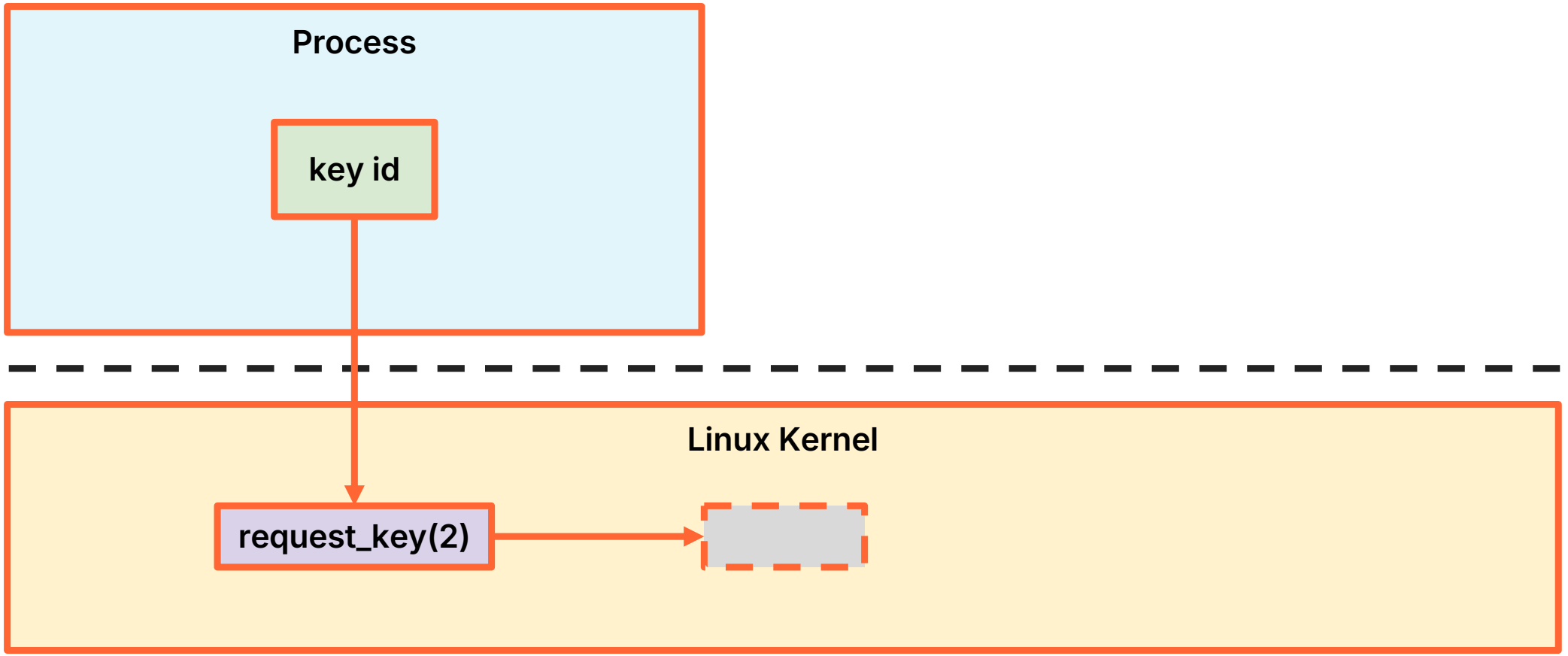
CLOUDFLARE

request_key(2)



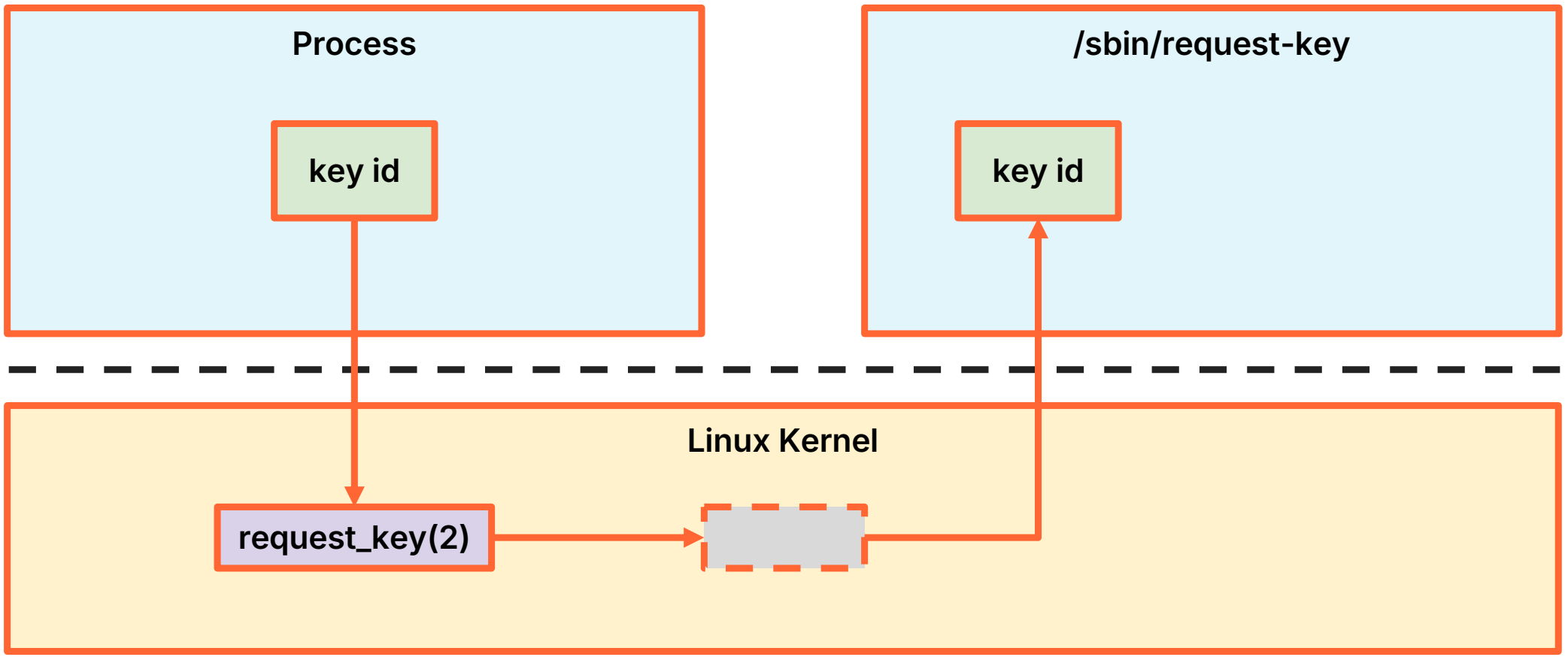
CLOUDFLARE

request_key(2)



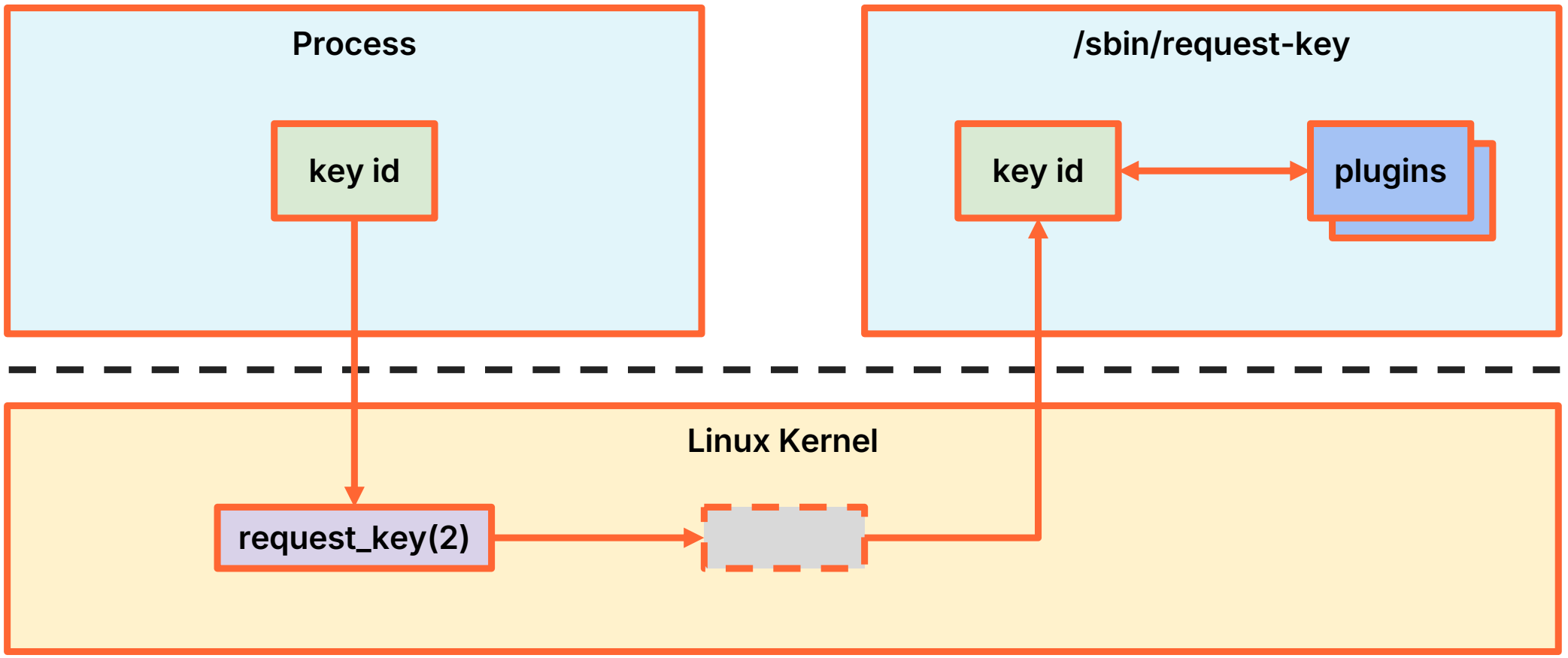
CLOUDFLARE

request_key(2)



CLOUDFLARE

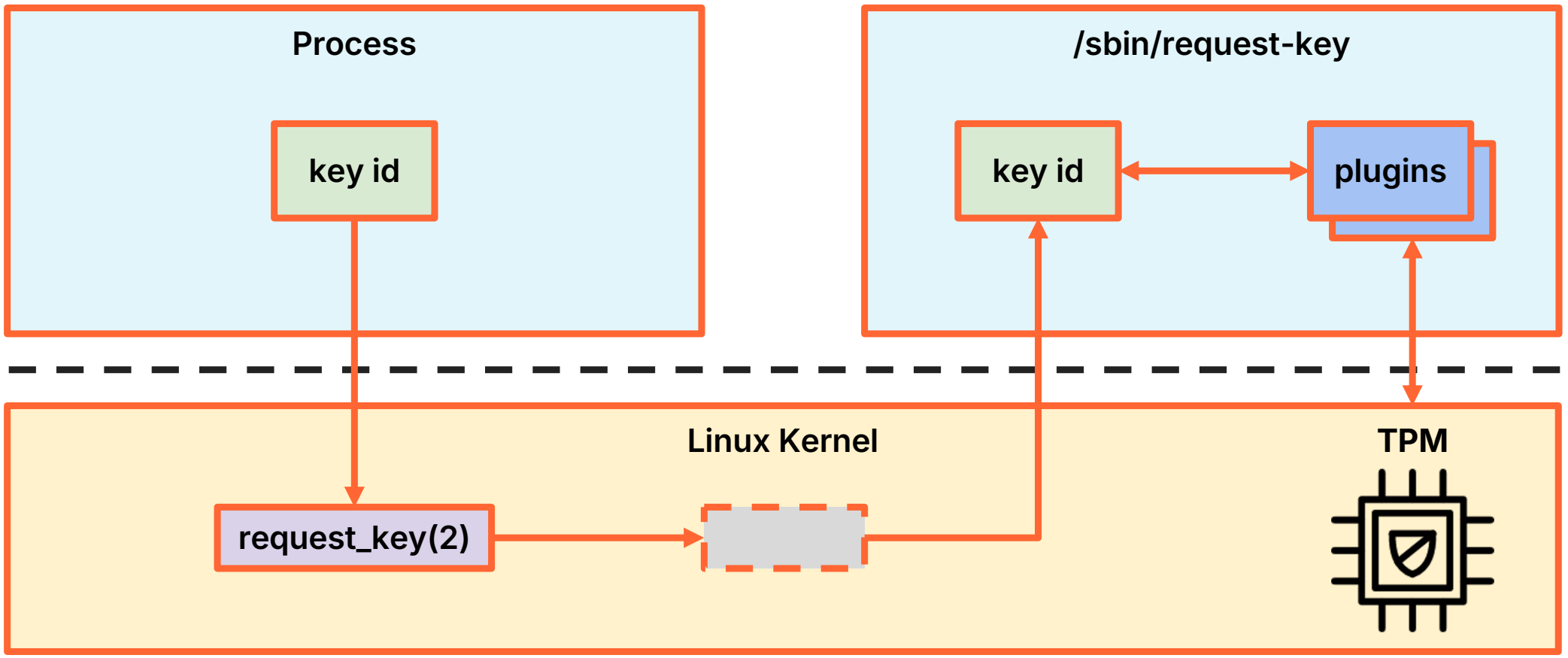
request_key(2)



@ignatkn

CLOUDFLARE

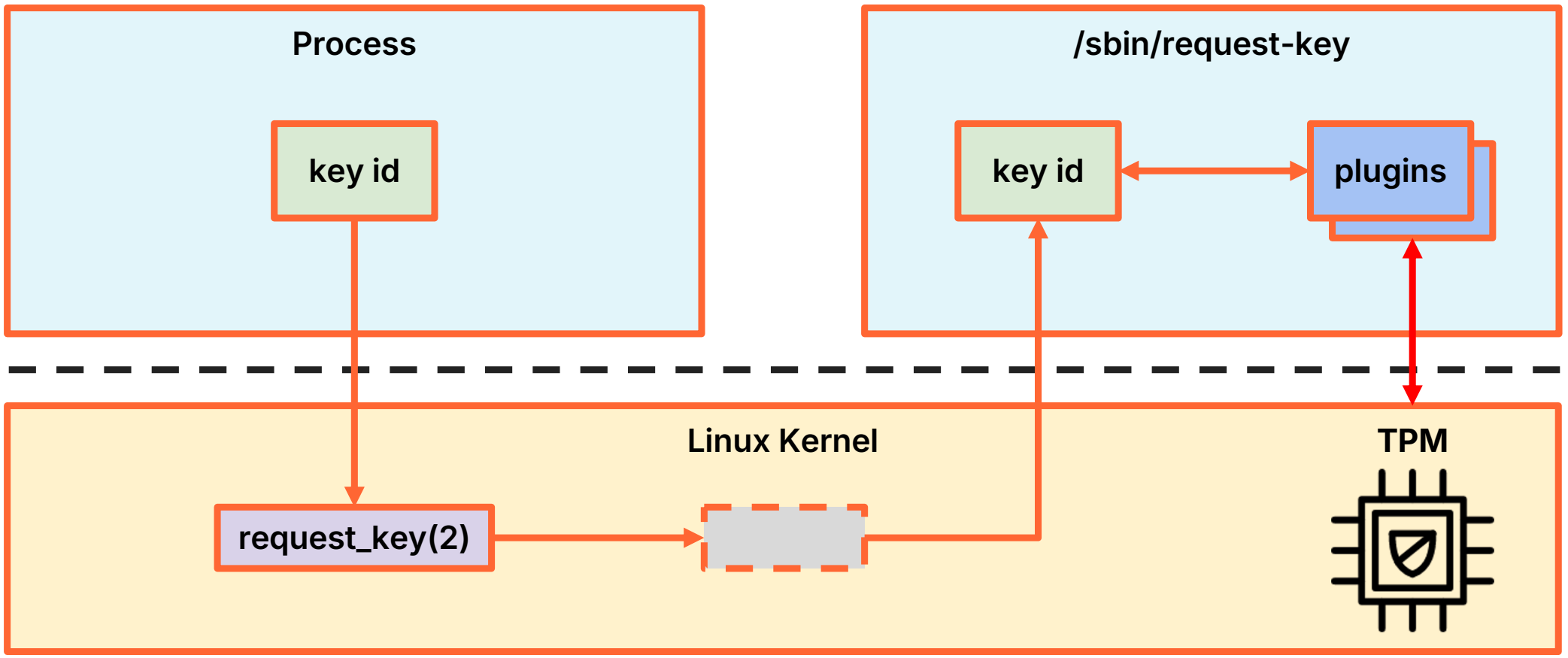
request_key(2)



@ignatkn

CLOUDFLARE

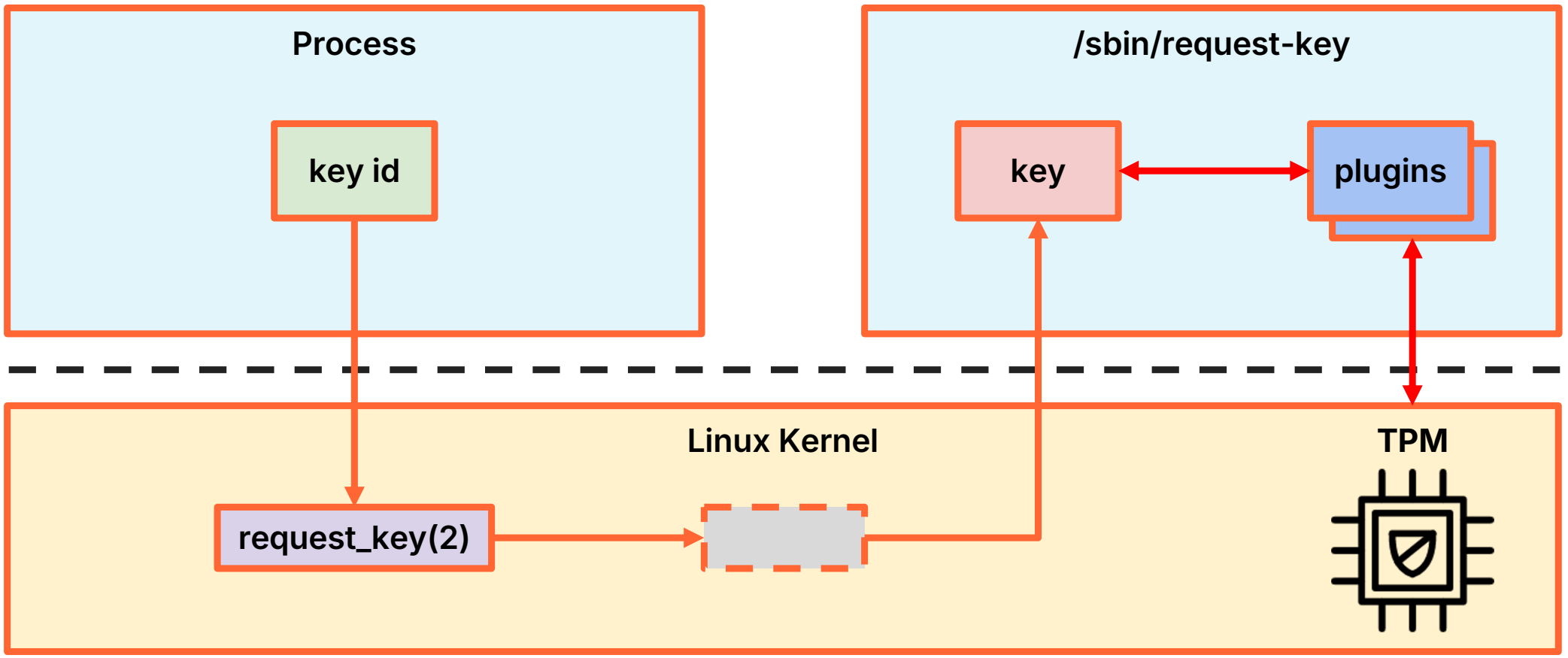
request_key(2)



@ignatkn

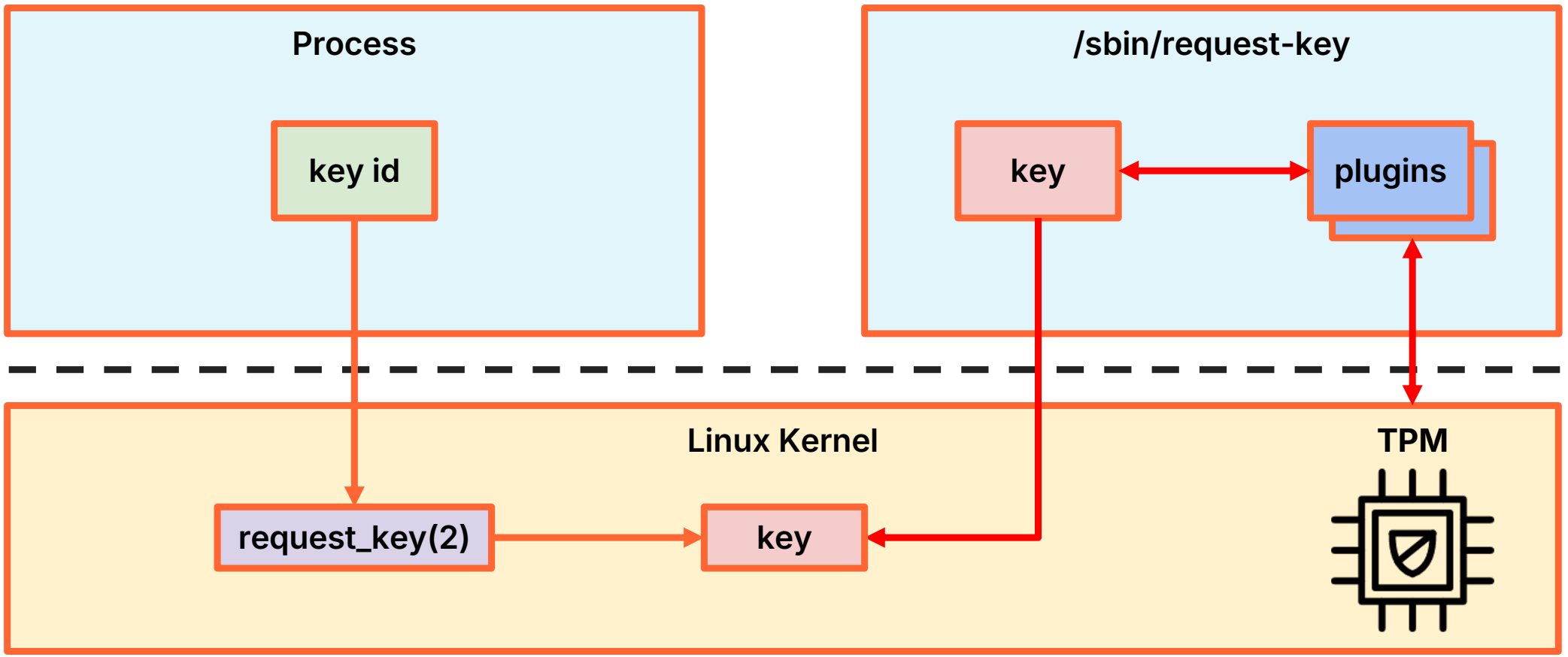
CLOUDFLARE

request_key(2)



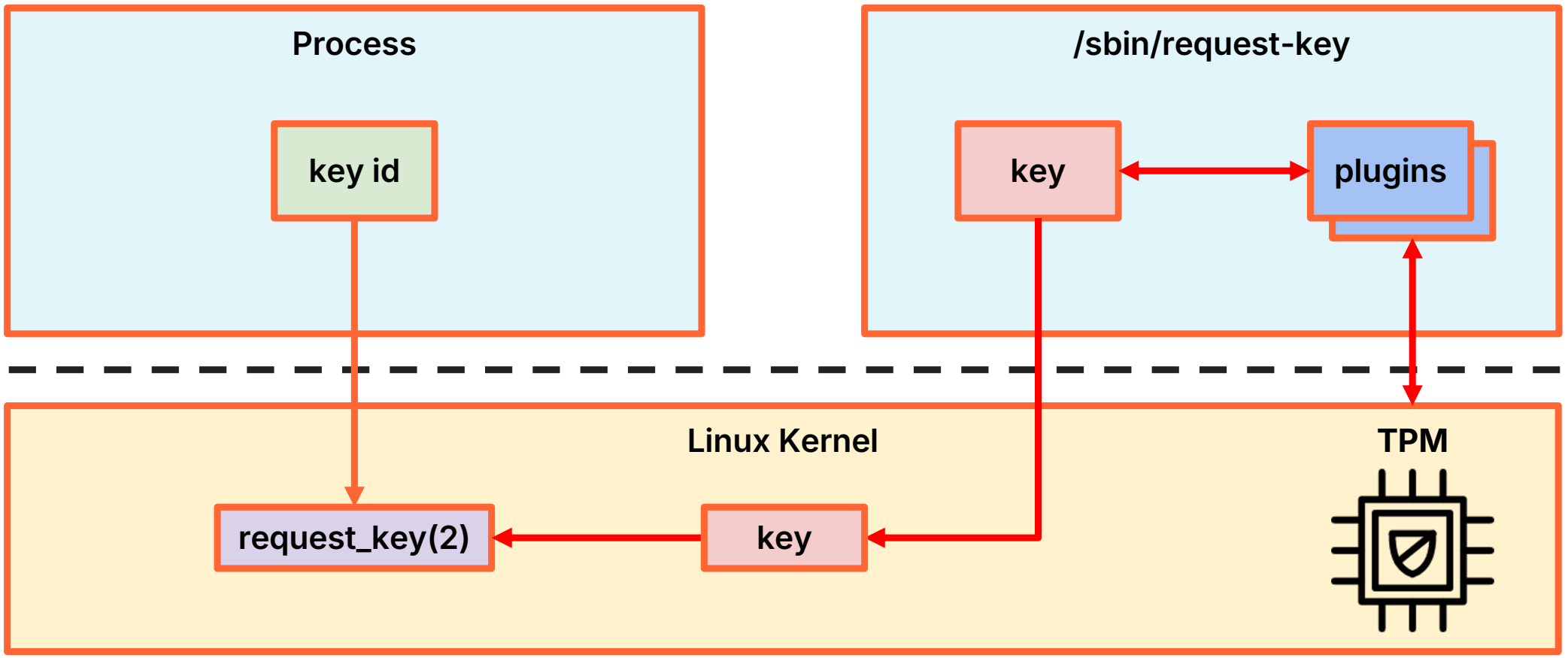
CLOUDFLARE

request_key(2)



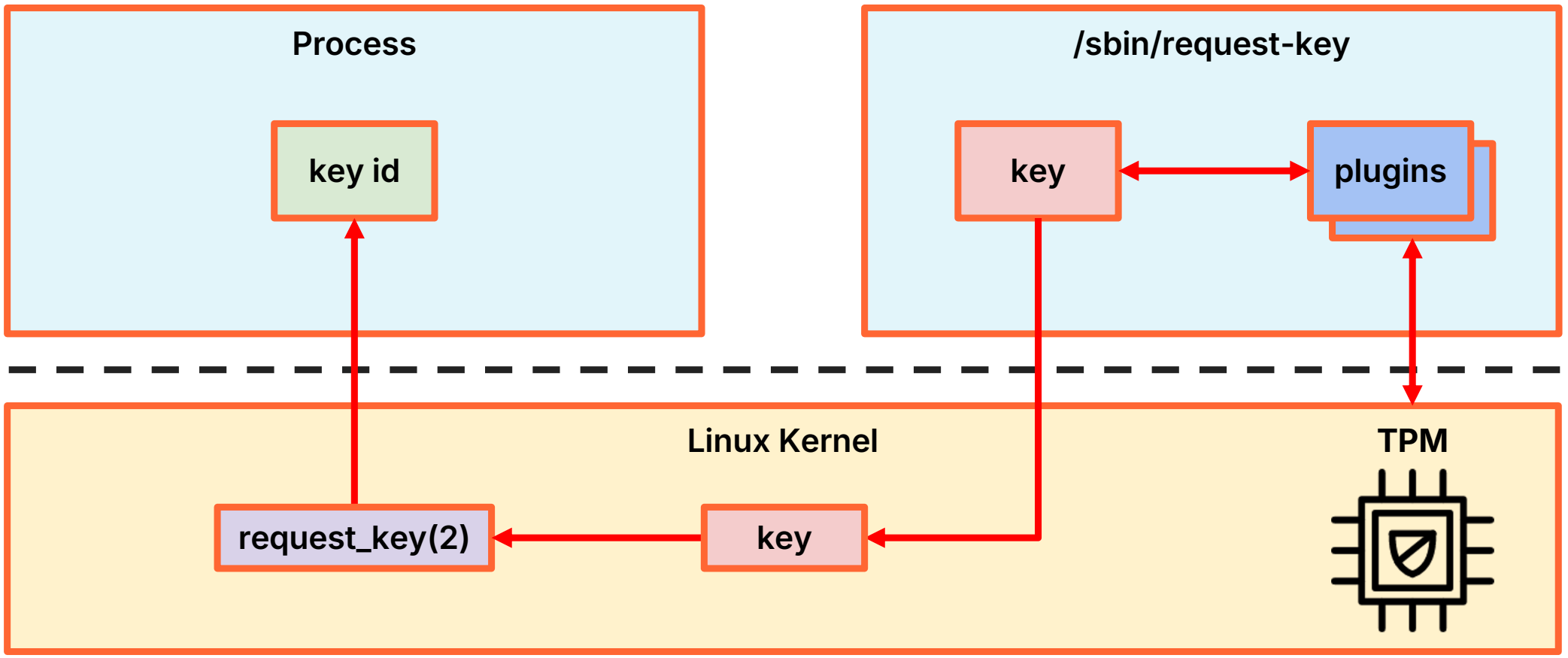
CLOUDFLARE

request_key(2)



CLOUDFLARE

request_key(2)



@ignatkn

CLOUDFLARE

TPM derived keys request_key(2) plugin

https://t.ly/0J6L-

@ignatkn

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ cat /etc/request-key.d/derived.conf
create * tpm2:derived:* * |/home/ignat/git/tpm-derived-keys/derived.py %t %d
%c %u %g
```

@ignatkn

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ cat /etc/request-key.d/derived.conf
create * tpm2:derived:* * |/home/ignat/git/tpm-derived-keys/derived.py %t %d
%c %u %g
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
655215536
```

@ignatkn

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ cat /etc/request-key.d/derived.conf
create * tpm2:derived:* * |/home/ignat/git/tpm-derived-keys/derived.py %t %d
%c %u %g
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
655215536
ignat@dev:~$ keyctl print 655215536
:hex:72b7392c62c9279806983 04f20b9d0d01d0b7fee3e54bba0c180086c940df023
```

@ignatkn

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ cat /etc/request-key.d/derived.conf
create * tpm2:derived:* * |/home/ignat/git/tpm-derived-keys/derived.py %t %d
%c %u %g
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
655215536
ignat@dev:~$ keyctl print 655215536
:hex:72b7392c62c927980698304f20b9d0d01d0b7fee3e54bba0c180086c940df023
ignat@dev:~$ keyctl unlink 655215536
1 links removed
```

@ignatkn

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ cat /etc/request-key.d/derived.conf
create * tpm2:derived:* * |/home/ignat/git/tpm-derived-keys/derived.py %t %d
%c %u %g
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
655215536
ignat@dev:~$ keyctl print 655215536
:hex:72b7392c62c9279806983 04f20b9d0d01d0b7fee3e54bba0c180086c940df023
ignat@dev:~$ keyctl unlink 655215536
1 links removed
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
806632423
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ cat /etc/request-key.d/derived.conf
create * tpm2:derived:* * |/home/ignat/git/tpm-derived-keys/derived.py %t %d
%c %u %g
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
655215536
ignat@dev:~$ keyctl print 655215536
:hex:72b7392c62c927980698304f20b9d0d01d0b7fee3e54bba0c180086c940df023
ignat@dev:~$ keyctl unlink 655215536
1 links removed
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
806632423
ignat@dev:~$ keyctl print 806632423
:hex:72b7392c62c927980698304f20b9d0d01d0b7fee3e54bba0c180086c940df023
```

@ignatkn

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ cat /etc/request-key.d/derived.conf
create * tpm2:derived:* * |/home/ignat/git/tpm-derived-keys/derived.py %t %d
%c %u %g
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
655215536
ignat@dev:~$ keyctl print 655215536
:hex:72b7392c62c927980698304f20b9d0d01d0b7fee3e54bba0c180086c940df023
ignat@dev:~$ keyctl unlink 655215536
1 links removed
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
806632423
ignat@dev:~$ keyctl print 806632423
:hex:72b7392c62c927980698304f20b9d0d01d0b7fee3e54bba0c180086c940df023
ignat@dev:~$ keyctl unlink 806632423
1 links removed
```

@ignatkn

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
806632423
ignat@dev:~$ keyctl print 806632423
:hex:72b7392c62c927980698304f20b9d0d01d0b7fee3e54bba0c180086c940df023
ignat@dev:~$ keyctl unlink 806632423
1 links removed
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
806632423
ignat@dev:~$ keyctl print 806632423
:hex:72b7392c62c927980698304f20b9d0d01d0b7fee3e54bba0c180086c940df023
ignat@dev:~$ keyctl unlink 806632423
1 links removed
ignat@dev:~$ cp /usr/bin/keyctl ./
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
806632423
ignat@dev:~$ keyctl print 806632423
:hex:72b7392c62c927980698304f20b9d0d01d0b7fee3e54bba0c180086c940df023
ignat@dev:~$ keyctl unlink 806632423
1 links removed
ignat@dev:~$ cp /usr/bin/keyctl ./
ignat@dev:~$ ./keyctl request2 user tpm2:derived:test "32 path" @s
302248702
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
806632423
ignat@dev:~$ keyctl print 806632423
:hex:72b7392c62c927980698304f20b9d0d01d0b7fee3e54bba0c180086c940df023
ignat@dev:~$ keyctl unlink 806632423
1 links removed
ignat@dev:~$ cp /usr/bin/keyctl ./
ignat@dev:~$ ./keyctl request2 user tpm2:derived:test "32 path" @s
302248702
ignat@dev:~$ keyctl print 302248702
:hex:21e346d301e9a3be6053505bd753cf68515fd152b5665ead6a4ec253371d2716
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
806632423
ignat@dev:~$ keyctl print 806632423
:hex:72b7392c62c927980698304f20b9d0d01d0b7fee3e54bba0c180086c940df023
ignat@dev:~$ keyctl unlink 806632423
1 links removed
ignat@dev:~$ cp /usr/bin/keyctl ./
ignat@dev:~$ ./keyctl request2 user tpm2:derived:test "32 path" @s
302248702
ignat@dev:~$ keyctl print 302248702
:hex:21e346d301e9a3be6053505bd753cf68515fd152b5665ead6a4ec253371d2716
ignat@dev:~$ keyctl unlink 302248702
1 links removed
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
806632423
ignat@dev:~$ keyctl print 806632423
:hex:72b7392c62c927980698304f20b9d0d01d0b7fee3e54bba0c180086c940df023
ignat@dev:~$ keyctl unlink 806632423
1 links removed
ignat@dev:~$ cp /usr/bin/keyctl ./
ignat@dev:~$ ./keyctl request2 user tpm2:derived:test "32 path" @s
302248702
ignat@dev:~$ keyctl print 302248702
:hex:21e346d301e9a3be6053505bd753cf68515fd152b5665ead6a4ec253371d2716
ignat@dev:~$ keyctl unlink 302248702
1 links removed
ignat@dev:~$ sudo ./keyctl request2 user tpm2:derived:test "32 path" @s
1037265117
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ /usr/bin/keyctl request2 user tpm2:derived:test "32 path" @s
806632423
ignat@dev:~$ keyctl print 806632423
:hex:72b7392c62c927980698304f20b9d0d01d0b7fee3e54bba0c180086c940df023
ignat@dev:~$ keyctl unlink 806632423
1 links removed
ignat@dev:~$ cp /usr/bin/keyctl ./
ignat@dev:~$ ./keyctl request2 user tpm2:derived:test "32 path" @s
302248702
ignat@dev:~$ keyctl print 302248702
:hex:21e346d301e9a3be6053505bd753cf68515fd152b5665ead6a4ec253371d2716
ignat@dev:~$ keyctl unlink 302248702
1 links removed
ignat@dev:~$ sudo ./keyctl request2 user tpm2:derived:test "32 path" @s
1037265117
ignat@dev:~$ keyctl print 1037265117
:hex:93130b4be4bc1a8fbc1d9fec3374ad5dc5698419982119352fd3c2e4ee22e577
```

@ignatkn

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ ./keyctl request2 user tpm2:derived:test "32 csum" @s
807021204
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ ./keyctl request2 user tpm2:derived:test "32 csum" @s
807021204
ignat@dev:~$ keyctl print 807021204
:hex:f638e269b0ebf1830faef47e0b4ba898220b5f8b77ae44a2fab0c2e41d13ba28
```

@ignatkn

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ ./keyctl request2 user tpm2:derived:test "32 csum" @s
807021204
ignat@dev:~$ keyctl print 807021204
:hex:f638e269b0ebf1830faef47e0b4ba898220b5f8b77ae44a2fab0c2e41d13ba28
ignat@dev:~$ keyctl unlink 807021204
1 links removed
```

@ignatkn

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ ./keyctl request2 user tpm2:derived:test "32 csum" @s
807021204
ignat@dev:~$ keyctl print 807021204
:hex:f638e269b0ebf1830faef47e0b4ba898220b5f8b77ae44a2fab0c2e41d13ba28
ignat@dev:~$ keyctl unlink 807021204
1 links removed
ignat@dev:~$ cp ./keyctl ./keyctl2
```

@ignatkn

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ ./keyctl request2 user tpm2:derived:test "32 csum" @s
807021204
ignat@dev:~$ keyctl print 807021204
:hex:f638e269b0ebf1830faef47e0b4ba898220b5f8b77ae44a2fab0c2e41d13ba28
ignat@dev:~$ keyctl unlink 807021204
1 links removed
ignat@dev:~$ cp ./keyctl ./keyctl2
ignat@dev:~$ ./keyctl2 request2 user tpm2:derived:test "32 csum" @s
776827534
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ ./keyctl request2 user tpm2:derived:test "32 csum" @s
807021204
ignat@dev:~$ keyctl print 807021204
:hex:f638e269b0ebf1830faef47e0b4ba898220b5f8b77ae44a2fab0c2e41d13ba28
ignat@dev:~$ keyctl unlink 807021204
1 links removed
ignat@dev:~$ cp ./keyctl ./keyctl2
ignat@dev:~$ ./keyctl2 request2 user tpm2:derived:test "32 csum" @s
776827534
ignat@dev:~$ keyctl print 776827534
:hex:f638e269b0ebf1830faef47e0b4ba898220b5f8b77ae44a2fab0c2e41d13ba28
```

@ignatkn

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ ./keyctl request2 user tpm2:derived:test "32 csum" @s
807021204
ignat@dev:~$ keyctl print 807021204
:hex:f638e269b0ebf1830faef47e0b4ba898220b5f8b77ae44a2fab0c2e41d13ba28
ignat@dev:~$ keyctl unlink 807021204
1 links removed
ignat@dev:~$ cp ./keyctl ./keyctl2
ignat@dev:~$ ./keyctl2 request2 user tpm2:derived:test "32 csum" @s
776827534
ignat@dev:~$ keyctl print 776827534
:hex:f638e269b0ebf1830faef47e0b4ba898220b5f8b77ae44a2fab0c2e41d13ba28
ignat@dev:~$ keyctl unlink 776827534
1 links removed
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ ./keyctl request2 user tpm2:derived:test "32 csum" @s
807021204
ignat@dev:~$ keyctl print 807021204
:hex:f638e269b0ebf1830faef47e0b4ba898220b5f8b77ae44a2fab0c2e41d13ba28
ignat@dev:~$ keyctl unlink 807021204
1 links removed
ignat@dev:~$ cp ./keyctl ./keyctl2
ignat@dev:~$ ./keyctl2 request2 user tpm2:derived:test "32 csum" @s
776827534
ignat@dev:~$ keyctl print 776827534
:hex:f638e269b0ebf1830faef47e0b4ba898220b5f8b77ae44a2fab0c2e41d13ba28
ignat@dev:~$ keyctl unlink 776827534
1 links removed
ignat@dev:~$ sed -i 's/Bad message/Bad massage/' ./keyctl2
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ ./keyctl request2 user tpm2:derived:test "32 csum" @s
807021204
ignat@dev:~$ keyctl print 807021204
:hex:f638e269b0ebf1830faef47e0b4ba898220b5f8b77ae44a2fab0c2e41d13ba28
ignat@dev:~$ keyctl unlink 807021204
1 links removed
ignat@dev:~$ cp ./keyctl ./keyctl2
ignat@dev:~$ ./keyctl2 request2 user tpm2:derived:test "32 csum" @s
776827534
ignat@dev:~$ keyctl print 776827534
:hex:f638e269b0ebf1830faef47e0b4ba898220b5f8b77ae44a2fab0c2e41d13ba28
ignat@dev:~$ keyctl unlink 776827534
1 links removed
ignat@dev:~$ sed -i 's/Bad message/Bad massage/' ./keyctl2
ignat@dev:~$ ./keyctl2 request2 user tpm2:derived:test "32 csum" @s
732784450
```

@ignatkn

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ ./keyctl request2 user tpm2:derived:test "32 csum" @s
807021204
ignat@dev:~$ keyctl print 807021204
:hex:f638e269b0ebf1830faef47e0b4ba898220b5f8b77ae44a2fab0c2e41d13ba28
ignat@dev:~$ keyctl unlink 807021204
1 links removed
ignat@dev:~$ cp ./keyctl ./keyctl2
ignat@dev:~$ ./keyctl2 request2 user tpm2:derived:test "32 csum" @s
776827534
ignat@dev:~$ keyctl print 776827534
:hex:f638e269b0ebf1830faef47e0b4ba898220b5f8b77ae44a2fab0c2e41d13ba28
ignat@dev:~$ keyctl unlink 776827534
1 links removed
ignat@dev:~$ sed -i 's/Bad message/Bad massage/' ./keyctl2
ignat@dev:~$ ./keyctl2 request2 user tpm2:derived:test "32 csum" @s
732784450
ignat@dev:~$ keyctl print 732784450
:hex:15257529326a3b5874d2e4165245a2c4a758b3e6c549e876e3b808fe8a748c80
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ keyctl request2 asymmetric tpm2:derived:test "32 csum" @s
700095445
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ keyctl request2 asymmetric tpm2:derived:test "32 csum" @s
700095445
ignat@dev:~$ echo abc | openssl sha256 -binary > abc.sha256
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ keyctl request2 asymmetric tpm2:derived:test "32 csum" @s
700095445
ignat@dev:~$ echo abc | openssl sha256 -binary > abc.sha256
ignat@dev:~$ keyctl pkey_sign 700095445 0 abc.sha256 enc=pkcs1 hash=sha256 |
openssl sha256
SHA2-256(stdin)=
bb82fda82a8cbfd2ff96d52258234c9eb565b807784fbb79ac422a0caa2b48c4
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ keyctl request2 asymmetric tpm2:derived:test "32 csum" @s
700095445
ignat@dev:~$ echo abc | openssl sha256 -binary > abc.sha256
ignat@dev:~$ keyctl pkey_sign 700095445 0 abc.sha256 enc=pkcs1 hash=sha256 |
openssl sha256
SHA2-256(stdin)=
bb82fda82a8cbfd2ff96d52258234c9eb565b807784fbb79ac422a0caa2b48c4
ignat@dev:~$ keyctl unlink 700095445
1 links removed
```

CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ keyctl request2 asymmetric tpm2:derived:test "32 csum" @s
700095445
ignat@dev:~$ echo abc | openssl sha256 -binary > abc.sha256
ignat@dev:~$ keyctl pkey_sign 700095445 0 abc.sha256 enc=pkcs1 hash=sha256 |
openssl sha256
SHA2-256(stdin)=
bb82fda82a8cbfd2ff96d52258234c9eb565b807784fbb79ac422a0caa2b48c4
ignat@dev:~$ keyctl unlink 700095445
1 links removed
ignat@dev:~$ keyctl request2 asymmetric tpm2:derived:test "32 csum" @s
734509723
```

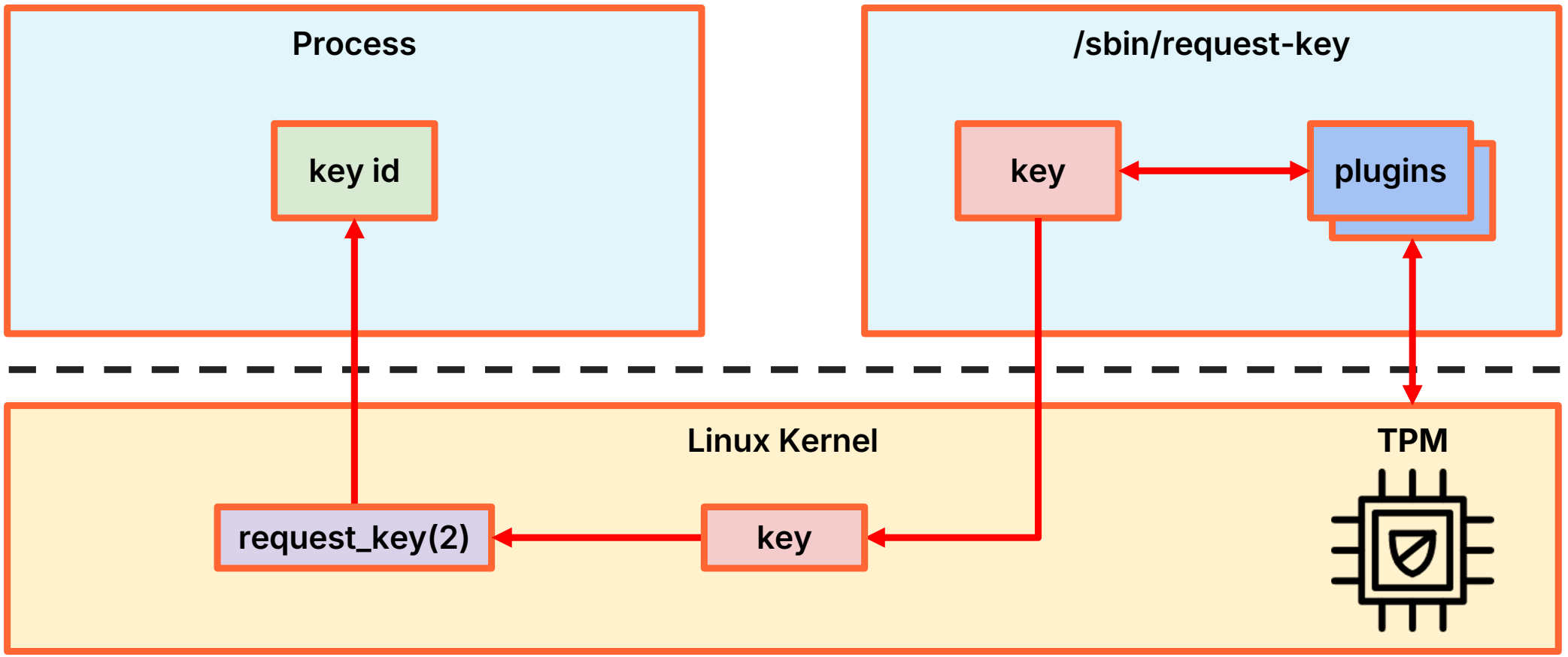
CLOUDFLARE

TPM derived keys via request_key(2)

```
ignat@dev:~$ keyctl request2 asymmetric tpm2:derived:test "32 csum" @s
700095445
ignat@dev:~$ echo abc | openssl sha256 -binary > abc.sha256
ignat@dev:~$ keyctl pkey_sign 700095445 0 abc.sha256 enc=pkcs1 hash=sha256 |
openssl sha256
SHA2-256(stdin)=
bb82fda82a8cbfd2ff96d52258234c9eb565b807784fbb79ac422a0caa2b48c4
ignat@dev:~$ keyctl unlink 700095445
1 links removed
ignat@dev:~$ keyctl request2 asymmetric tpm2:derived:test "32 csum" @s
734509723
ignat@dev:~$ keyctl pkey_sign 734509723 0 abc.sha256 enc=pkcs1 hash=sha256 |
openssl sha256
SHA2-256(stdin)=
bb82fda82a8cbfd2ff96d52258234c9eb565b807784fbb79ac422a0caa2b48c4
```

CLOUDFLARE

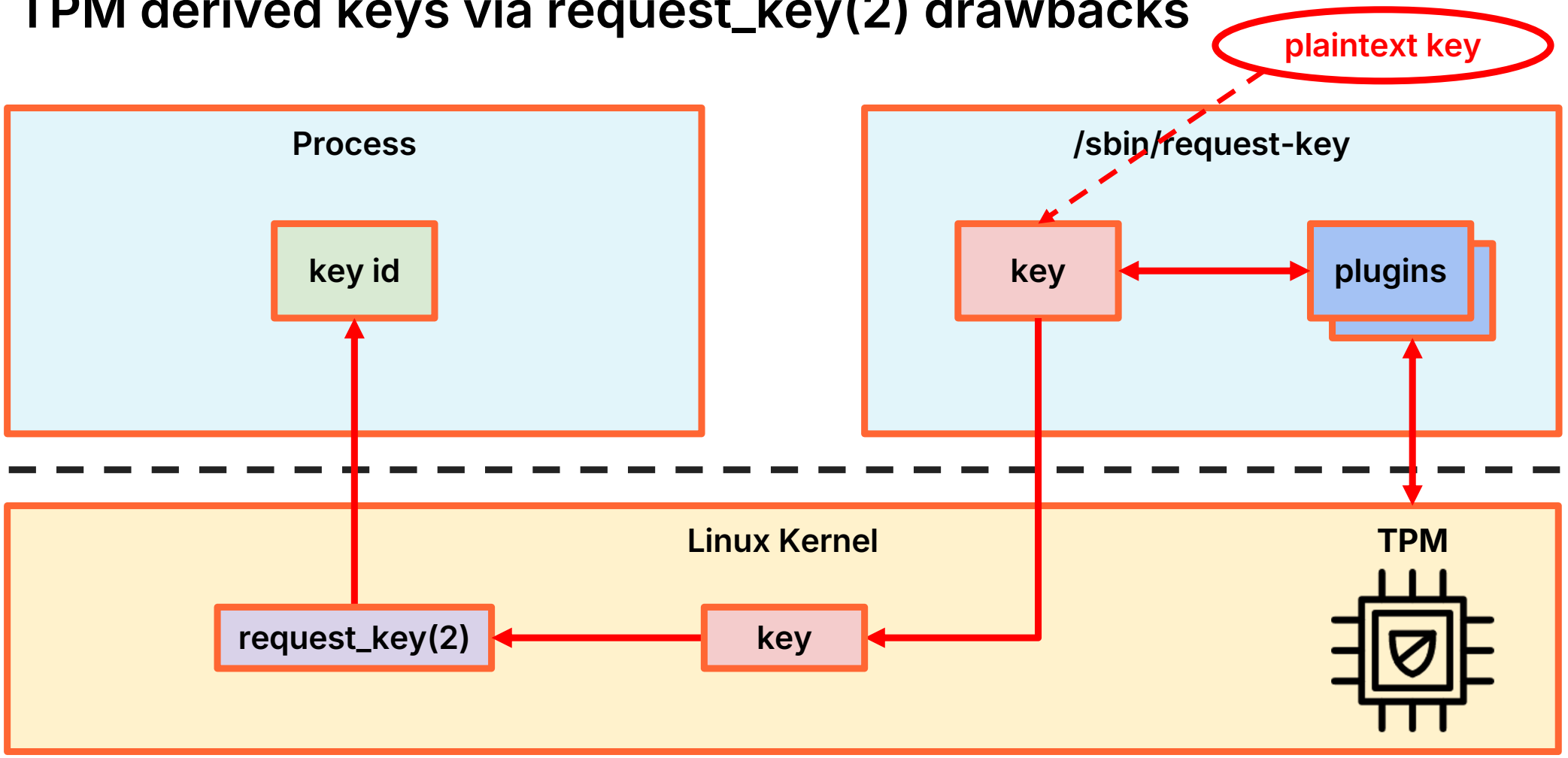
TPM derived keys via request_key(2) drawbacks



@ignatkn

CLOUDFLARE

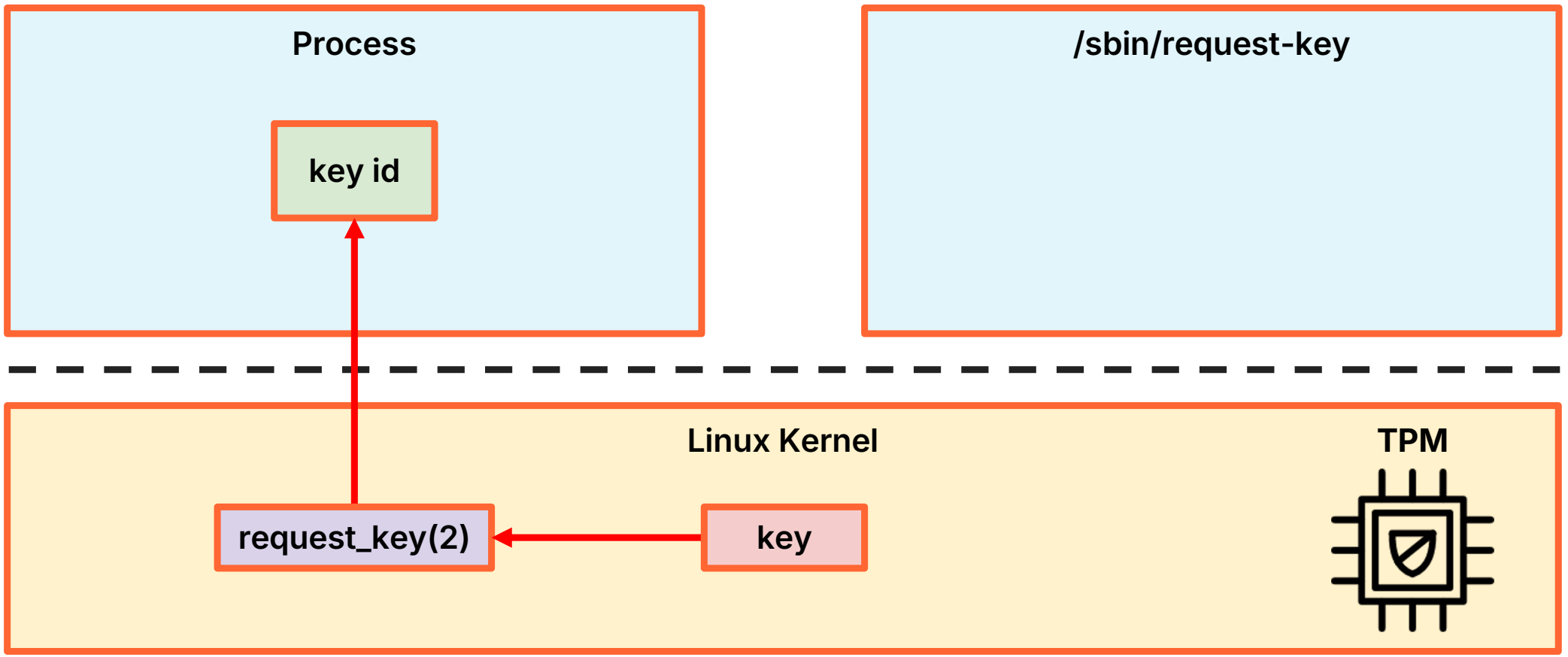
TPM derived keys via request_key(2) drawbacks



@ignatkn

CLOUDFLARE

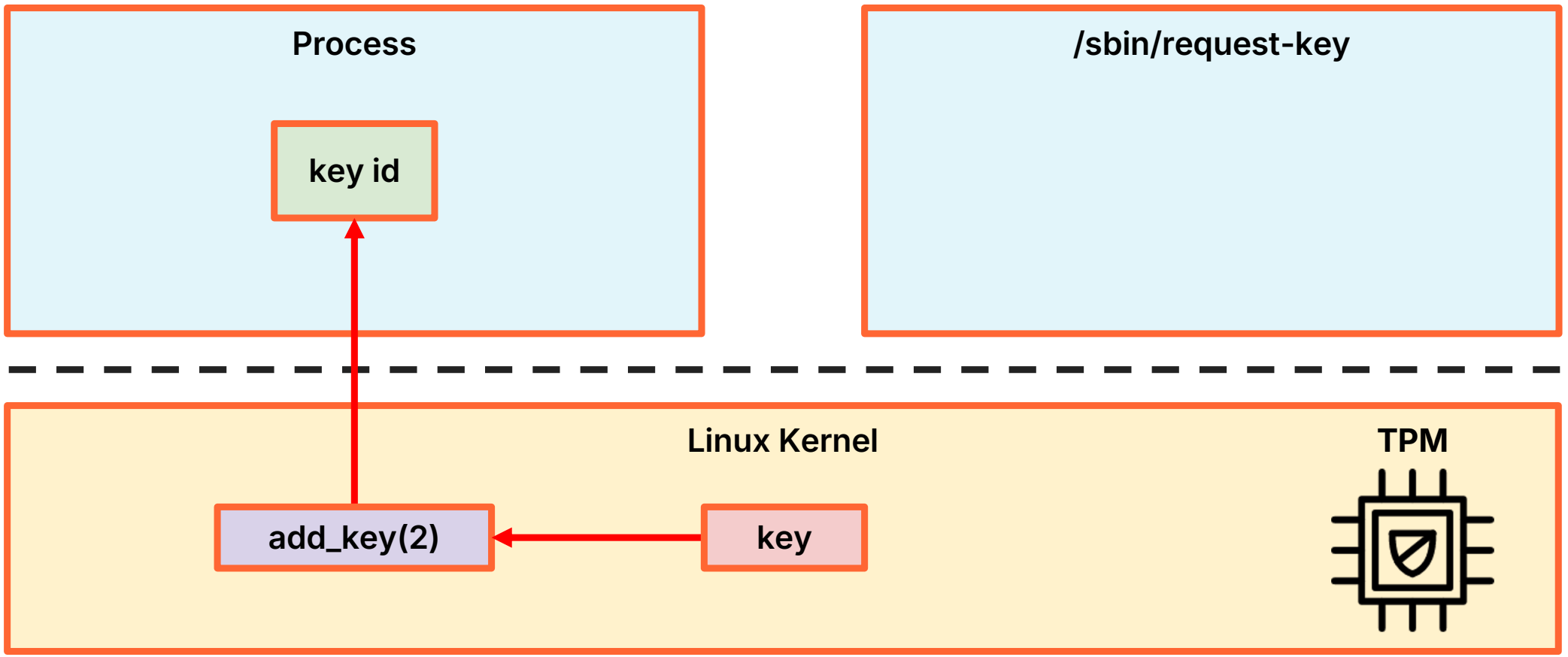
TPM derived keys directly in the kernel



@ignatkn

CLOUDFLARE

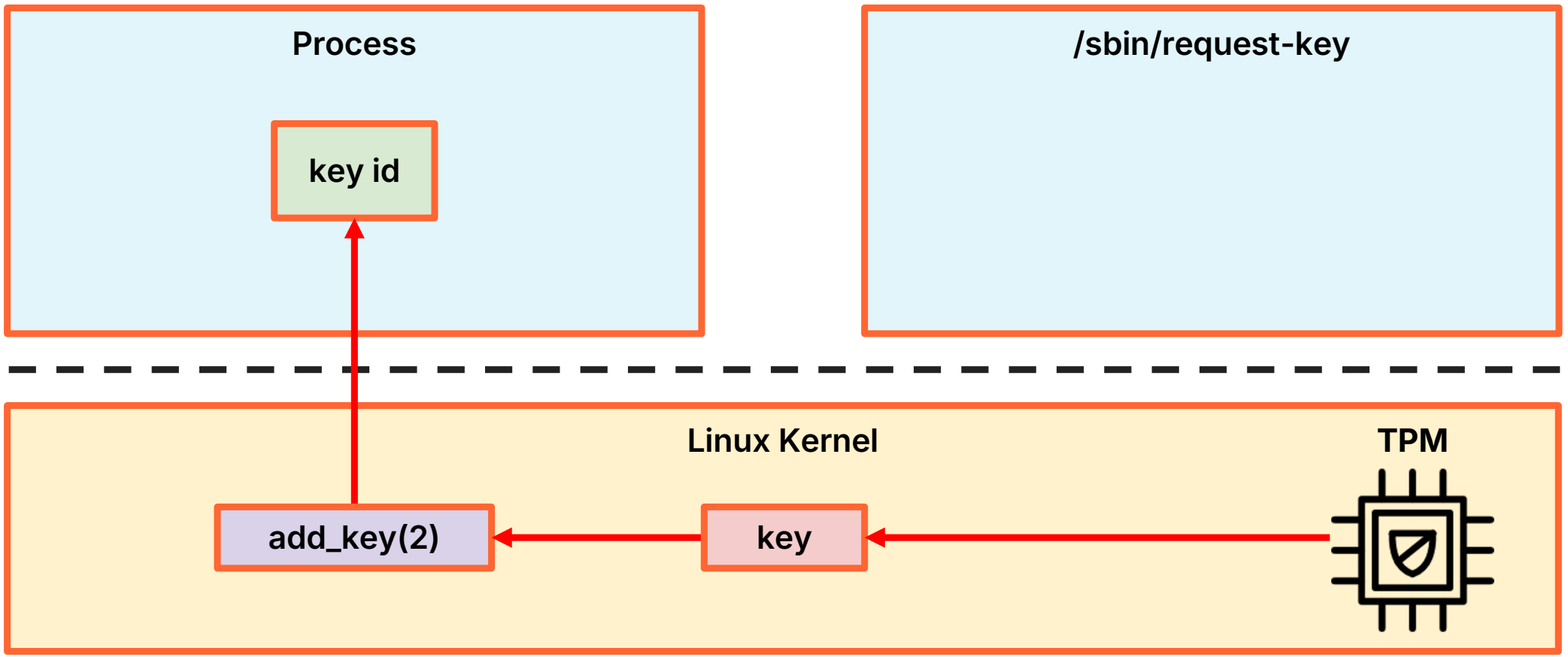
TPM derived keys directly in the kernel



@ignatkn

CLOUDFLARE

TPM derived keys directly in the kernel



CLOUDFLARE

TPM derived keys request_key(2) plugin

https://lore.kernel.org/linux-kernel/20240503221634.44274-2-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”

CLOUDFLARE

Conclusions

- Interfacing with TPMs is hard, so applications avoid them altogether

CLOUDFLARE

Conclusions

- Interfacing with TPMs is hard, so applications avoid them altogether
- Linux Kernel key retention service (keystore) can be a good layer to abstract away the TPM interaction complexity for applications
  - but some additional development might be needed

CLOUDFLARE

Conclusions

- Interfacing with TPMs is hard, so applications avoid them altogether
- Linux Kernel key retention service (keystore) can be a good layer to abstract away the TPM interaction complexity for applications
  - but some additional development might be needed
- TPM derived keys is a good alternative to TPM wrapped keys providing similar hardware-backed security with potentially easier key management
  - can be implemented via a request_key(2) plugin for current kernels
  - in-kernel version is needed to avoid exposing the plaintext key material to userspace

CLOUDFLARE

Conclusions

- Interfacing with TPMs is hard, so applications avoid them altogether
- Linux Kernel key retention service (keystore) can be a good layer to abstract away the TPM interaction complexity for applications
  - but some additional development might be needed
- TPM derived keys is a good alternative to TPM wrapped keys providing similar hardware-backed security with potentially easier key management
  - can be implemented via a request_key(2) plugin for current kernels
  - in-kernel version is needed to avoid exposing the plaintext key material to userspace
- Exposing TPMs through Linux Kernel keystore can provide applications with a straightforward path to adopting hardware security without too much exposure to TPM internals
  - probably true for other security chips

CLOUDFLARE

Links

- https://www.kernel.org/doc/html/latest/security/keys/core.html
- https://www.kernel.org/doc/html/latest/security/keys/trusted-encrypted.html
- https://lore.kernel.org/lkml/20240528210823.28798-2-jarkko@kernel.org/T/
- https://gist.github.com/ignatk/9038d139e983ca355136aec7ec2d9bfc
- https://lore.kernel.org/linux-kernel/20240503221634.44274-2-ignat@cloudflare.com/T/

@ignatkn

CLOUDFLARE

Thank you!

Questions?