WIBU SYSTEMS

SECURITY
LICENSING
PERFECTION IN PROTECTION

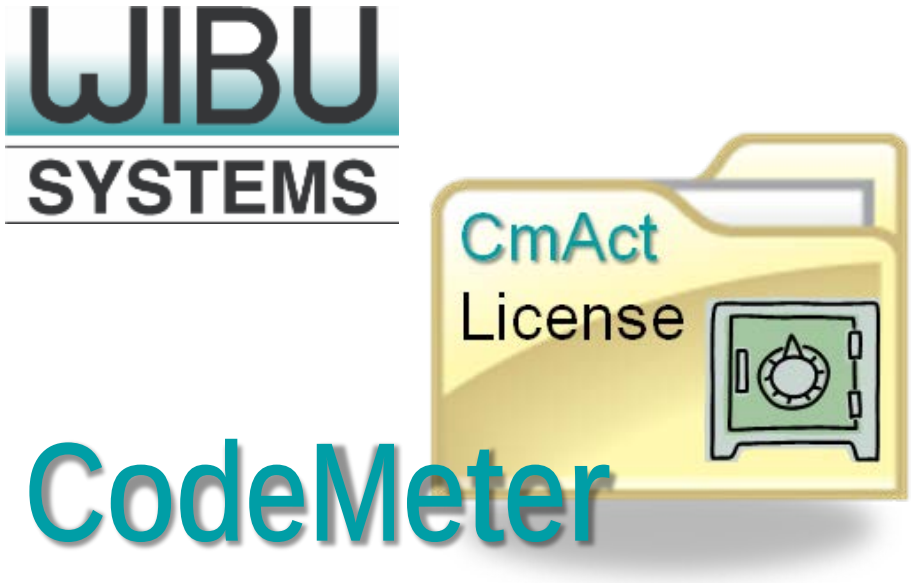
Security and Licensing in IoT Devices

Use of secure trusted execution environments (TEE) like Intel's SGX technology with Codemeter

Oliver Winzenried | CEO Wibu-Systems
oliver.winzenried@wibu.com

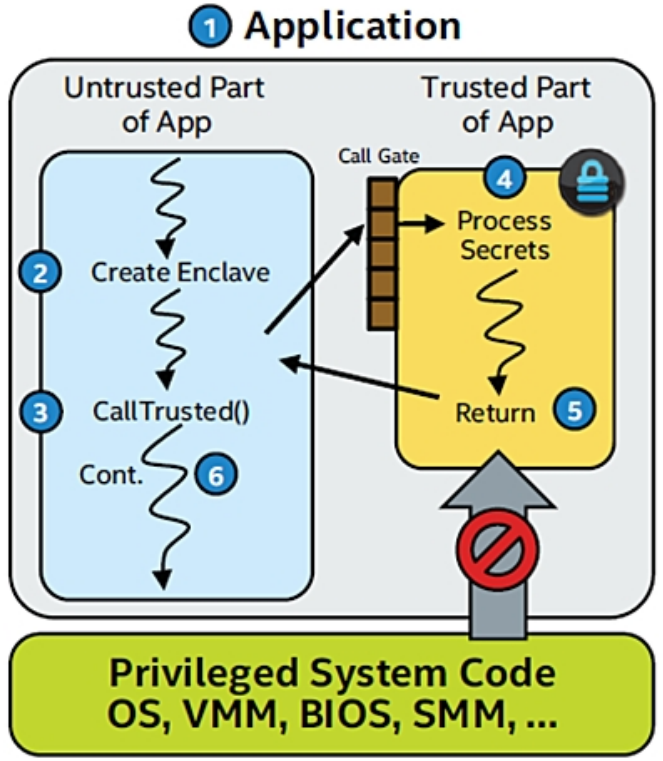
Trusted Execution Environments

Secure Software Protection and Licensing with SGX



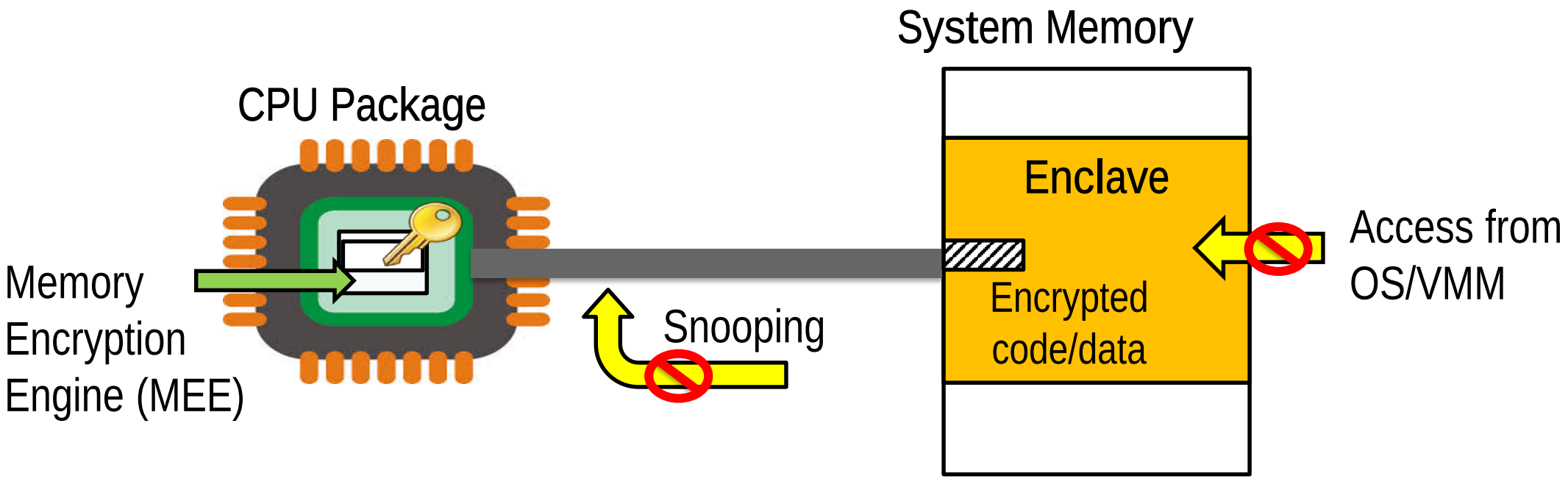
Intel SGX TEE

- Intel Software Guard Extensions – new instructions added to the x64 instruction set
- Incorporated directly into CPU, e.g., Intel i7-6700K, Dell Inspiron 11 i3153
- (Not a separate chip like TPM.)
- Application can created trusted memory “enclave”
- Only trusted functions (stored in enclave) can see or modify enclave
- Application software can be protected from privileged software



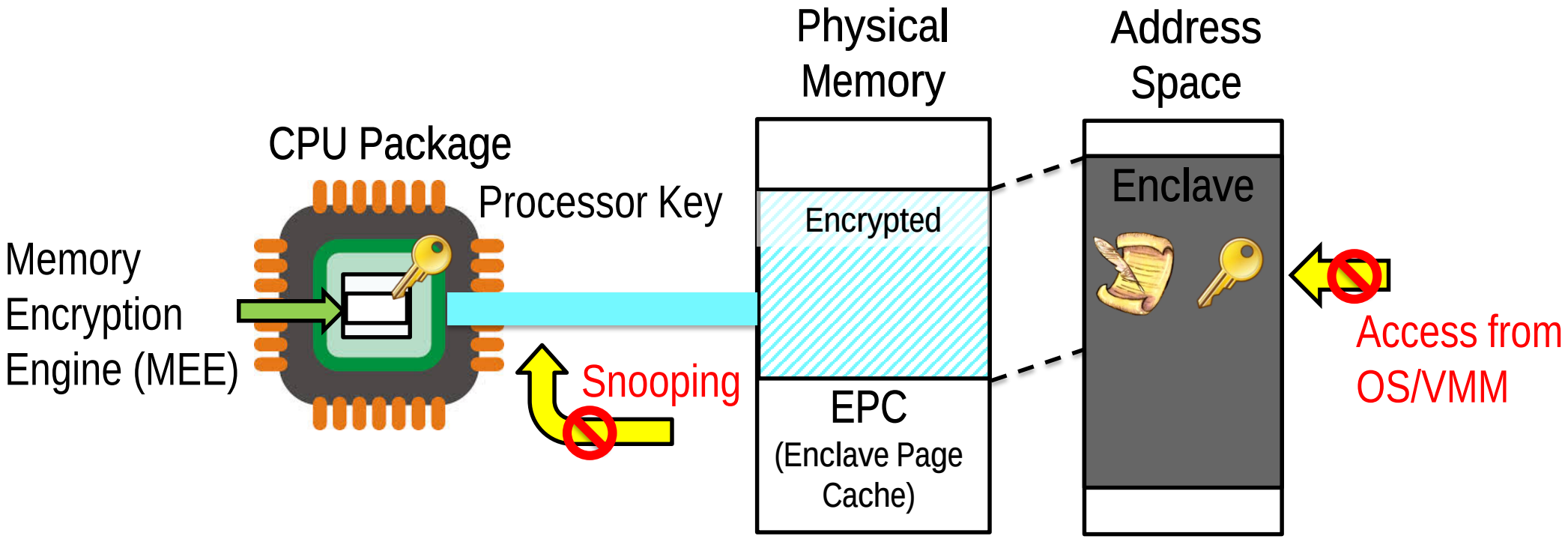
https://software.intel.com/en-us/sgx/details

Intel SGX TEE

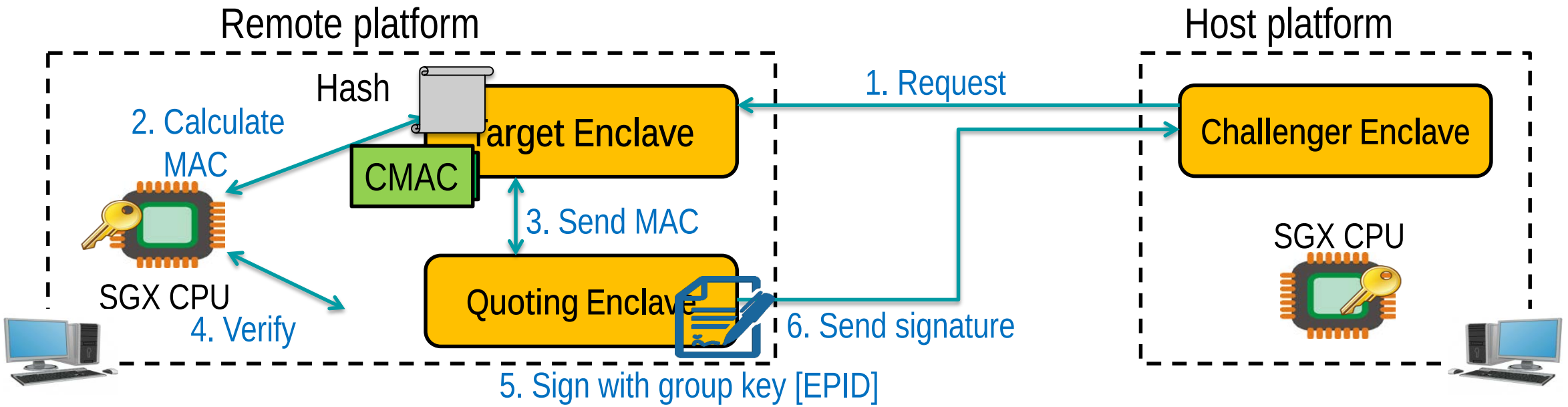


- Application keeps its data/code inside the "enclave"
  - Smallest attack surface by reducing TCB (App + processor)
  - Protect app's secret from untrusted privilege software (e.g., OS, VMM)

Intel SGX : Isolated execution

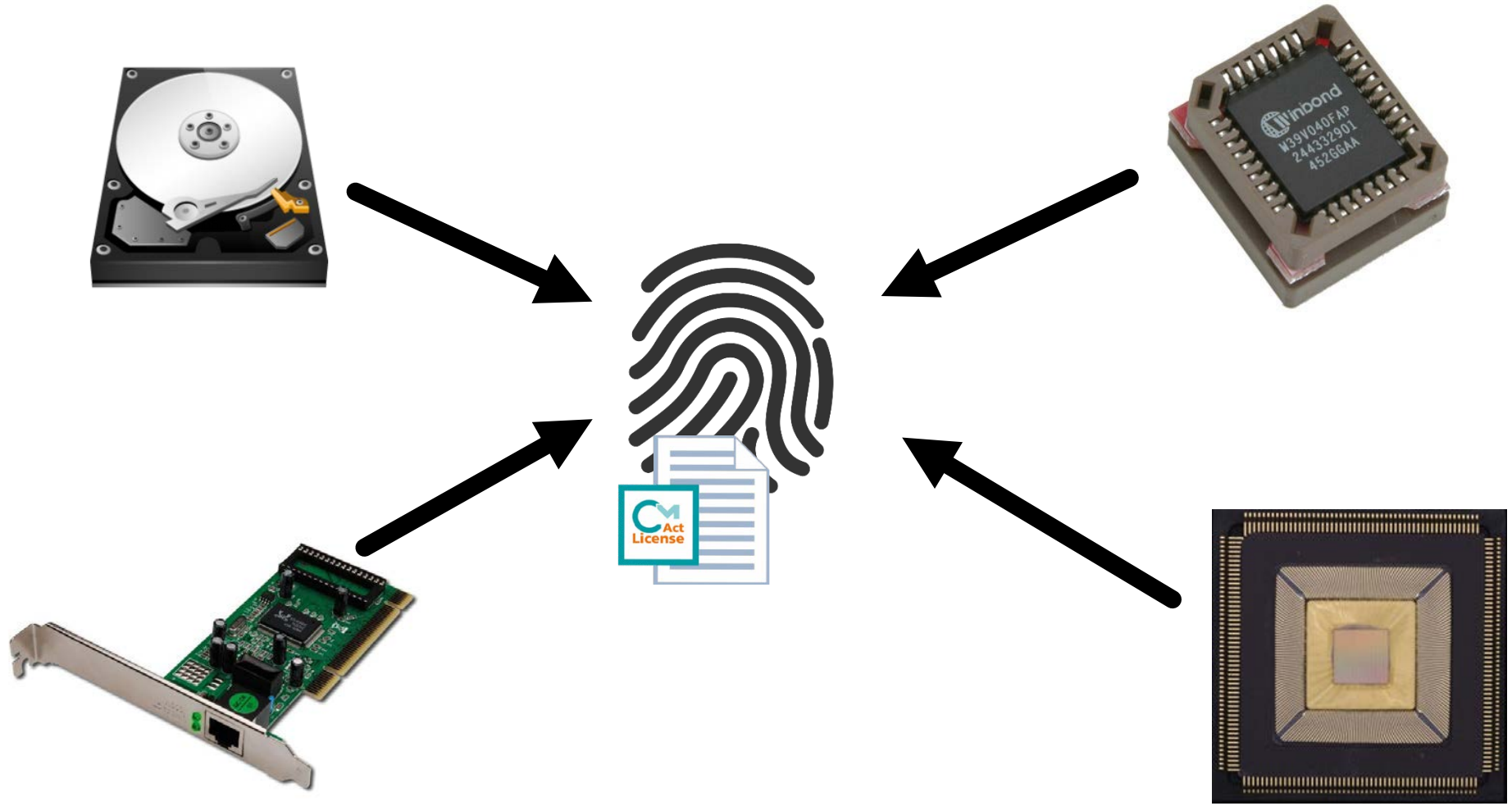


Intel SGX : Remote Attestation



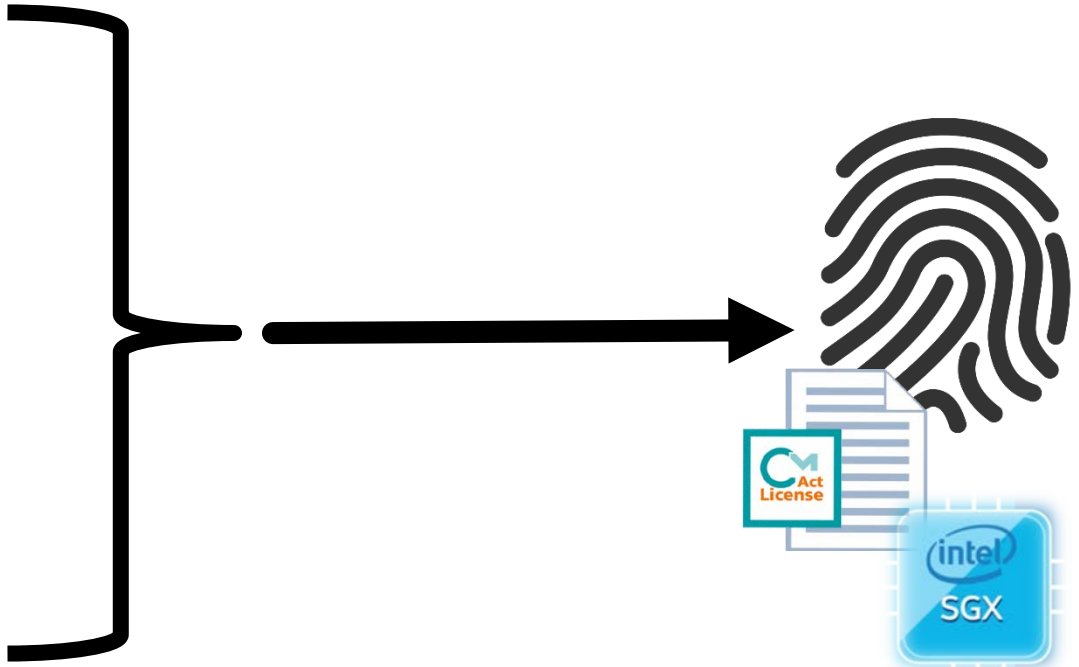
- Attest an application on remote platform
- Check the identity of enclave (**hash of code/data pages**)
- Can establish a "secure channel" between enclaves

Smartbind: Automatic Binding (HW Fingerprint)

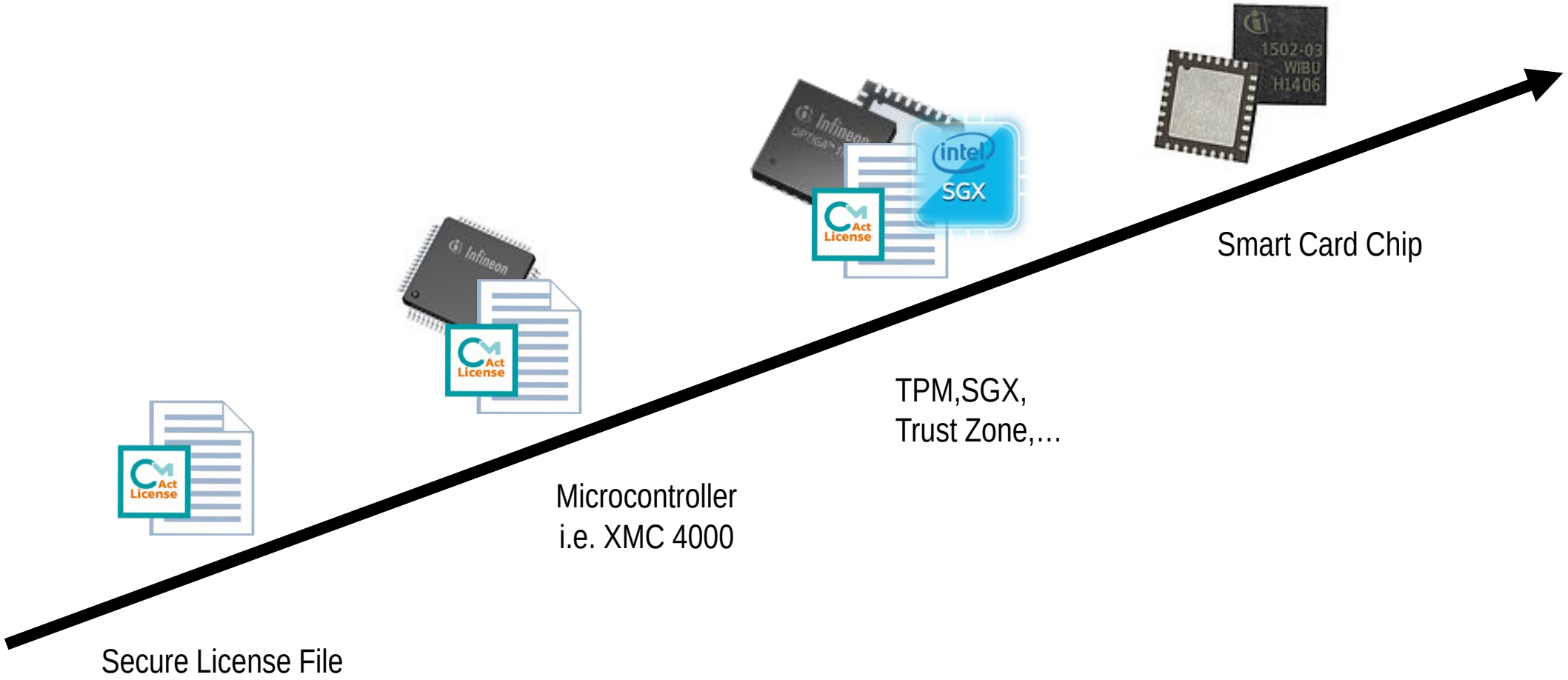


Individual Binding - Individual Implementation

- Non modifiable serial number
- Physical Uncloneable Function
- Non modifiable IMEI
- Non modifiable CPU ID
- SGX
- Trust Zone
- …



Scalable Solution

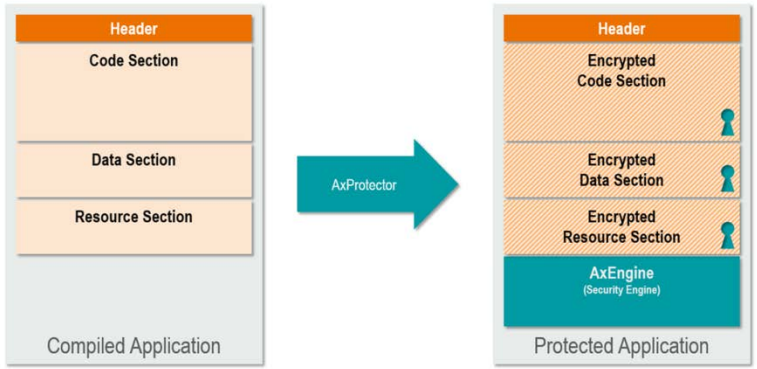


Kerckhoffs‘s Principle

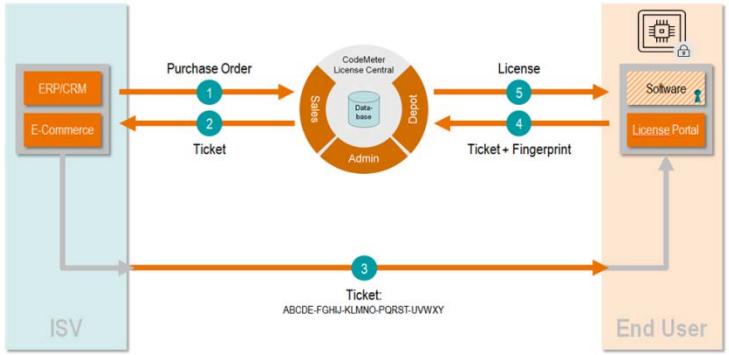
The security of an encryption process is based on the secrecy of the key, not on the secrecy of the algorithm that is used.

Trusted Execution Environment (TEE)

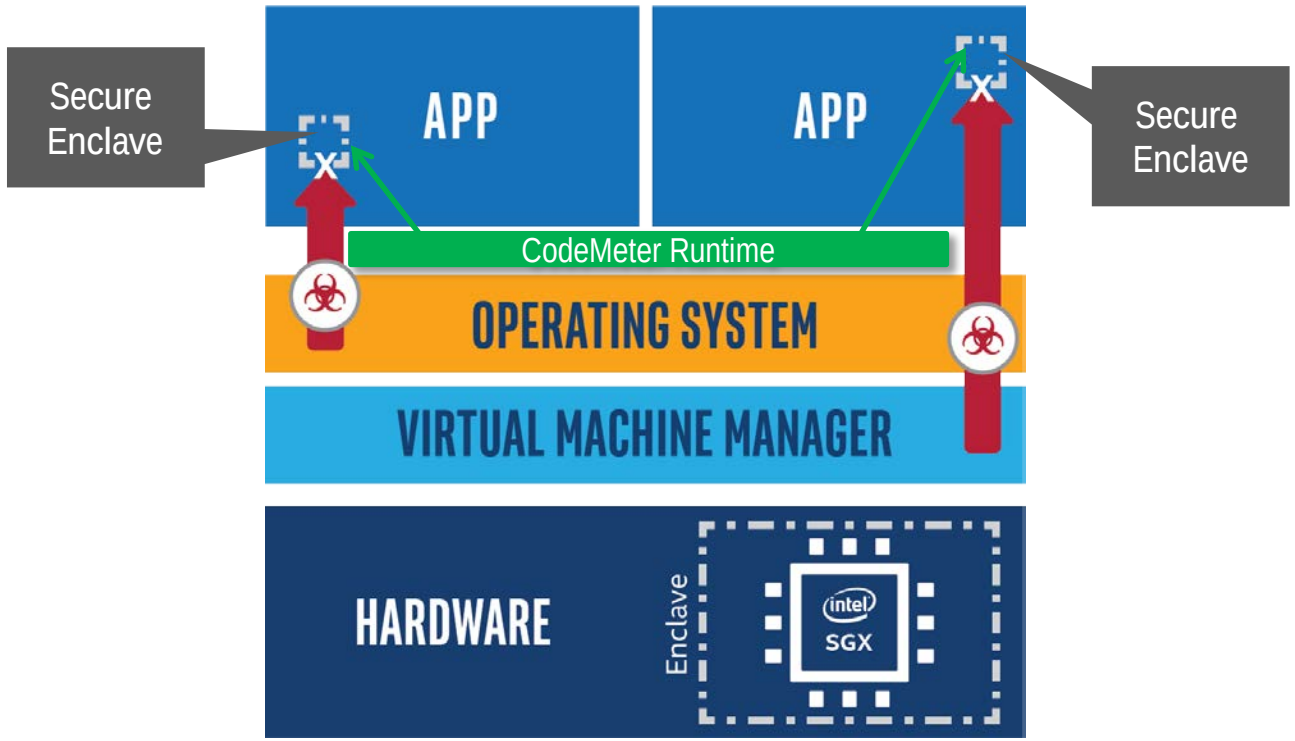
AxProtector – Software Protection



License Central License Entitlement



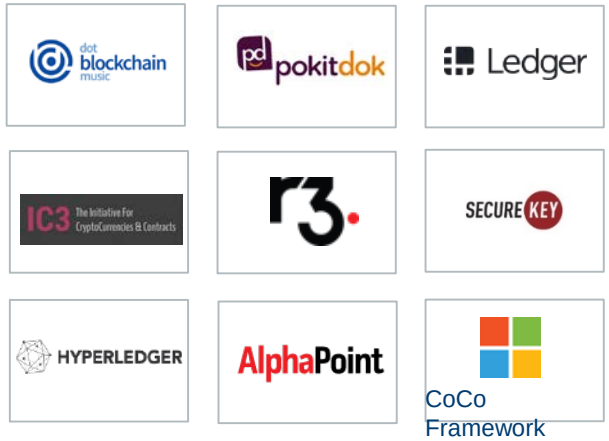
Intel® Software Guard extensions



SGX Ecosystem Solutions

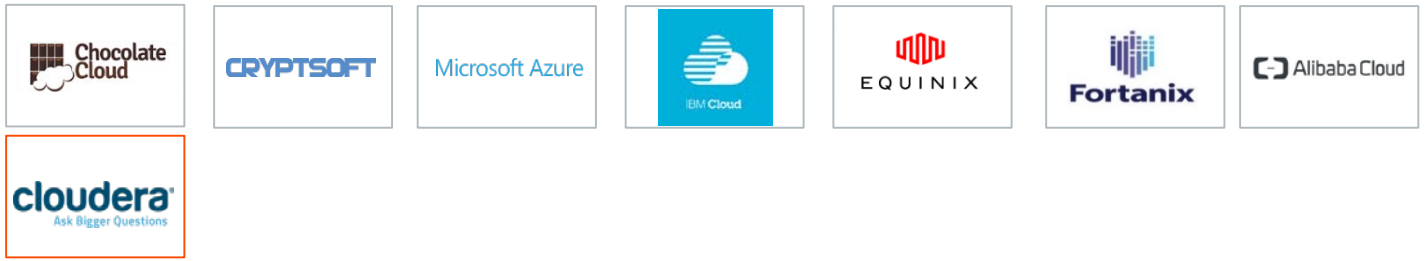
Business Client & Consumer

Blockchain



Internet of Things

Data Center / Cloud



Publically disclosed partnerships with active SGX products

Publically disclosed partnerships, but have not released products to market

Many thanks for your kind attention.

Visit WIBU-SYSTEMS in **hall 6, booth C15,**

and IUNO in **hall 6, booth D02**

Deutschland: +49-721-931720

USA: +1-425-7756900

China: +86-21-55661790

http://www.wibu.com

info@wibu.com