

An Open Attestation & Authentication Infrastructure for Trusted Execution Platform

ZHANG Yuanyuan

Department of Computer Science and Engineering,
Shanghai Jiao Tong University, China

November 4th, 2021

饮水思源 · 爱国荣校

yyjess@sjtu.edu.cn
<http://yyjess.com>

Trusted Execution Environment (TEE) Technology

Enclave TEE

X86 systems:

- Intel Security Guard eXtension (SGX)
- AMD Secure Encrypted Virtualization (SEV)

Intel® SGX

AMD Secure Encrypted Virtualization (SEV)

RISC-V systems:

- Sanctum
- Keystone
- CURE
- Penglai



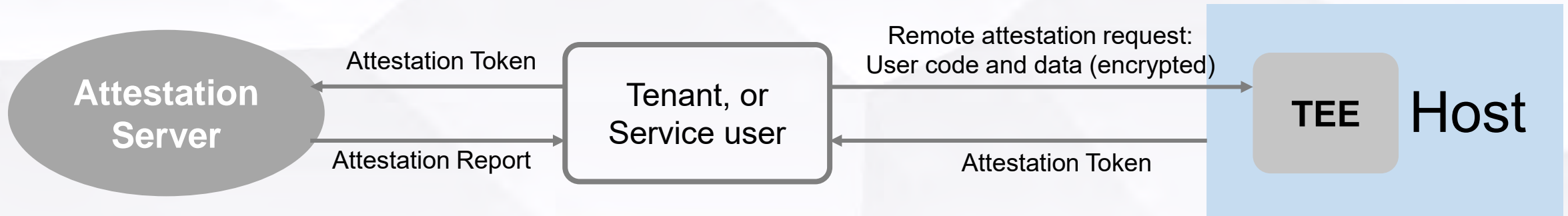
RISC-V: The Free and Open RISC
Instruction Set Architecture

Non-enclave TEE:

- TrustZone
- TPM



TEE Attestation



Attestation is provided to answer the cloud users' question:

Is this TEE authentic?

Is the enclave code legit?

Challenges in building trust for Trusted Execution Platform (TEP)

- Stakeholders in Cloud TEP:

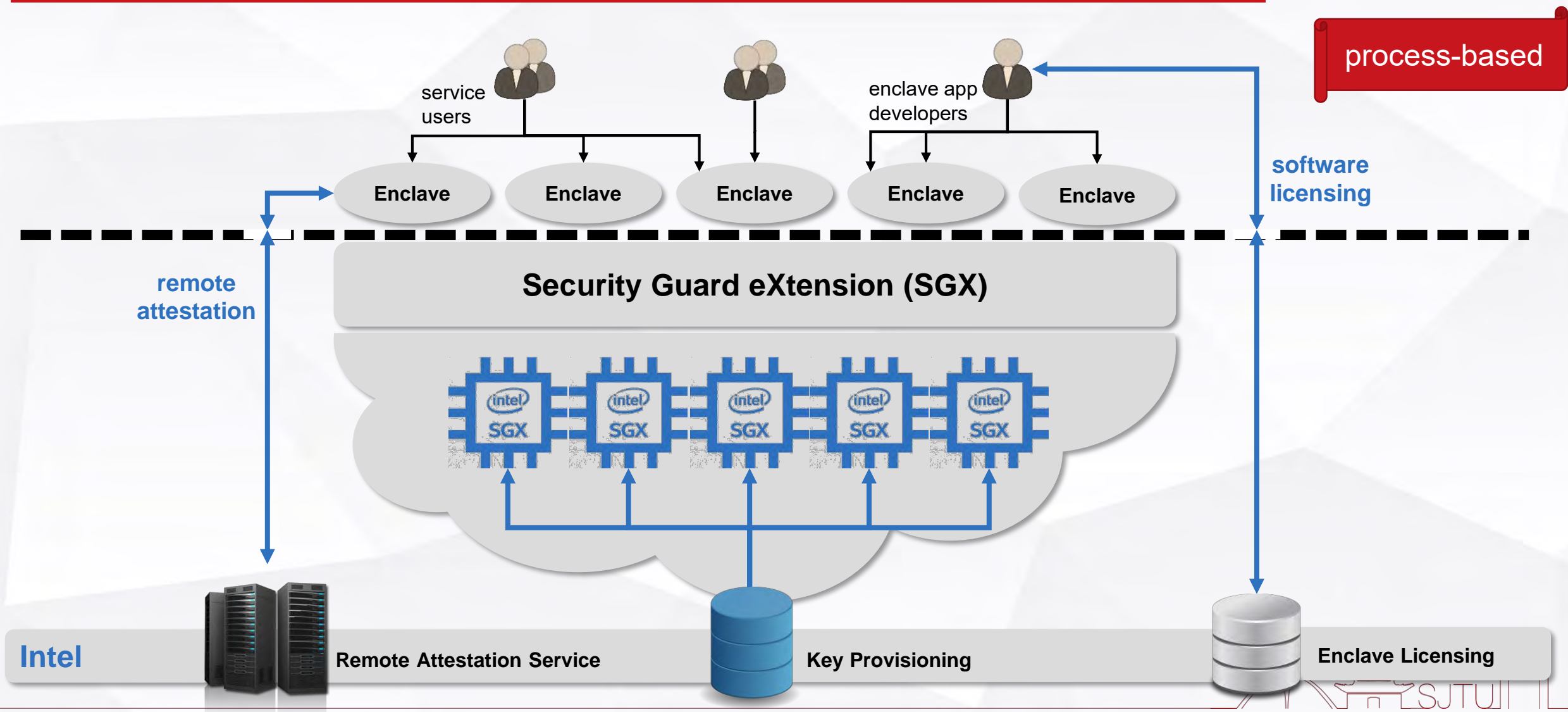
- Chip manufacturers
- Platform developers
- Enclave users/ VM tenants
- Enclave authors

- Some attestation requirements:

- | | |
|-----------------------------|--|
| ▪ Chip manufacturers: | Preserve/Attest the root of security |
| ▪ Platform developers: | Implement an attestation service for the users |
| ▪ Enclave users/VM tenants: | Is this execution platform is a TEP, and how to attest it? |
| ▪ Enclave authors: | Is this enclave app running on the host a legit copy? |

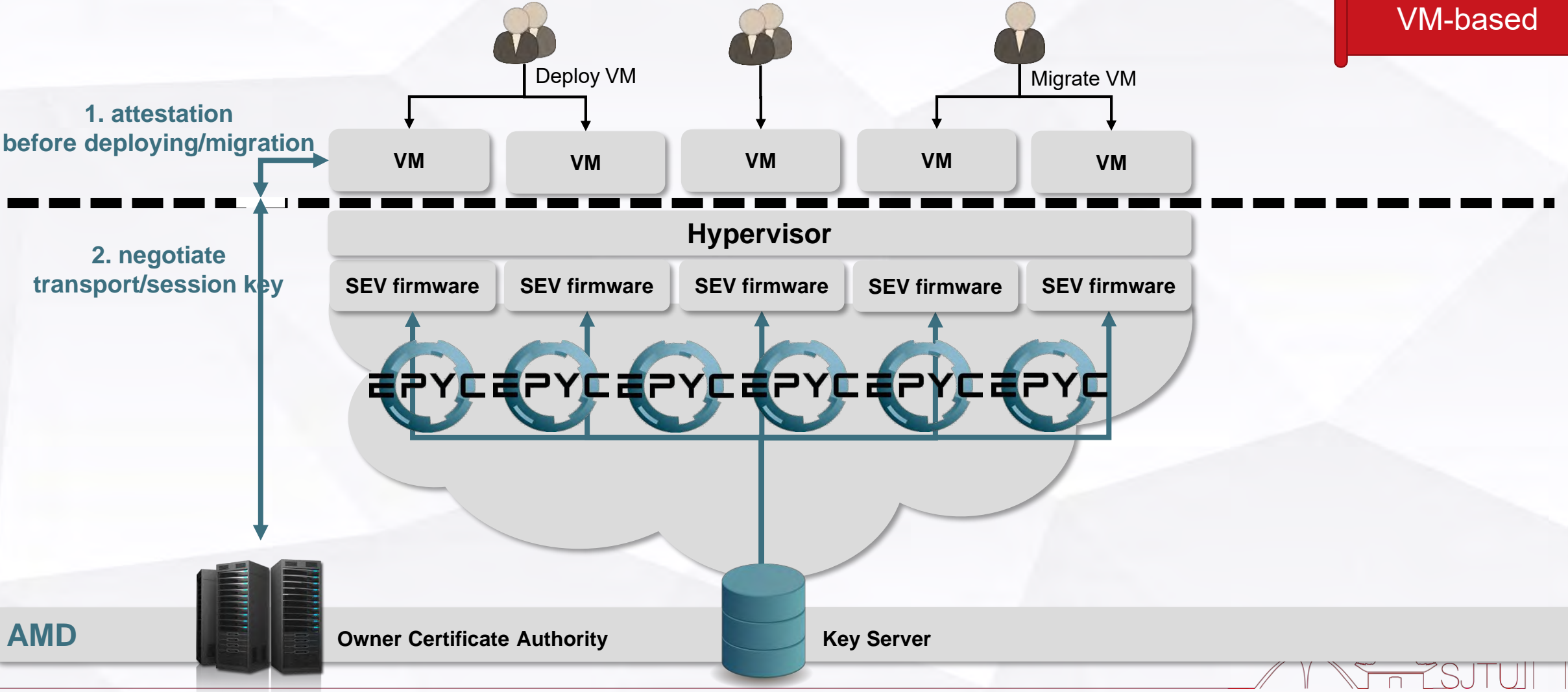


Intel SGX and its attestation services



AMD SEV Remote Attestation

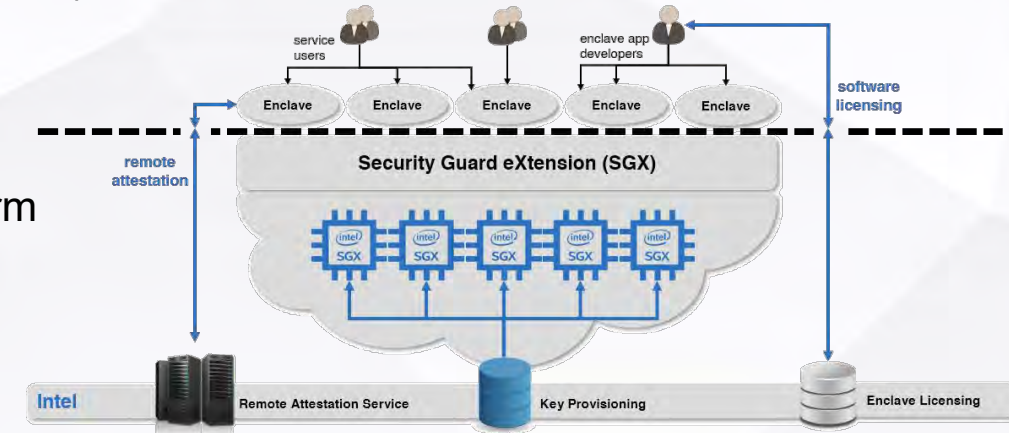
VM-based



Example: Intel Remote Attestation based on EPID

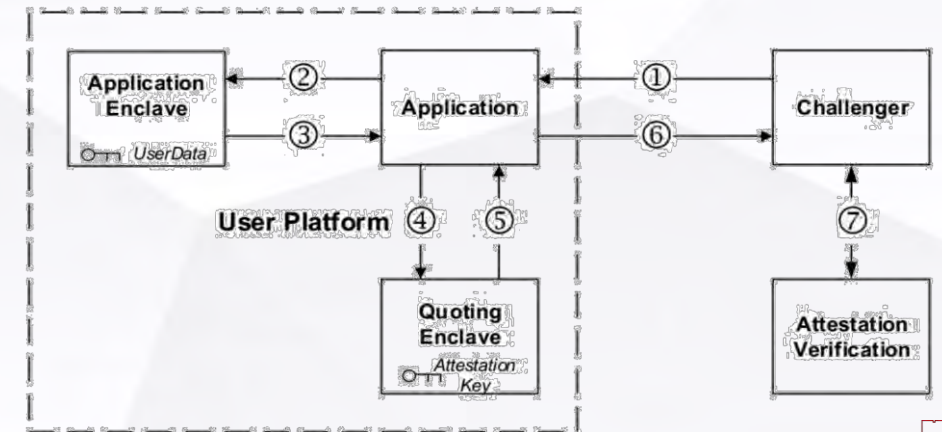


- Platform: Provisioning Secret(e-fuse) \leftrightarrow Intel: Provisioning Secret (server)
- Provisioning: Intel Provisioning Server derives Provisioning Key (PK),
 $ENC_{PK}(\text{attestation key/member private key}) \rightarrow \text{SGX Platform}$
- Signing Quote: $\text{Sign}_{\text{attestationkey}}(\text{Quote}) \rightarrow \text{Challenger}$
- Attestation: Challenger \rightarrow IAS verifies $\text{Sign}_{\text{attestationkey}}(\text{Quote}) \rightarrow \text{report}$



Feature of EPID-based attestations:

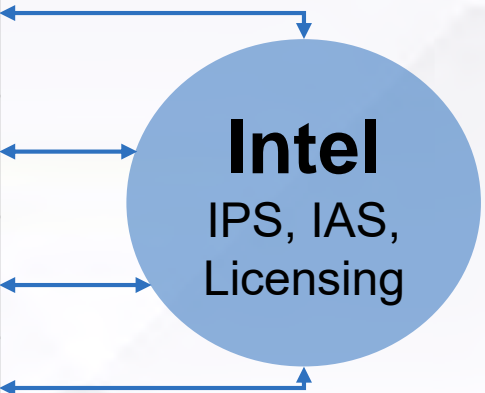
- Increased privacy protections (group EPID signature)
- Provisioning and attestation at workload runtime
- IAS is responsible for the attestation verification



Challenges in Building Trust for TEP

Solutions?

Chip manufacturers	Attest with the root of security	Key server; Burn the key on e-fuse
Platform developers	How do we prove this TEP is trustworthy to the users?	Signed platform quote
Cloud users	Is this platform a TEP?	Remote attestation
Enclave app venders	Is this enclave the legit version, is it running on a TEP?	Software licensing



Existing Remote Attestation Schemes

Intel Family:

- Intel SGX Remote Attestation: EPID, DCAP
- Marblerun¹: Gramine (previously known as Graphene) Attestation Service Mesh
- OPERA²: Open Remote Attestation for Intel's Secure Enclaves

AMD Family:

- AMD SEV Remote Attestation
- Industrial implementations in development ?

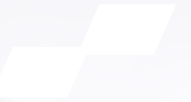
Other Open Enclave Families:

- CURE³ Remote Attestation

1. Gramine: A Library OS for Linux multi-process applications, with Intel SGX support. <https://github.com/gramineproject/gramine>

2. Guoxing Chen, et al. OPERA: Open Remote Attestation for Intel's Secure Enclaves, CCS'19

3. CURE: A Security Architecture with CUsomizable and Resilient Enclaves, Security'21



Third-Party Attestation



Intel ECDSA Attestation (DCAP Attestation)

Elliptic Curve Digital Signature Algorithm (ECDSA) Attestation

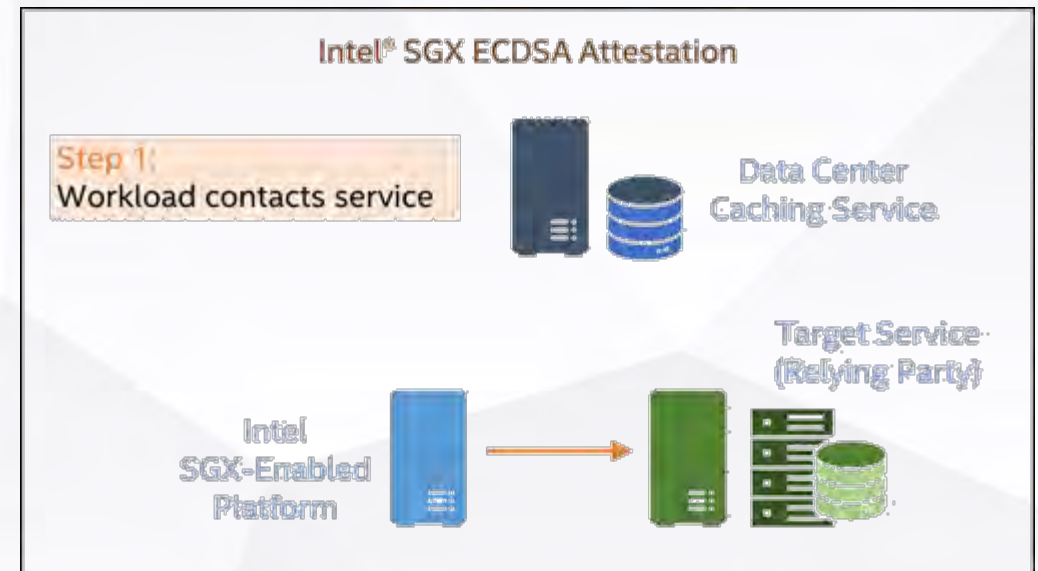
This method enables third-party attestation via the Intel SGX Data Center Attestation Primitives (DCAP).

Supported processors:

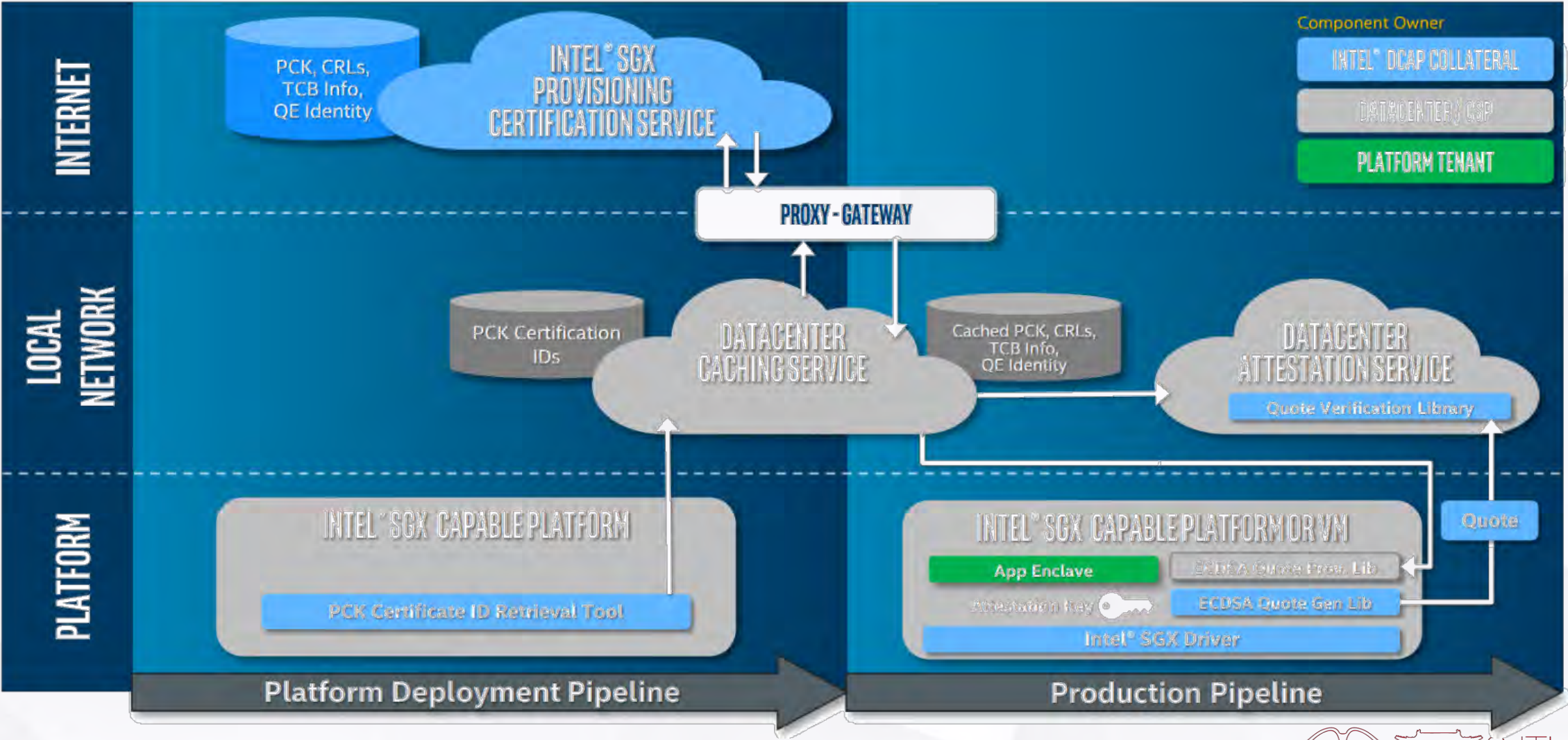
- 3rd generation Intel Xeon Scalable processor
- selected Intel Xeon E3 processors

Features:

- Provides flexible provisioning based on ECDSA certificates
- Allows for construction of on-premise attestation services
- Requires flexible launch control in supported Intel platforms
- Available under an open-source licensing model



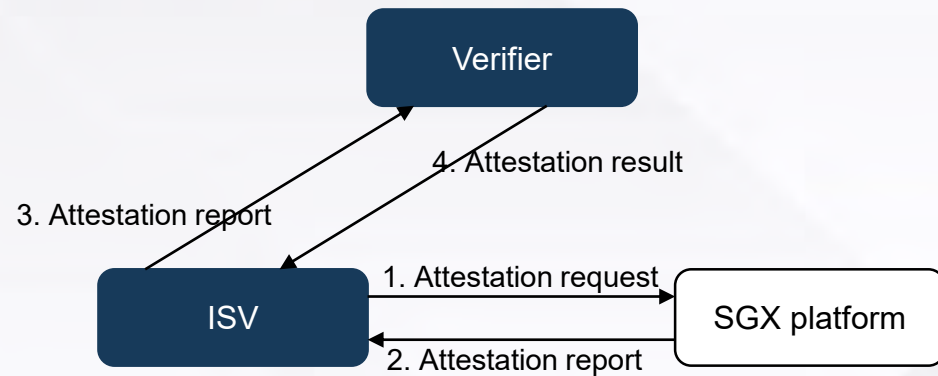
Intel ECDSA Attestation



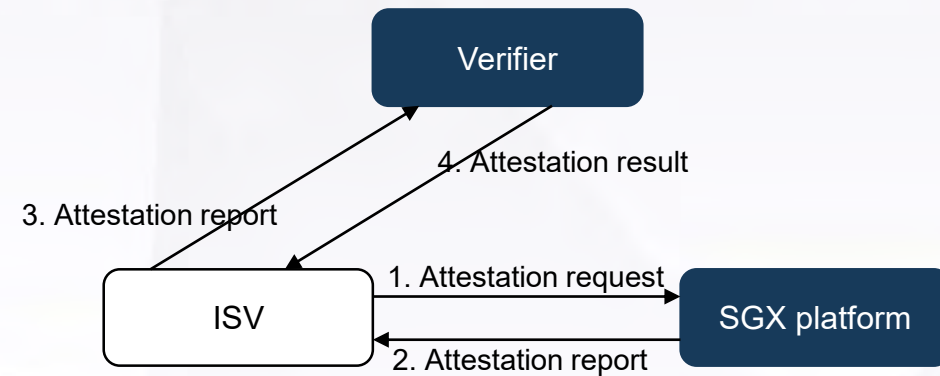
Attacks on Intel DCAP



entity It means they reside on/in the same platform / local network / controlled environment



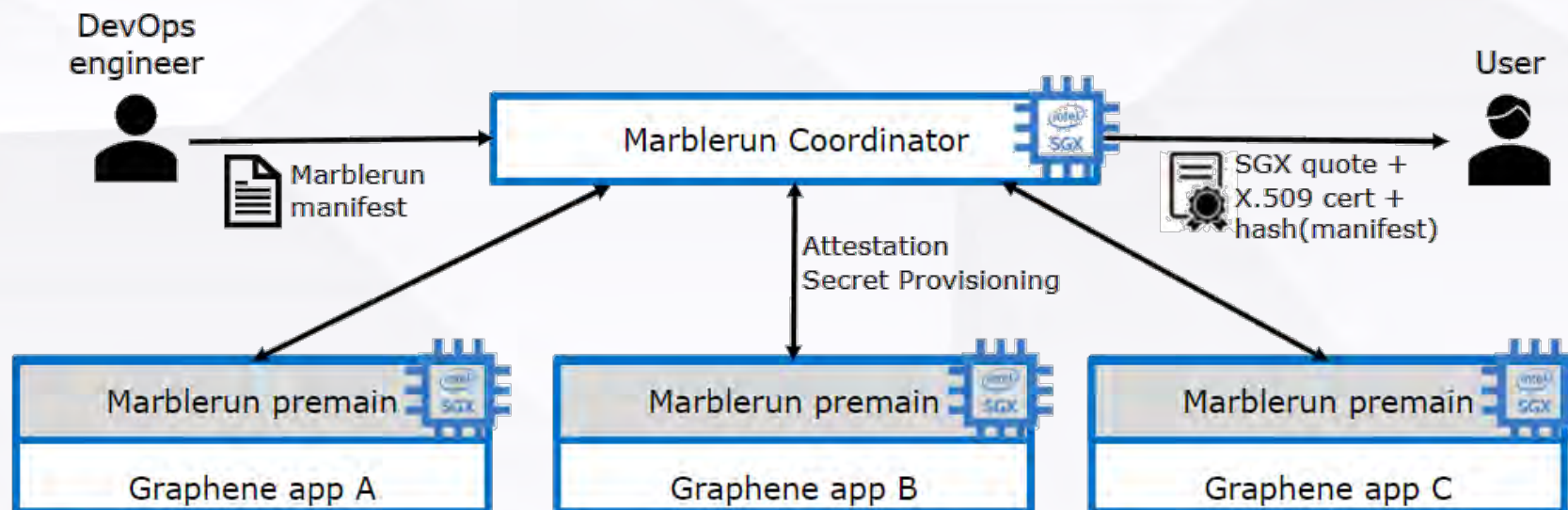
When the certificates are public to all,
ISV can perform the verification by themselves.
(It causes ISV's privacy exposure to Verifier.)



When the certificates are private to service providers,
ISV has to fully trust third-party attestation results.
(Collusion attack by Verifier and SGX platform)

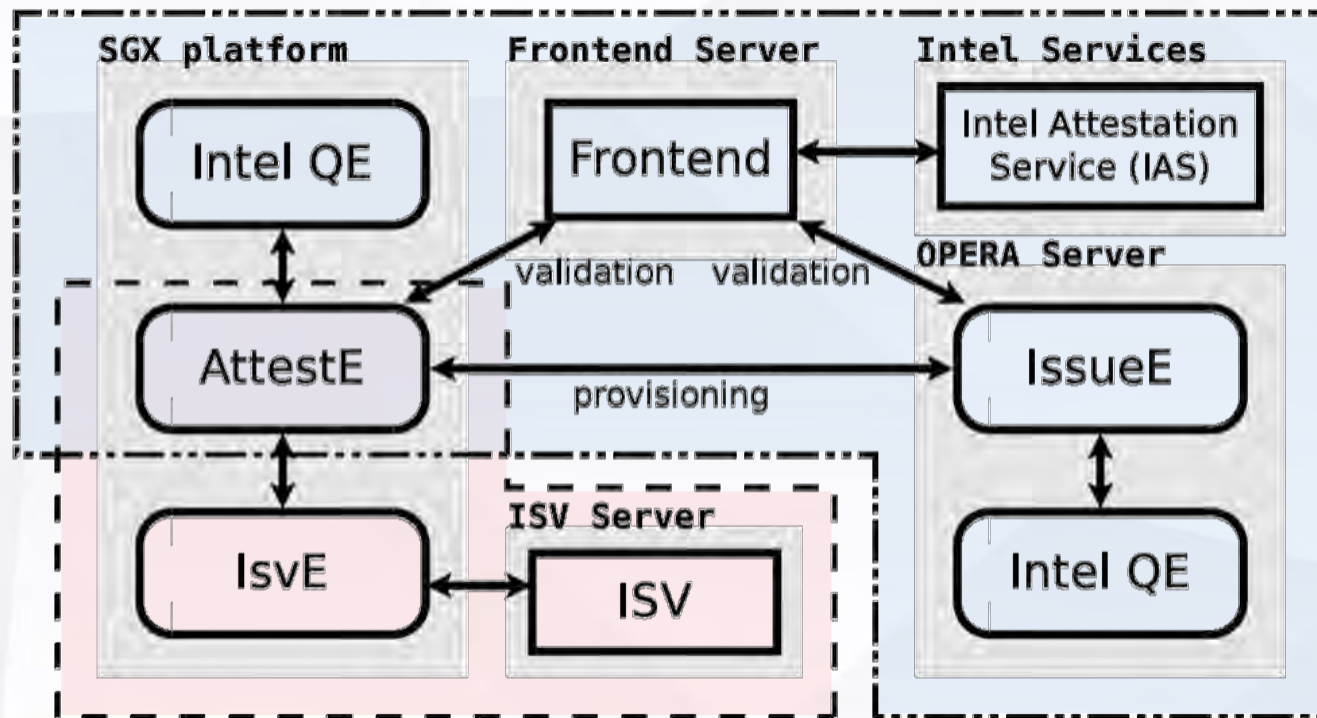
Marblerun¹: Gramine Attestation Service Mesh



Gramine



Marblerun is the service mesh for confidential computing from Edgeless Systems

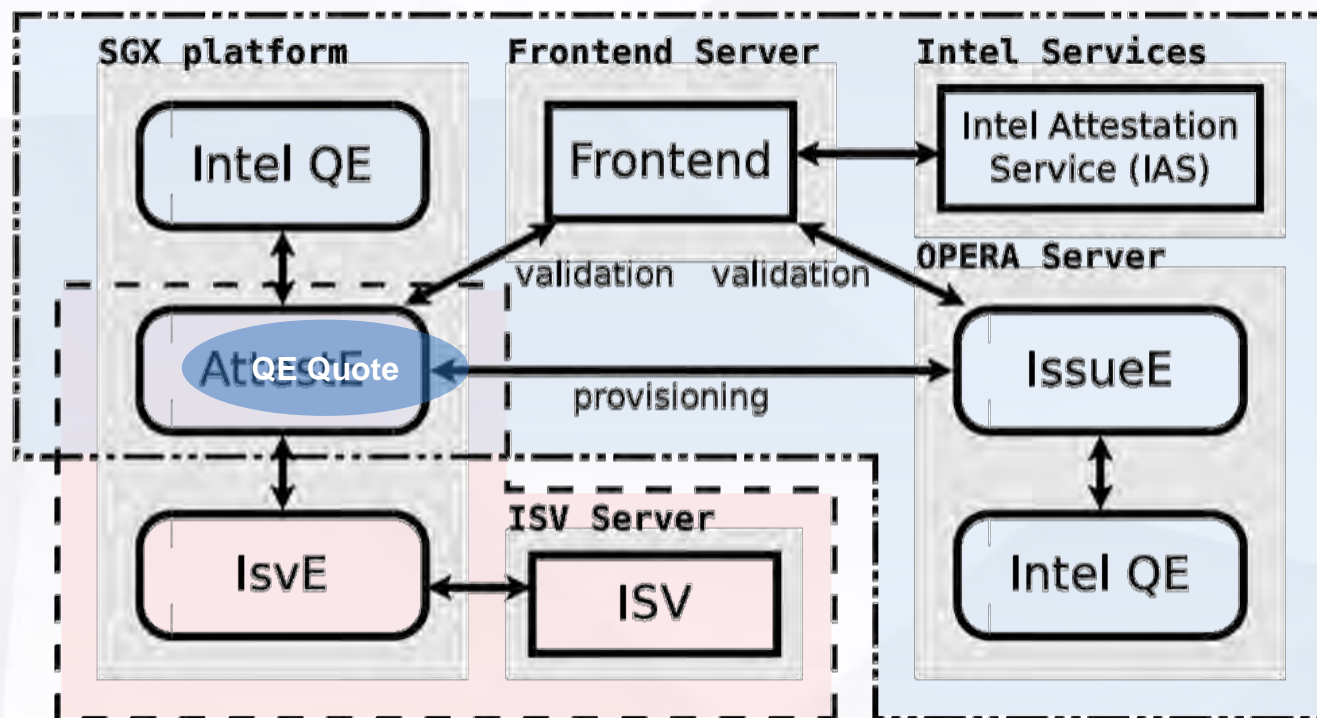
- Coordinator (the centralized attestation & secret provisioning service) deployed in the cluster
- Marbles (separate Gramine applications) integrated with each application



 OPERA attestation
 OPERA registration and preparation

- Registration
 - IssueE setup
 - IssueE validation
- Preparation
 - AttestE setup
 - AttestE validation
- Attestation
 - AttestE generates a *quote*
 - IsvE verifies the *quote* locally





- Registration
 - IssueE setup
 - IssueE validation



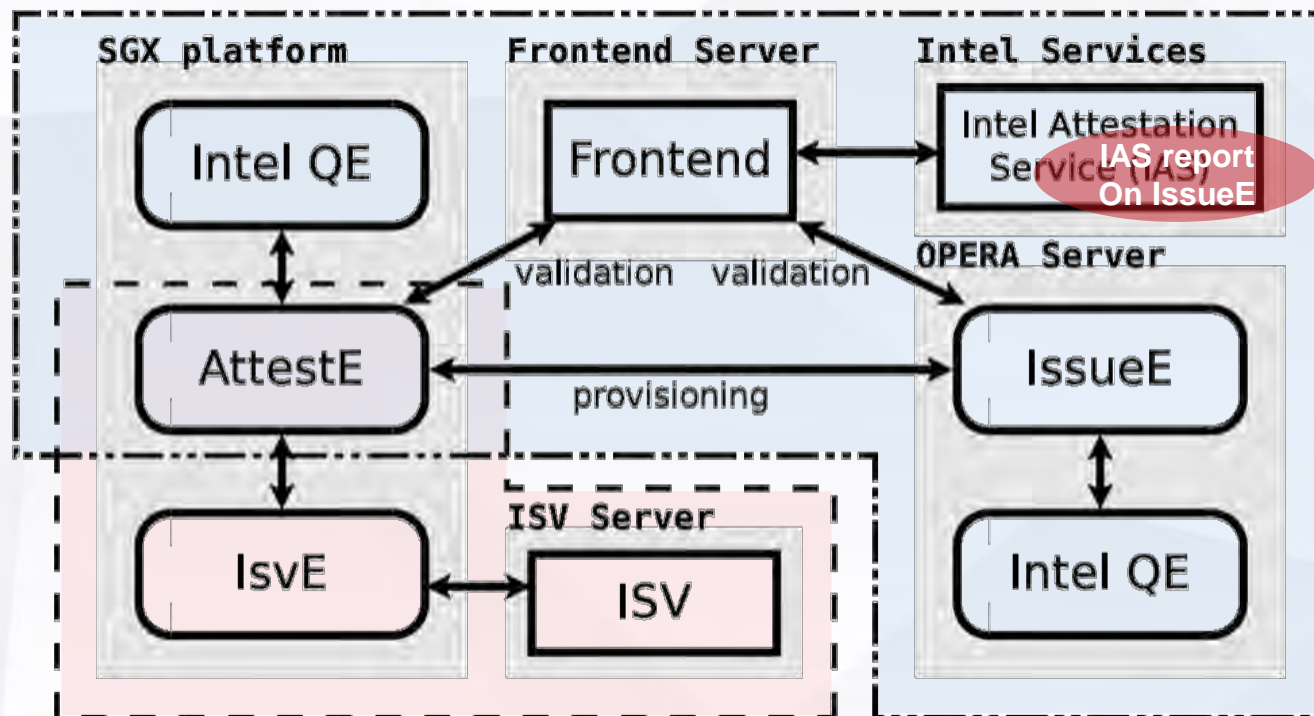
OPERA attestation

OPERA registration and preparation

QE Quote

QE's IAS Quote



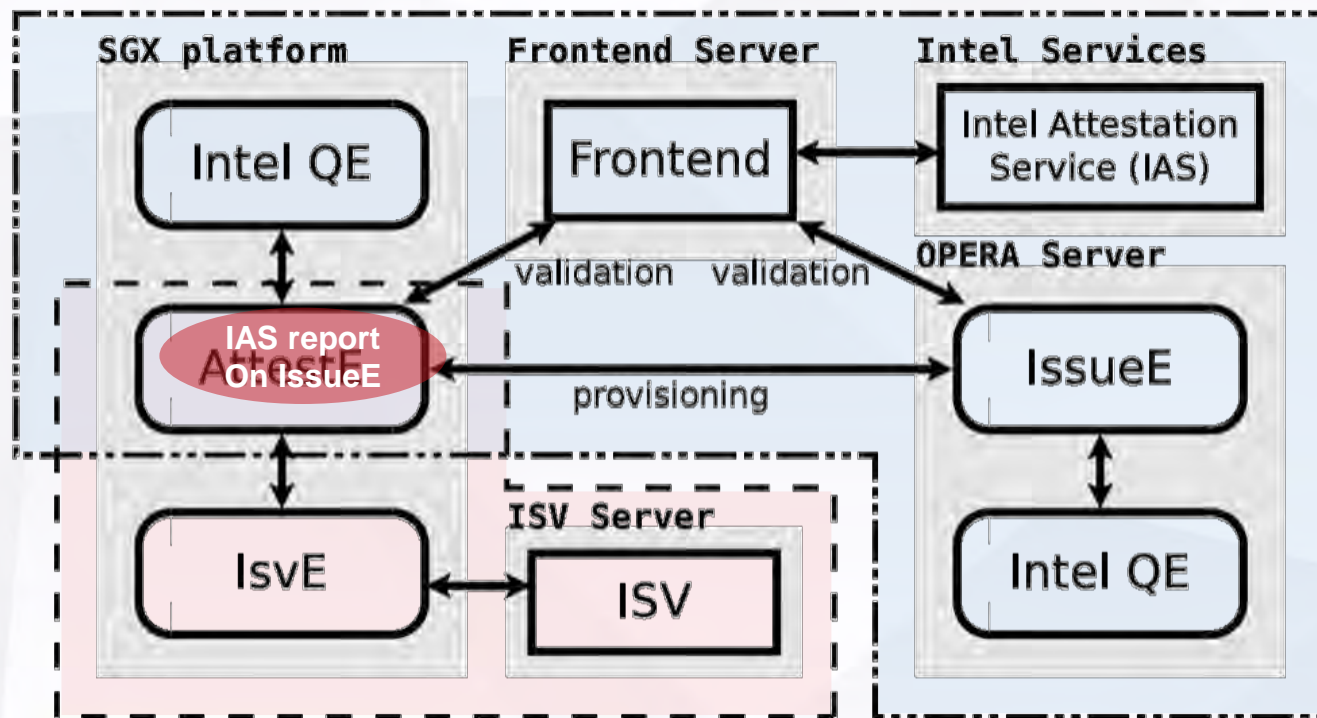


- Registration
 - IssueE setup
 - IssueE validation
- Preparation
 - AttestE setup
 - AttestE validation

IAS report
On IssueE

A message containing the Intel Attestation Service report for IssueE





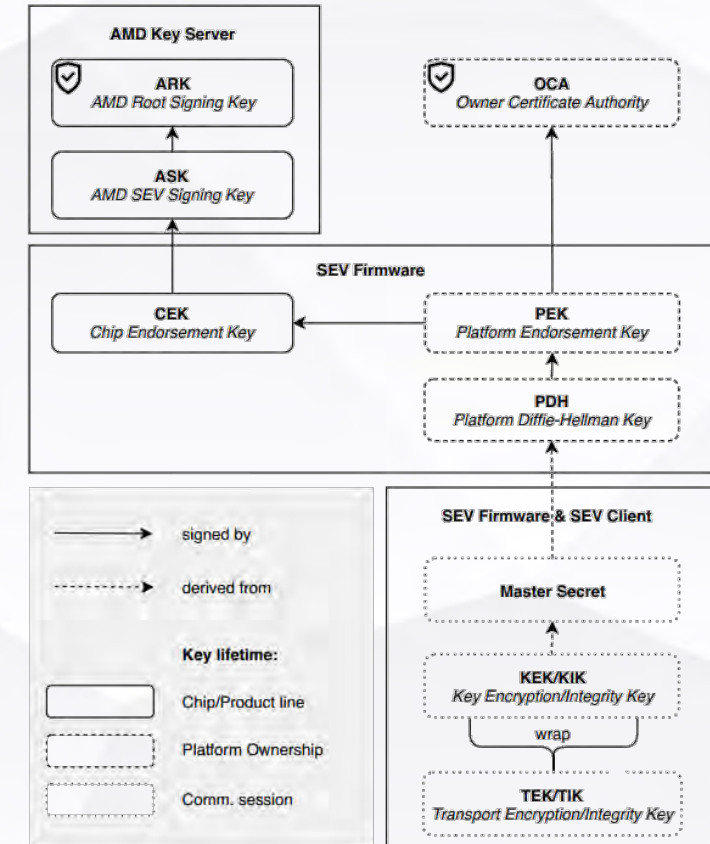
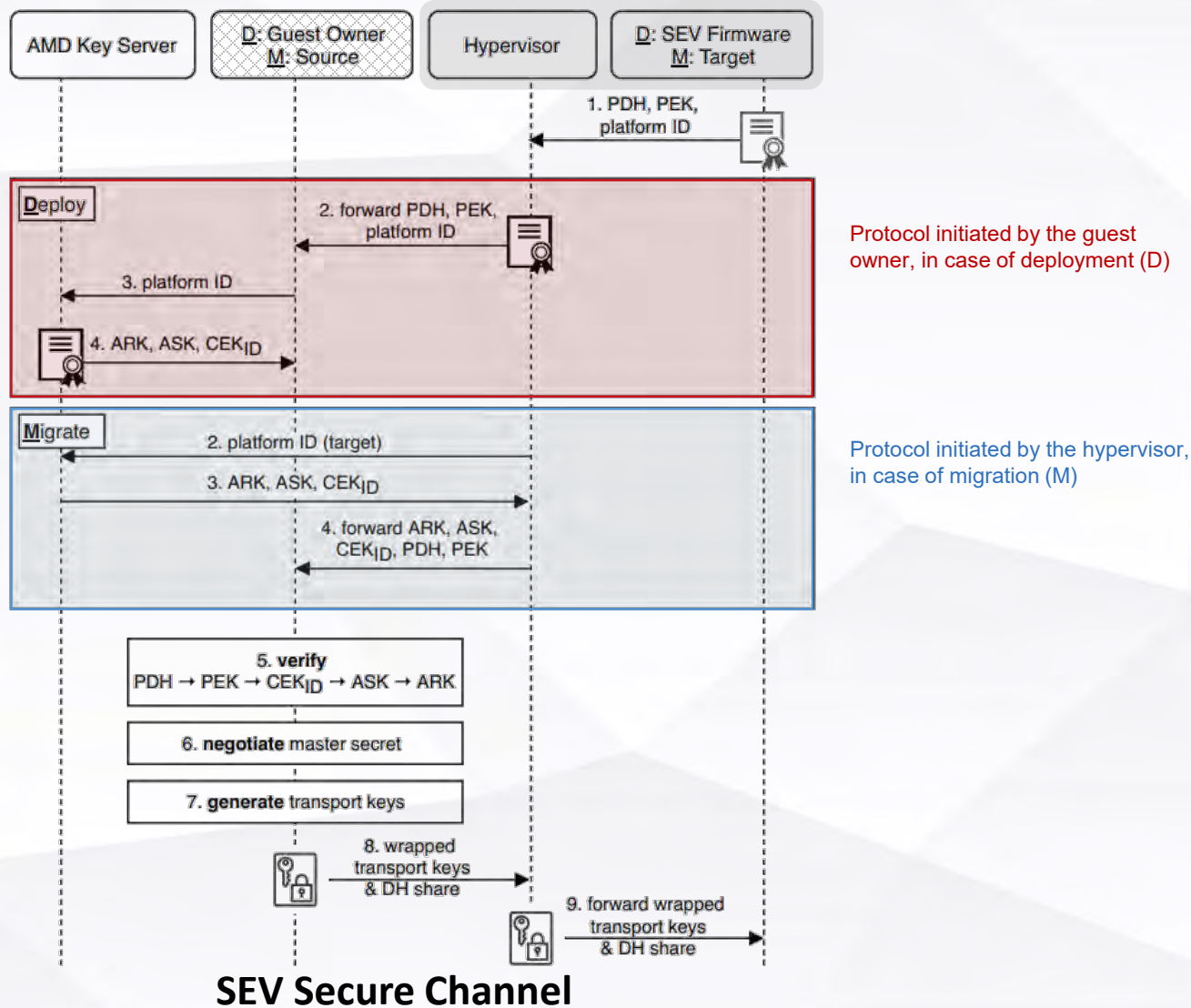
- Registration
 - IssueE setup
 - IssueE validation
- Preparation
 - AttestE setup
 - AttestE validation
- Attestation
 - AttestE generates a *quote*
 - IsvE verifies the *quote* locally

IAS report
On IssueE

A message containing the Intel Attestation Service report for IssueE



AMD SEV's Remote Attestation¹ for VM



Cryptographic keys in SEV



Attacks

▪ Fake SEV

- Goal: It fakes the presence of SEV, and gains access to guest data
- Attacker: a cloud provider, has had access to an SEV-enabled system for one-time extraction of the CEK private key and the corresponding platform ID
- Victim: a cloud customer who is deploying a VM to the host
- Method: forge the verification chain PEK->PDH->transport key...

▪ Migration Attack

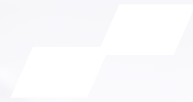
- Goal: extract runtime data of a guest from a host system
- Attacker: has any CEK private key and certificate (not necessarily the CEK of this platform), access to management interface of an SEV-enabled host
- Victim: a cloud customer who successfully deployed a VM on the SEV-enabled host
- Method: use the false CEK to forge a fake SEV-enabled destination host

Lack of
backward
Secrecy



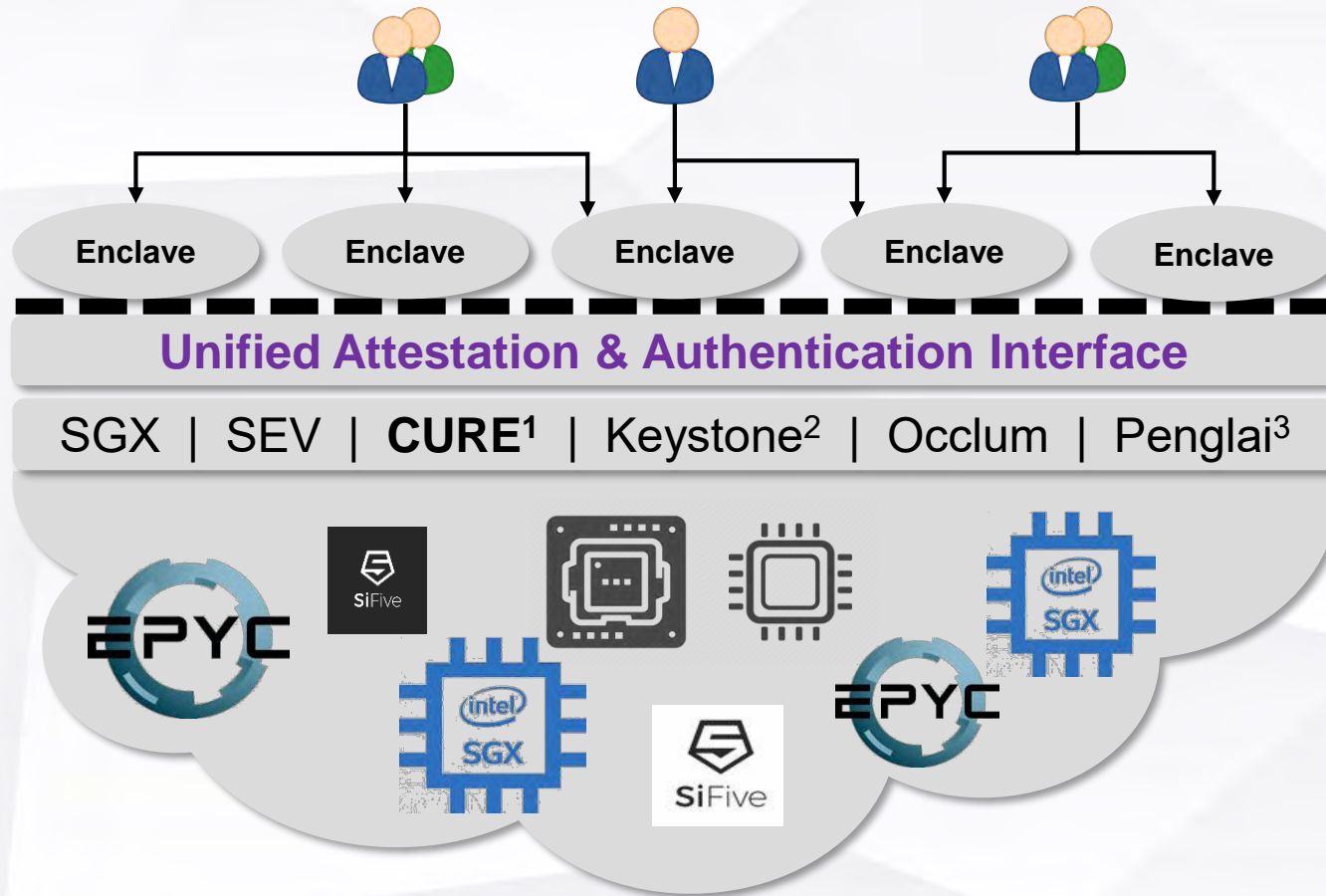
Comparison

Remote Attestation	Scenarios	Pros	Cons
Intel EPID	<i>Intel SGX Enclave Remote Attestation</i>	EPID privacy preserving	Intel centralized attestation
Intel DCAP	<i>Intel SGX Enclave Remote Attestation</i>	Third-party (Intel ECDSA)	Relying on the Intel authorizing PCE; Collusion attacks
Marblerun (for Intel)	<i>Intel SGX Enclave Remote Attestation</i>	<ul style="list-style-type: none">• EPID privacy preserving• Third-party (Intel ECDSA)	<ul style="list-style-type: none">• Intel centralized attestation• Collusion attacks
OPERA (for Intel)	<i>Intel SGX Enclave Remote Attestation</i>	Third-party (Intel EPID)	Relying on the IAS ¹ report
AMD SEV	<i>AMD SEV VM Remote Attestation</i>	Introduce OCA ²	Fake attack, migration attack



Attestation for Open TEP

Hybrid Trusted Execution Platforms (H-TEPs)



Requirements for an open attestation & authentication infrastructure:

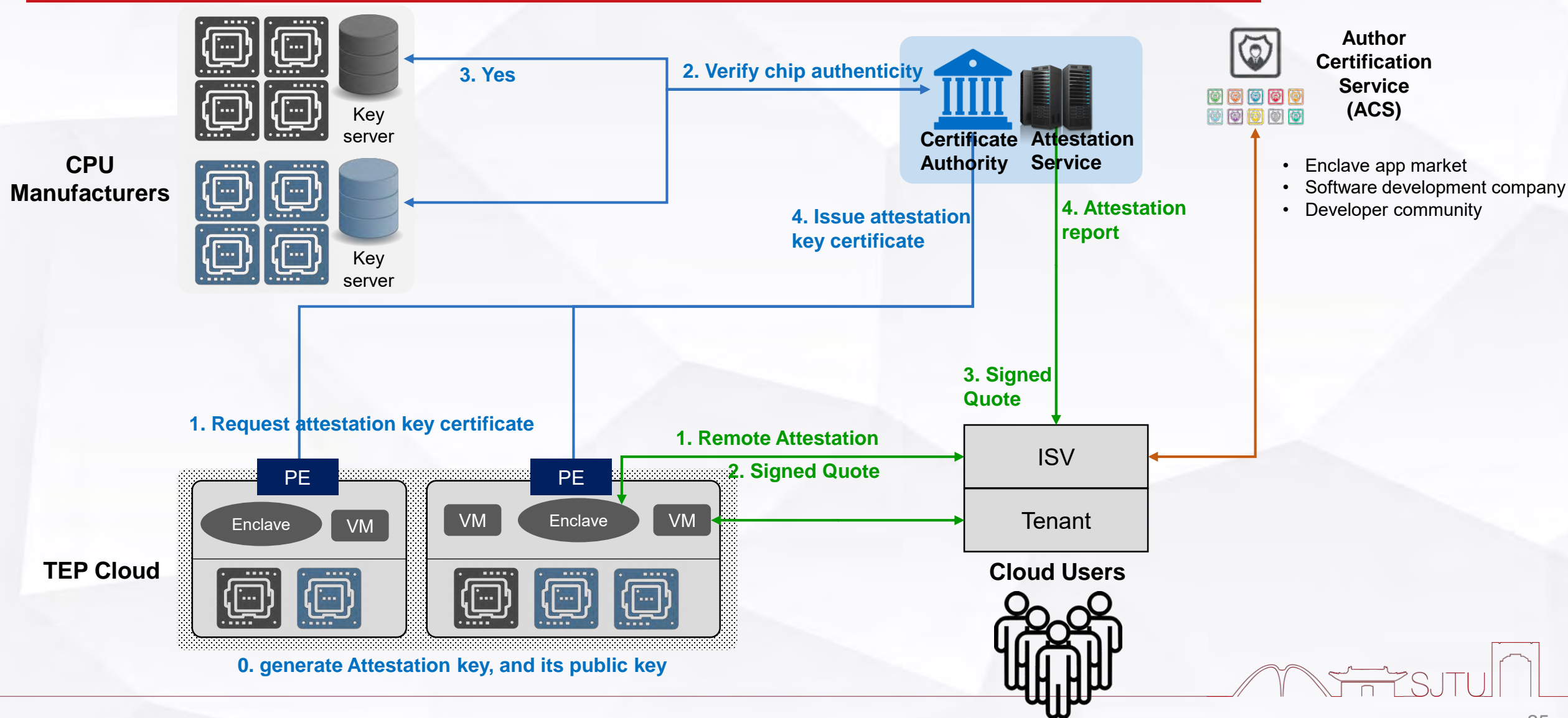
- **Separation of Powers**
- Authentication: chips, platforms, VMs, applications(enclaves)
- Privacy: no trace for the attesters or the platform
- Distribution of authority
- Usability: unified attestation Interface
- Performance: attestation for enclave container swarm

1. CURE: A Security Architecture with CUsomizable and Resilient Enclaves (Usenix Security 2021)

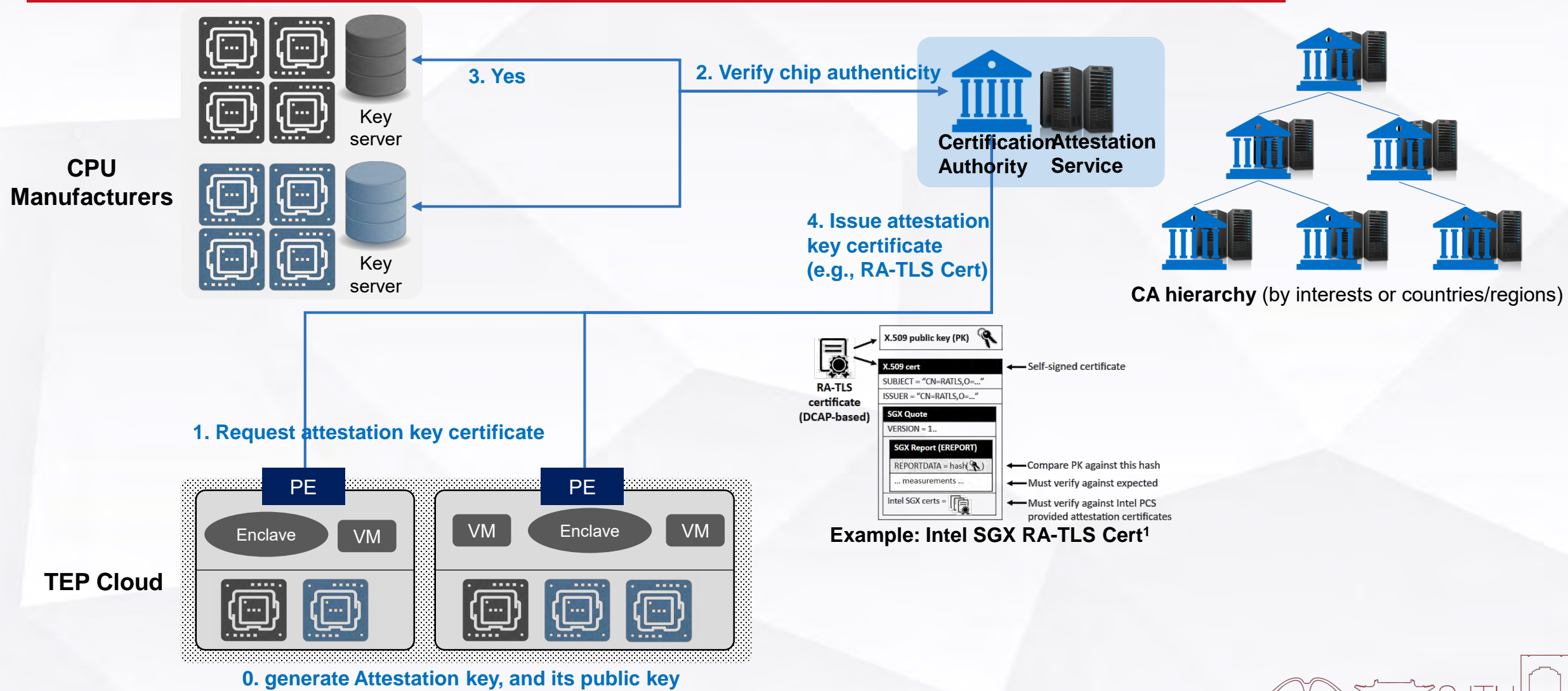
2. Keystone: A framework for architecting tees (EuroSys 2019)

3. Open-sourced secure and scalable TEE system for RISC-V. <https://penglai-enclave.systems/>

Attestation for Open TEP: Overview



Attestation for Open TEP: Secret Provisioning



Attestation for Open TEP: Enclave Remote Attestation

- An enclave's attestation token includes (take SGX Quote as an example):
 - Enclave's REPORT
 - Enclave measurement : memory layout hash
 - TCB svn
 - ISV product id & ISV svn
 - Report data
 - Epoch (time of generation)
 - Token Generator's version
 - Attestation Service Provider's info

```
75 typedef struct _quote_t
76 {
77     uint16_t    version;        /* 0 */
78     uint16_t    sign_type;      /* 2 */
79     sgx_epid_group_id_t epid_group_id; /* 4 */
80     sgx_isv_svn_t qe_svn;       /* 8 */
81     sgx_isv_svn_t pce_svn;      /* 10 */
82     uint128_t   qe_id;          /* 12 */
83     sgx_base_name_t base_name;  /* 16 */
84     sgx_report_body_t report_body; /* 48 */
85     uint32_t    signature_len; /* 432 */
86     uint8_t     signature[]; /* 436 */
87 } sgx_quote_t;
```

Example: sgx_quote_t



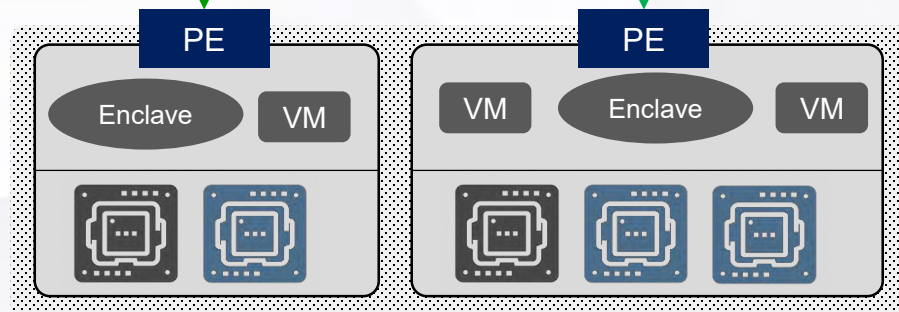
2. PE Attestation Report

1. PE Attestation (One time)

3. RA request

4. Attestation report

TEP Cloud

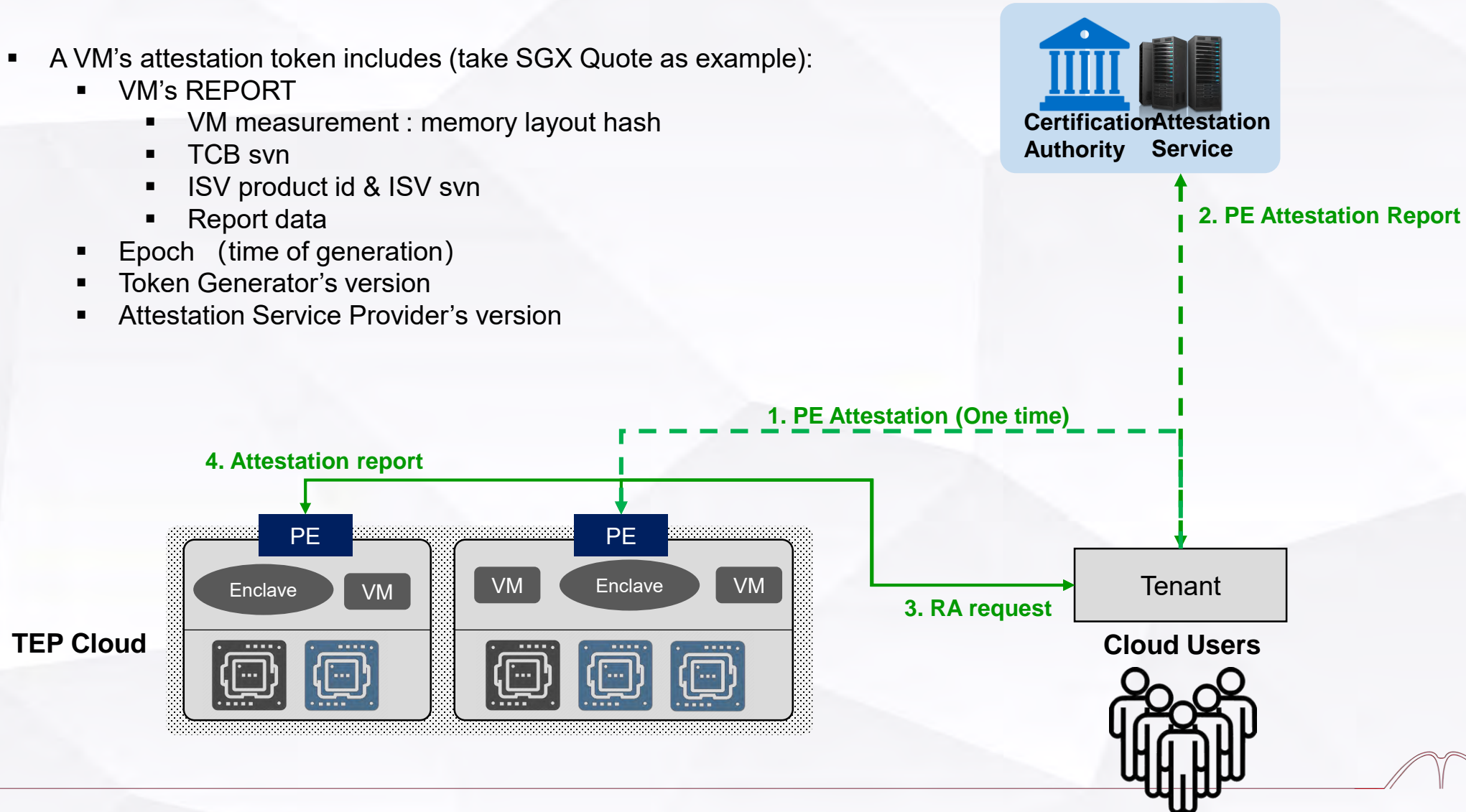


Cloud Users



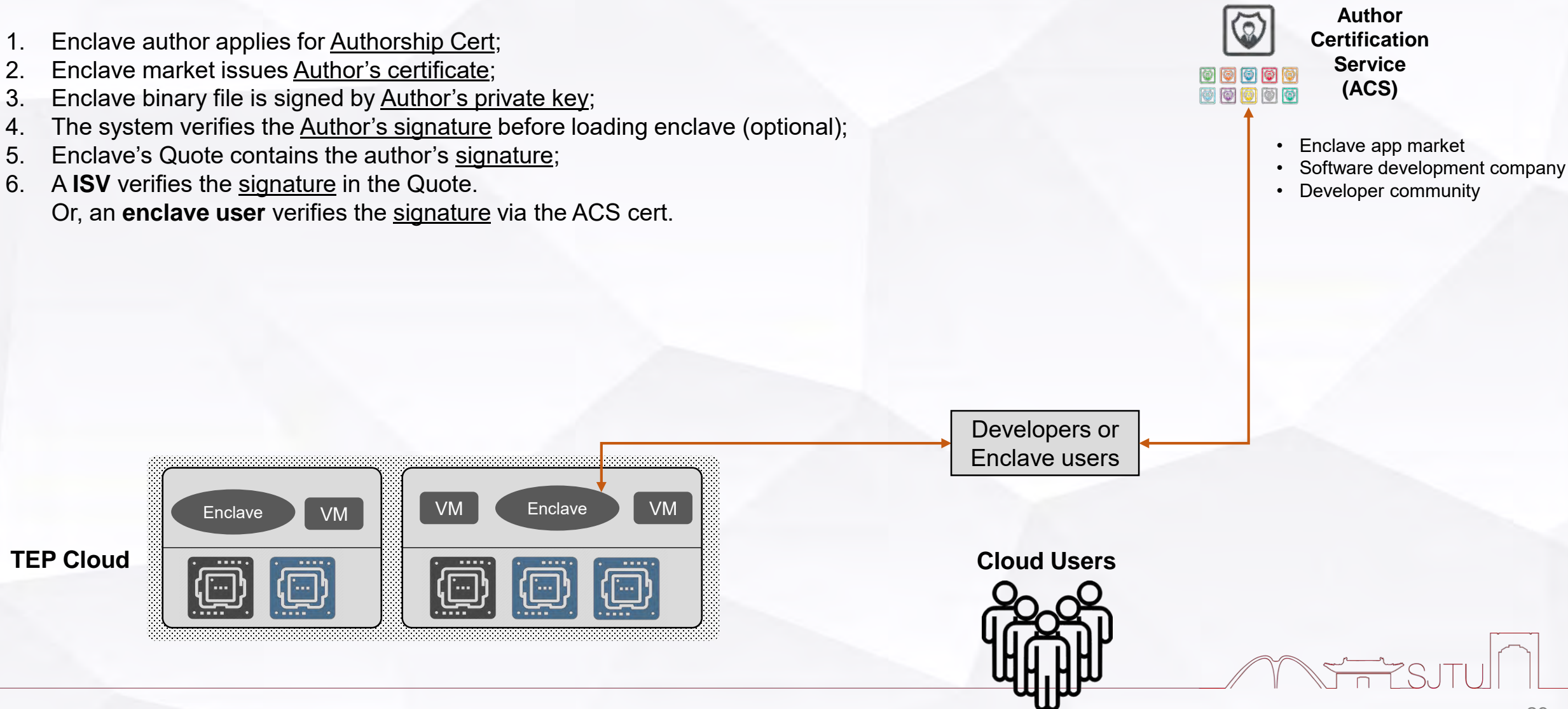
Attestation for Open TEP: VM Attestation

- A VM's attestation token includes (take SGX Quote as example):
 - VM's REPORT
 - VM measurement : memory layout hash
 - TCB svn
 - ISV product id & ISV svn
 - Report data
 - Epoch (time of generation)
 - Token Generator's version
 - Attestation Service Provider's version



Attestation for Open TEP: Enclave Authorship Authentication

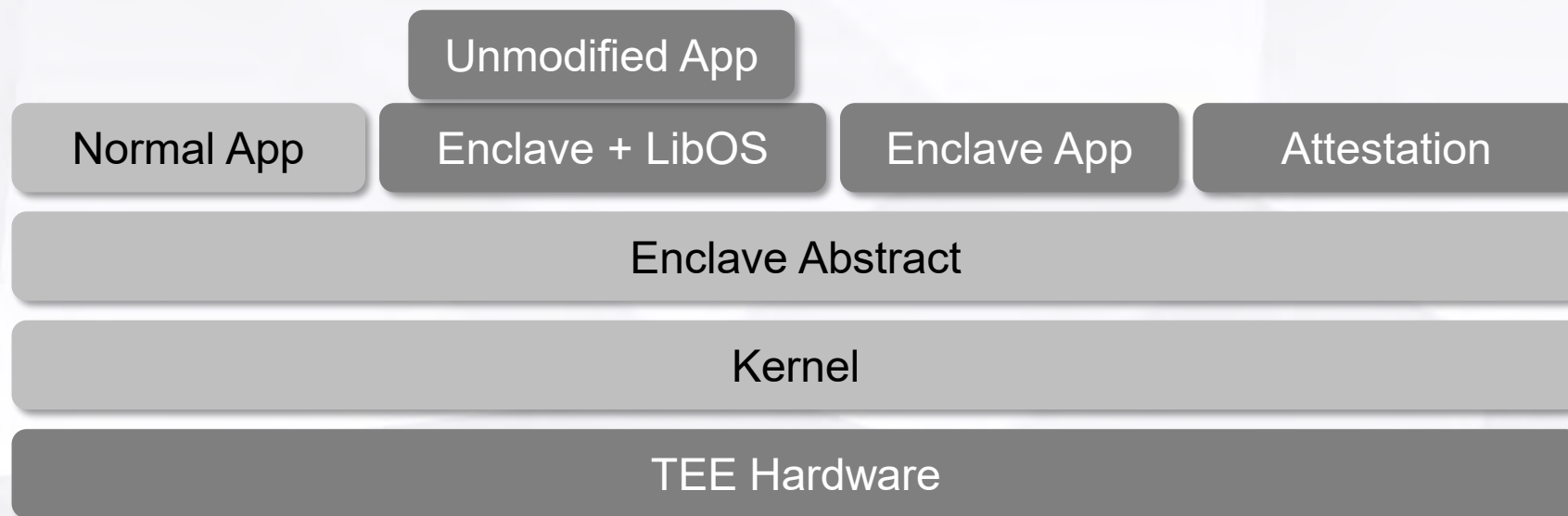
1. Enclave author applies for Authorship Cert;
2. Enclave market issues Author's certificate;
3. Enclave binary file is signed by Author's private key;
4. The system verifies the Author's signature before loading enclave (optional);
5. Enclave's Quote contains the author's signature;
6. A **ISV** verifies the signature in the Quote.
Or, an **enclave user** verifies the signature via the ACS cert.



Open TEP Ecosystem

SGX-like programming
paradigm

Developers write code from scratch,
fight with the low-level TCB.



Open TEP Ecosystem

Open TEP programming paradigm

Developers are set free from low-level security,
ship unmodified app to TEP.
Enclave code security logic is neat and clean.



Conclusion & Future Work

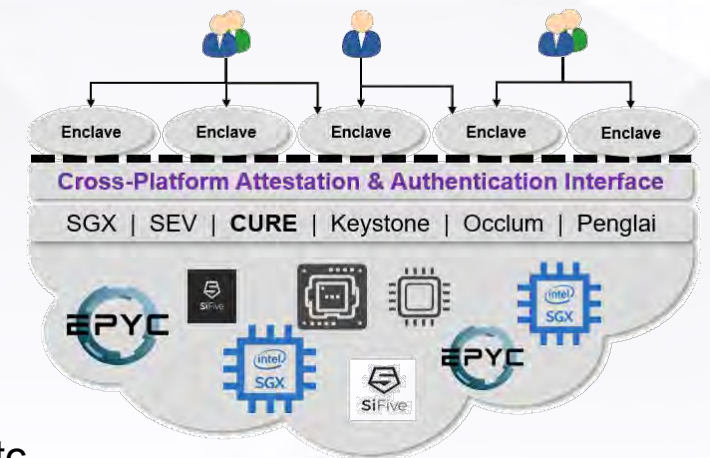
- The trust from the open Hybrid-TEP is built on the attestation service
 - Cloud service users → Cloud provider
 - Enclave developer → Cloud provider
- Authentication services should be open and decentralized
 - Verifying the authenticity of a chip
 - Issuing attestation certificate — by a non-interested authority
 - Enclave authorship authentication — by Enclave App Markets/Communities

Emerging works

- OPERA, Gramine, ProximiTEE, MAGE, etc.
- Open Enclaves Ecosystem (for SGX): Gramine, Open Enclave, CCF, Mysitkos, etc.
- Standards: IETF RATS WG

Future work

- **Implementation on CURE**
- Attempt to unify the remote attestation service interface (for SGX, SEV, CURE and other open enclave systems)
- Standardize the attestation flow and protocol format (e.g., IETF RATS WG)
- Attend to new attestation paradigms, e.g., swarm attestation ...



An Open Attestation & Authentication Infrastructure for Trusted Execution Platform

Thank You

ZHANG Yuanyuan

yyjess@sjtu.edu.cn

<http://yyjess.com>

饮水思源 爱国荣校