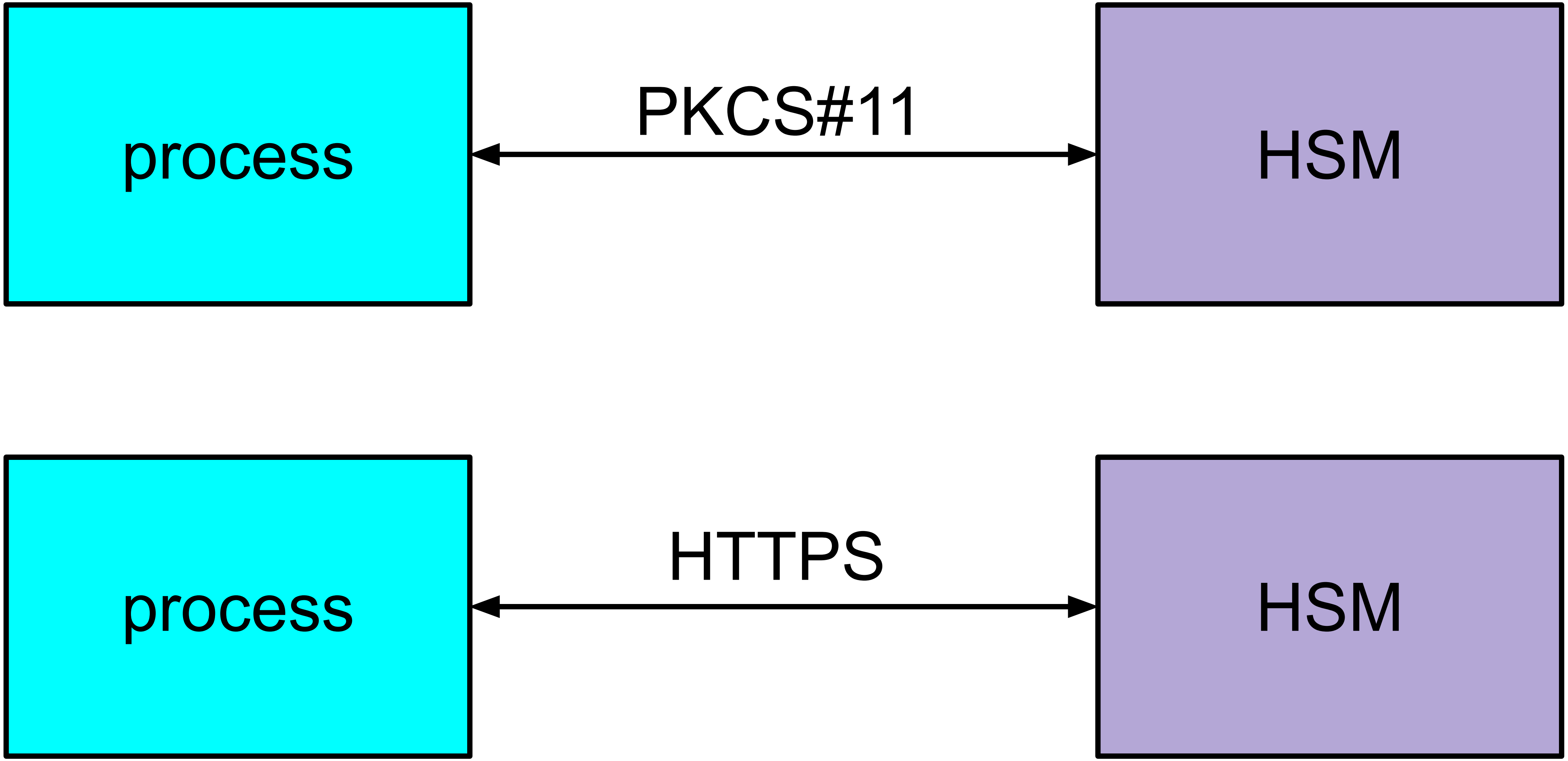
One Ring -3 To Secure Them All

Computing with Hardware Enclaves

Trusted

Execution Environment

How do you solve **secure execution** for **critically sensitive** data?



process

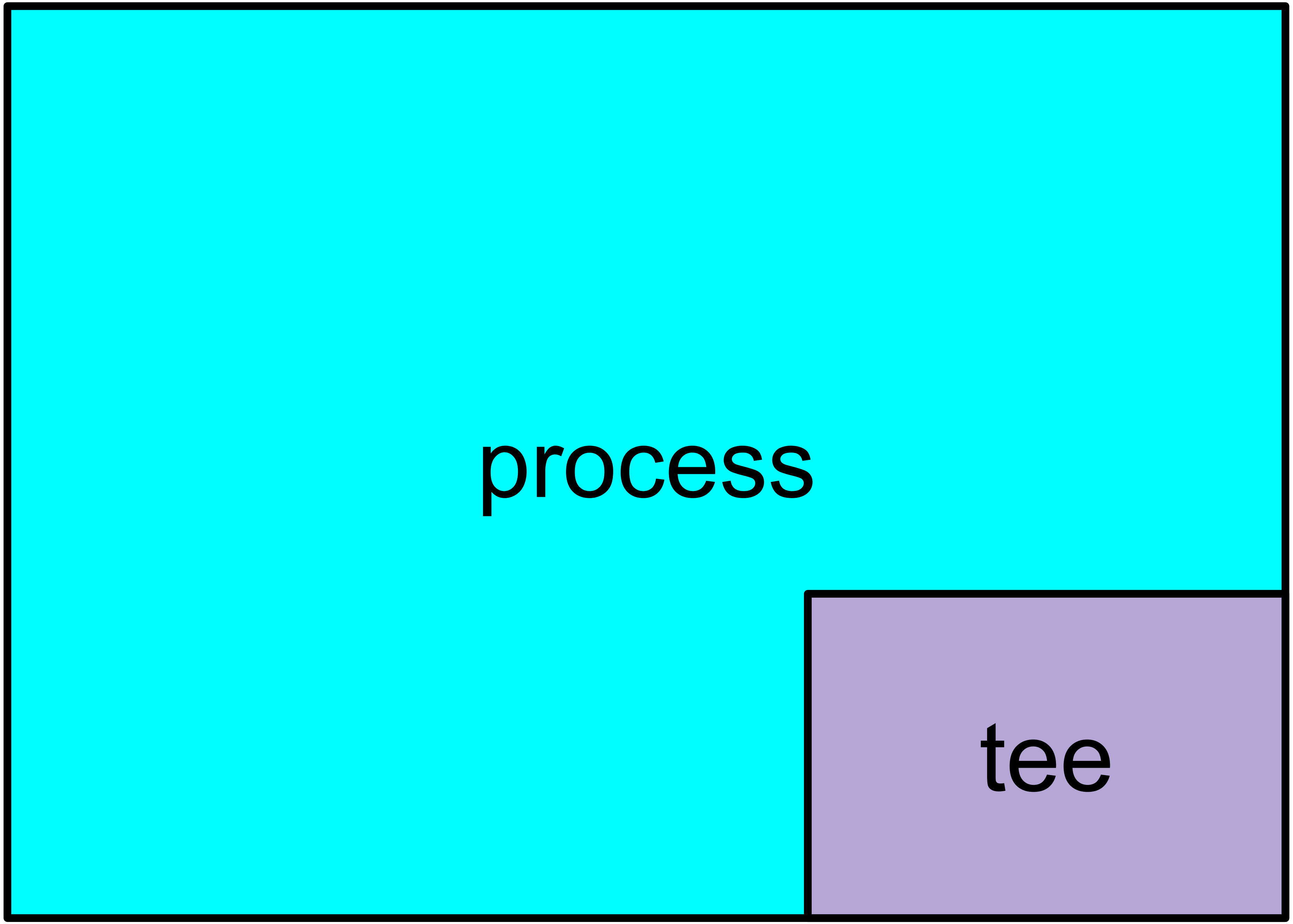
PKCS#11

HSM

process

HTTPS

HSM



process

tee

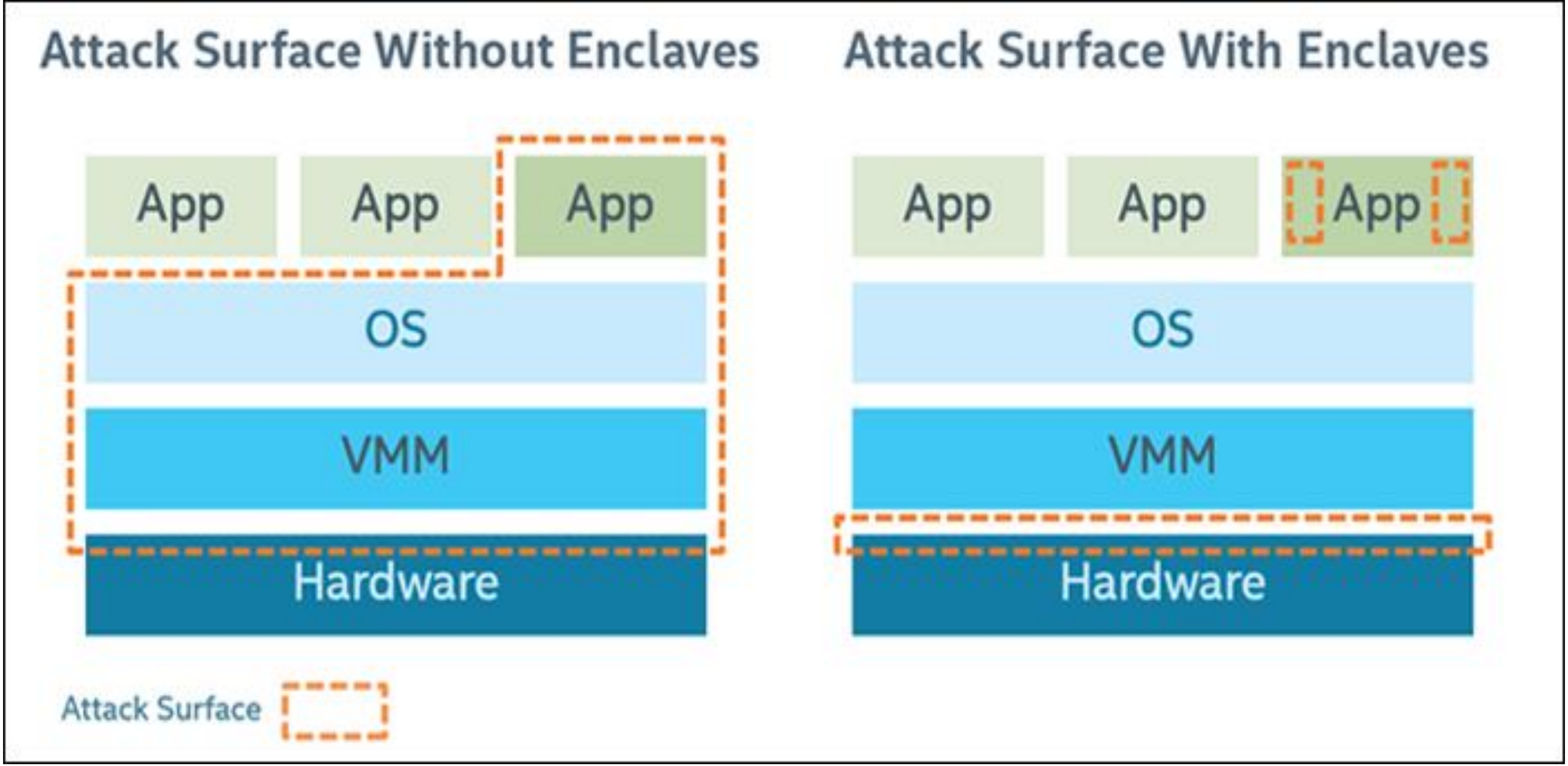
Not All Created **Equal**

Available Options*

- Intel SGX
- AMD SEV
- ARM TrustZone
- Apple Secure Enclave
- AWS Nitro Enclaves

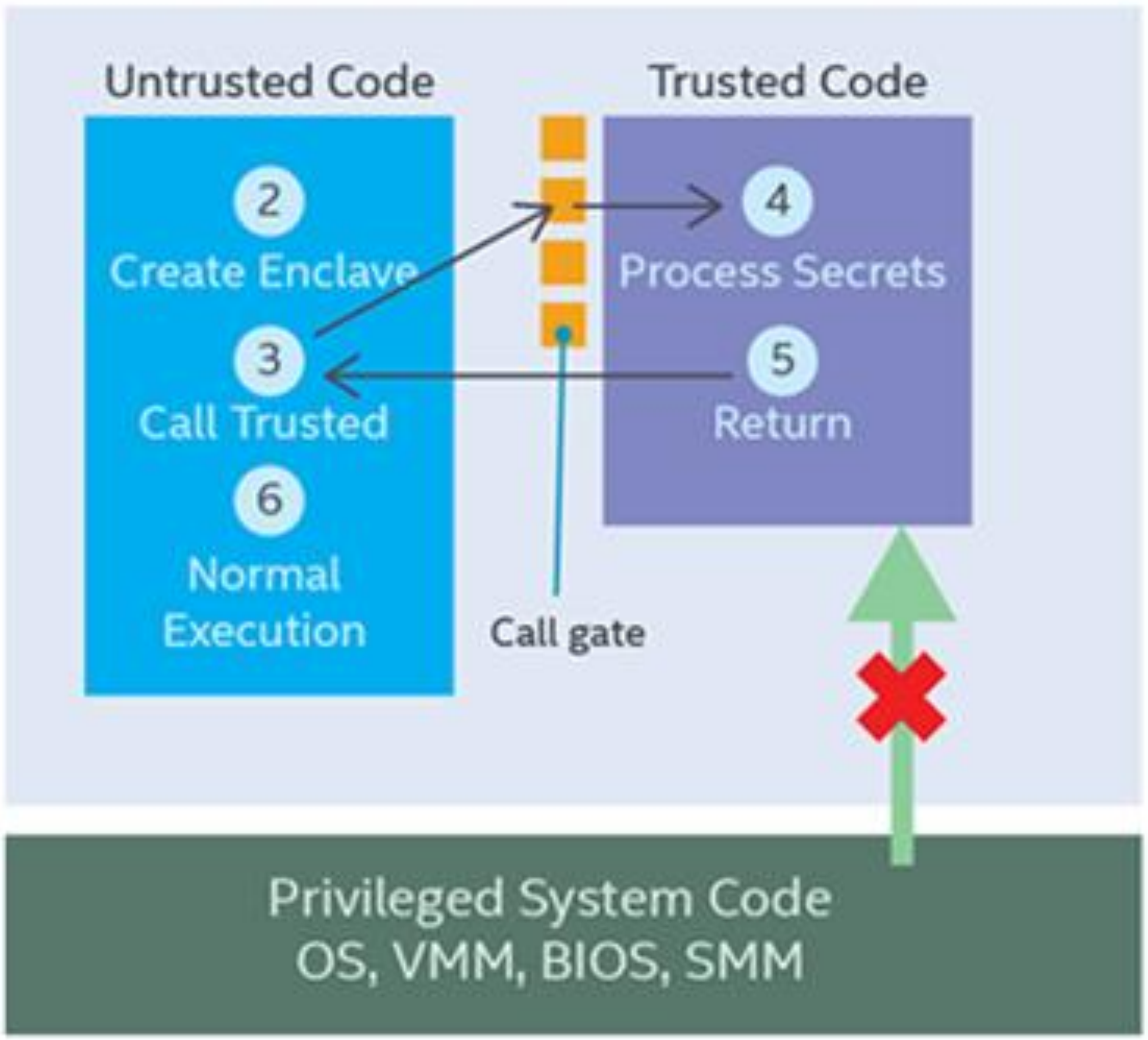
* Other options available. This list represents the most broadly applicable.

It represents a **change** in the **Threat Model**



https://software.intel.com/content/www/us/en/develop/articles/intel-software-guard-extensions-tutorial-part-1-foundation.html

1 Intel® SGX Application



1. App is built with trusted and untrusted parts
2. App runs and creates the enclave, which is placed in trusted memory
3. Trusted function is called, and execution is transitioned to the enclave
4. Enclave sees all process data in the clear; external access to the enclave data is denied
5. Function returns; enclave data remains in trusted memory
6. Normal execution resumes

https://software.intel.com/content/www/us/en/develop/articles/intel-software-guard-extensions-tutorial-part-1-foundation.html

First Impressions

Ergonomics:

Broad application: arm

Most depth:

intel®

Considerations

Performance

The **Threat Model** is **changed**, but **threats** still exist

Microcode issues are **difficult** to fix

Still **vulnerable** to **some speculative execution** attacks

Some designs rely on **protection rings** vs **true separation**

Some implementations are **gated** by the vendor

Some implementations are **difficult** to use

Some suffer from

limited availability

Hardware Enclaves are a **key component** in advancing the design of **secure software**

Secure design should consider tactical use of **hardware** to solve difficult **trust** problems

Links and References

- github.com/abedra/sgx_bootstrapping
- aaronbedra.com/post/sgx_getting_started
- hal.archives-ouvertes.fr/hal-02947792/document
- software.intel.com/content/www/us/en/develop/topics/software-guard-extensions.html
- developer.amd.com/sev
- developer.arm.com/ip-products/security-ip/trustzone
- aws.amazon.com/ec2/nitro/nitro-enclaves
- openenclave.io/sdk