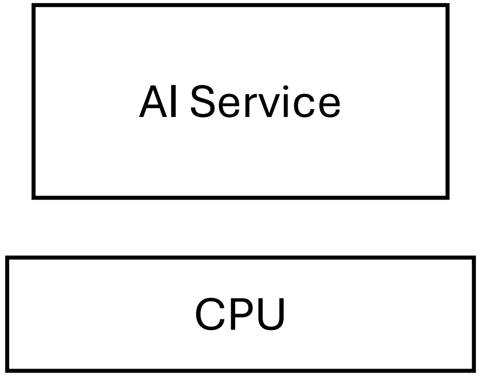
# Proving Attributes about Confidential Compute Services with Validation and Endorsement Services

Anjo Vahldiek-Oberwagner, Marcela S. Melara

intel® labs

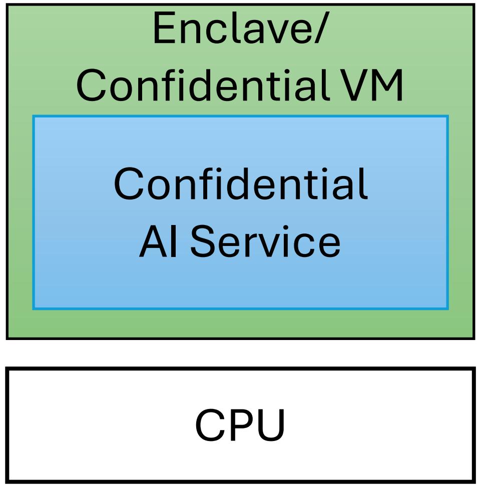
# Confidential Compute Services Today



AI Service

CPU

# Confidential Compute Services Today

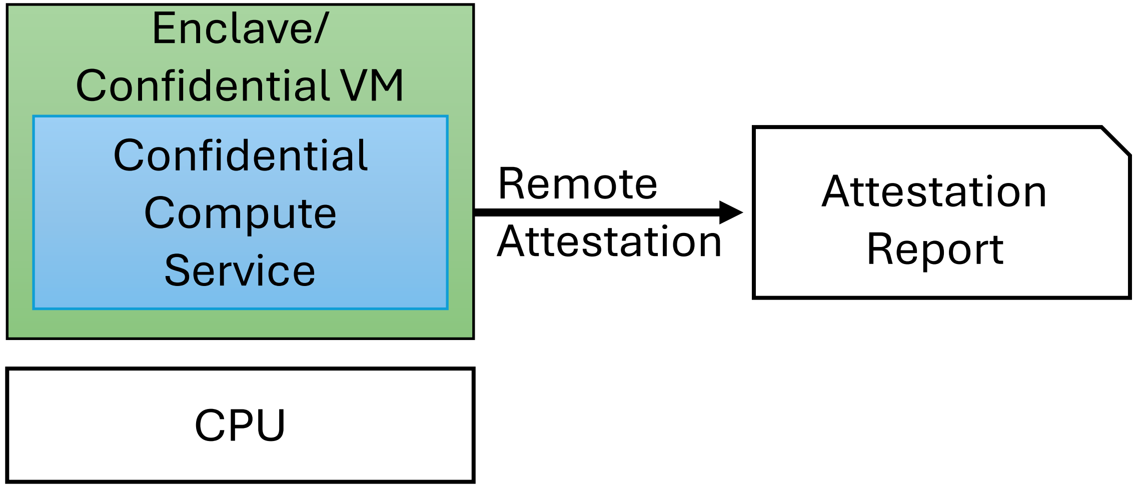


Enclave/
Confidential VM

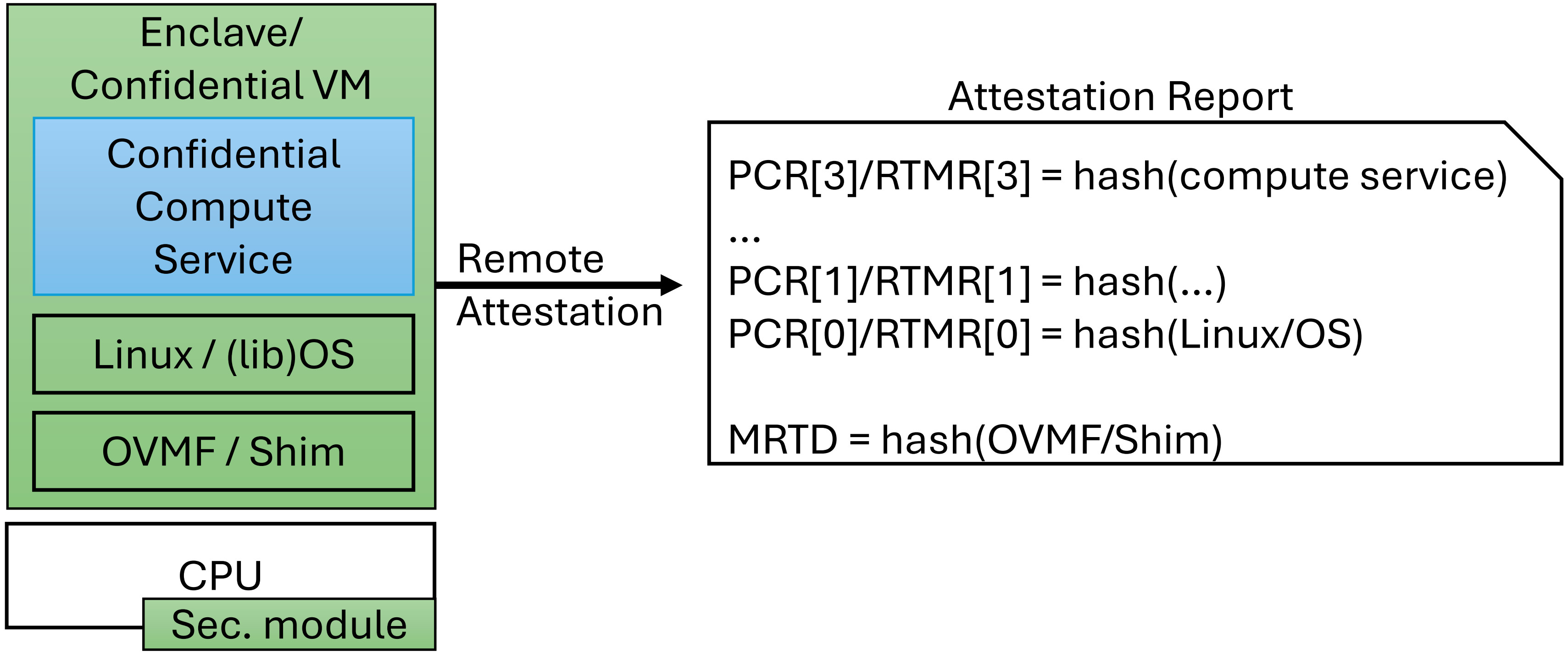
Confidential
AI Service

CPU

# Confidential Compute Services Today



# Challenge: Building Trust in Confidential Compute Services



Enclave/
Confidential VM

Confidential Compute Service

Linux / (lib)OS

OVMF / Shim

CPU

Sec. module

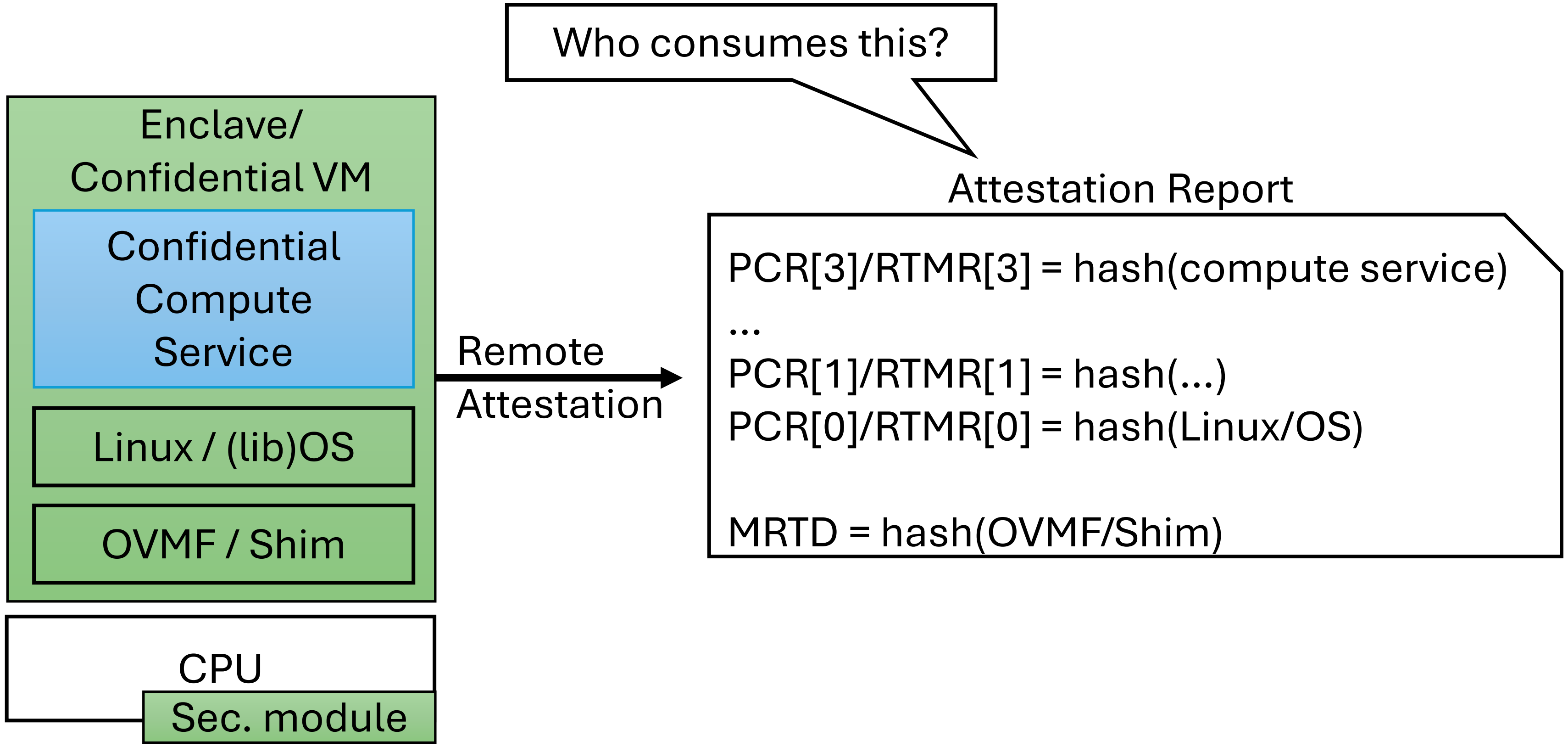
Remote Attestation

Attestation Report

PCR[3]/RTMR[3] = hash(compute service)
...
PCR[1]/RTMR[1] = hash(...)
PCR[0]/RTMR[0] = hash(Linux/OS)

MRTD = hash(OVMF/Shim)

# Challenge: Building Trust in Confidential Compute Services



Who consumes this?

Enclave/ Confidential VM

Confidential Compute Service

Linux / (lib)OS

OVMF / Shim

CPU

Sec. module

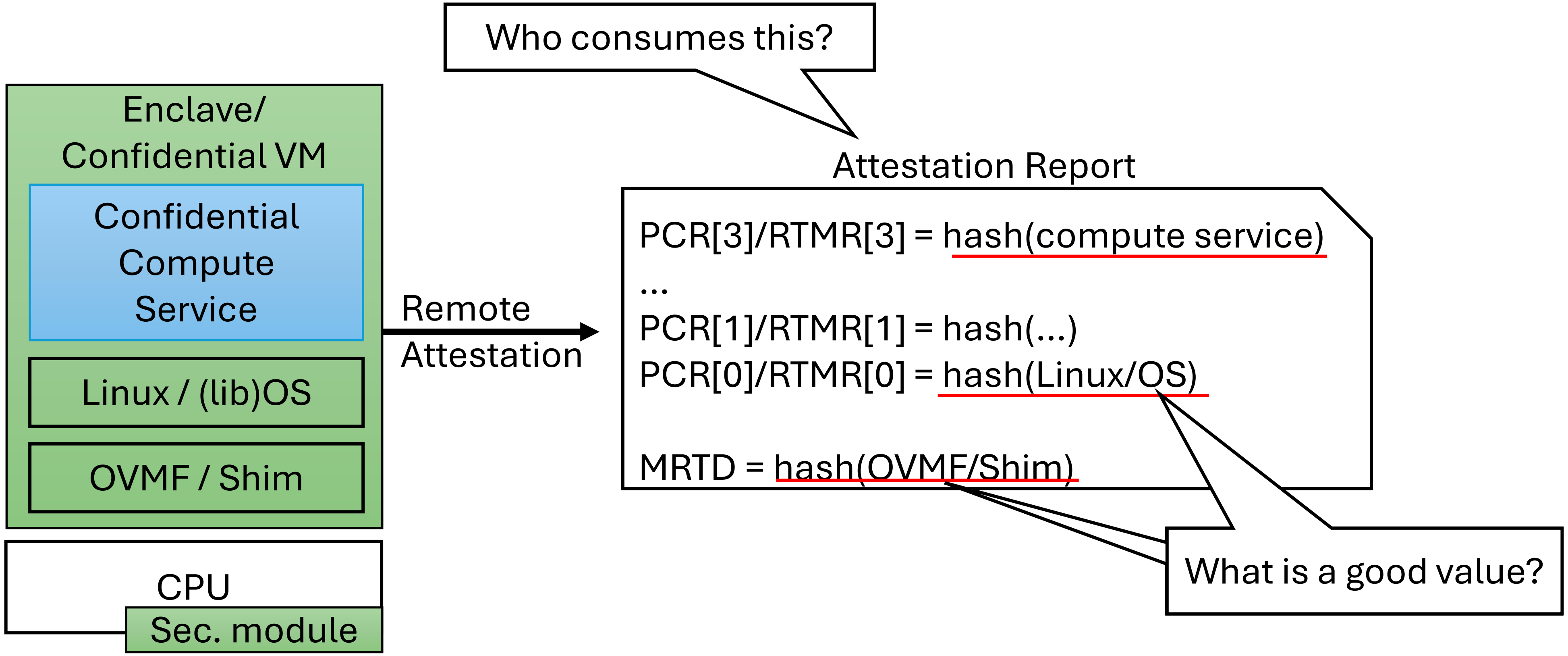
Remote Attestation

Attestation Report

PCR[3]/RTMR[3] = hash(compute service)
…
PCR[1]/RTMR[1] = hash(…)
PCR[0]/RTMR[0] = hash(Linux/OS)

MRTD = hash(OVMF/Shim)

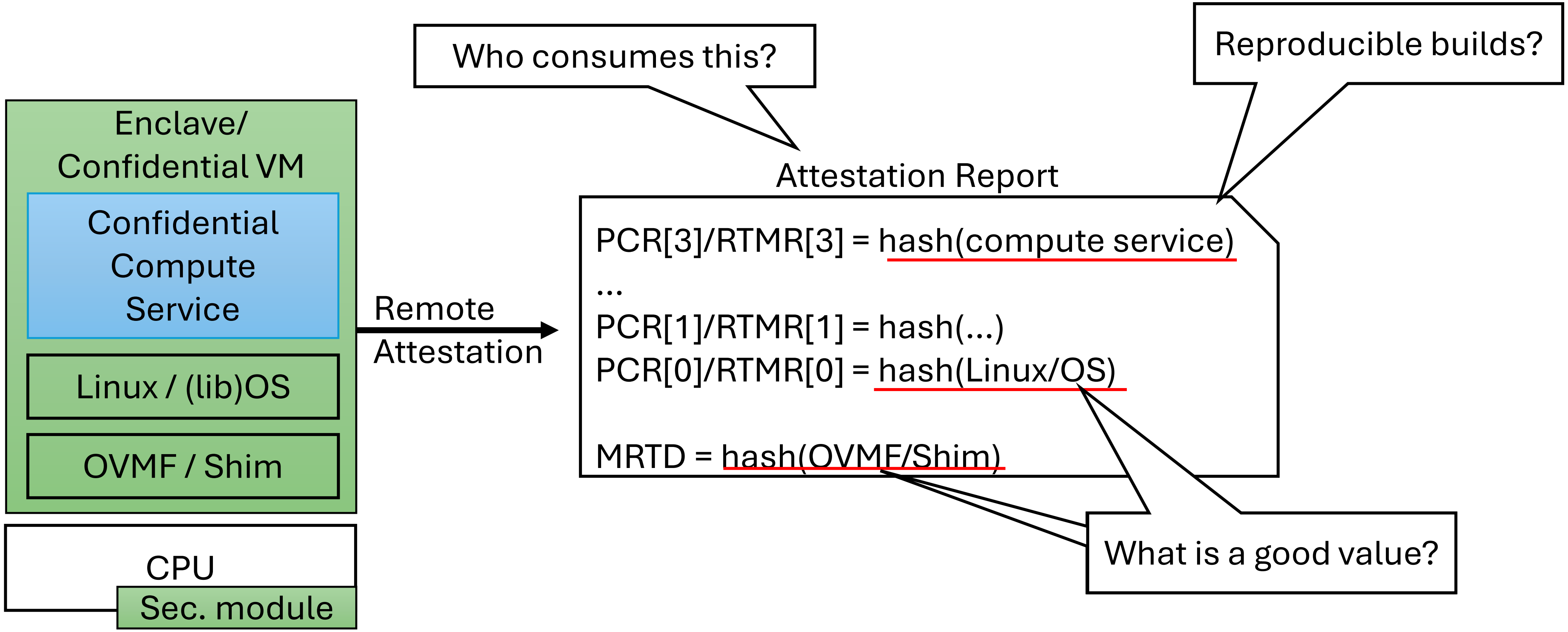
# Challenge: Building Trust in Confidential Compute Services



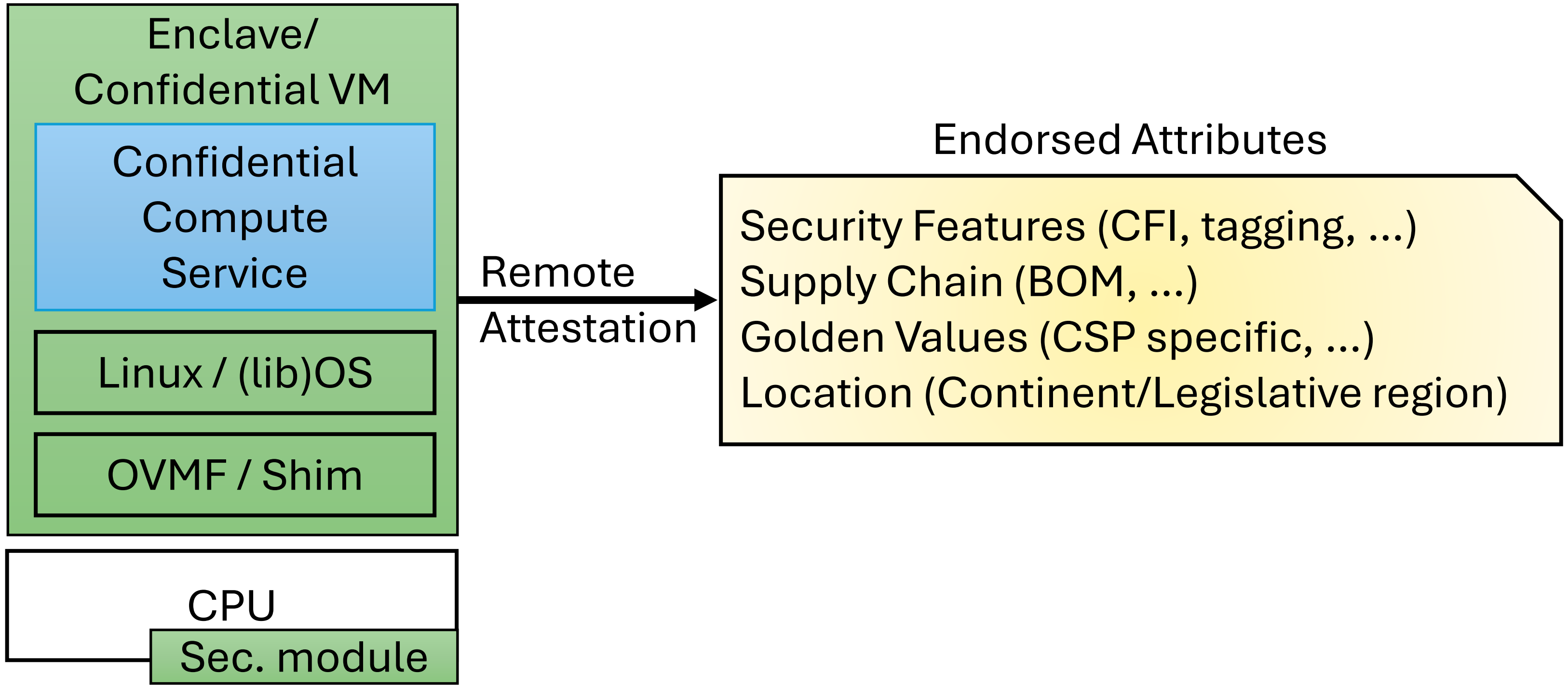
PCR[3]/RTMR[3] = hash(compute service)
...
PCR[1]/RTMR[1] = hash(...)
PCR[0]/RTMR[0] = hash(Linux/OS)

MRTD = hash(OVMF/Shim)

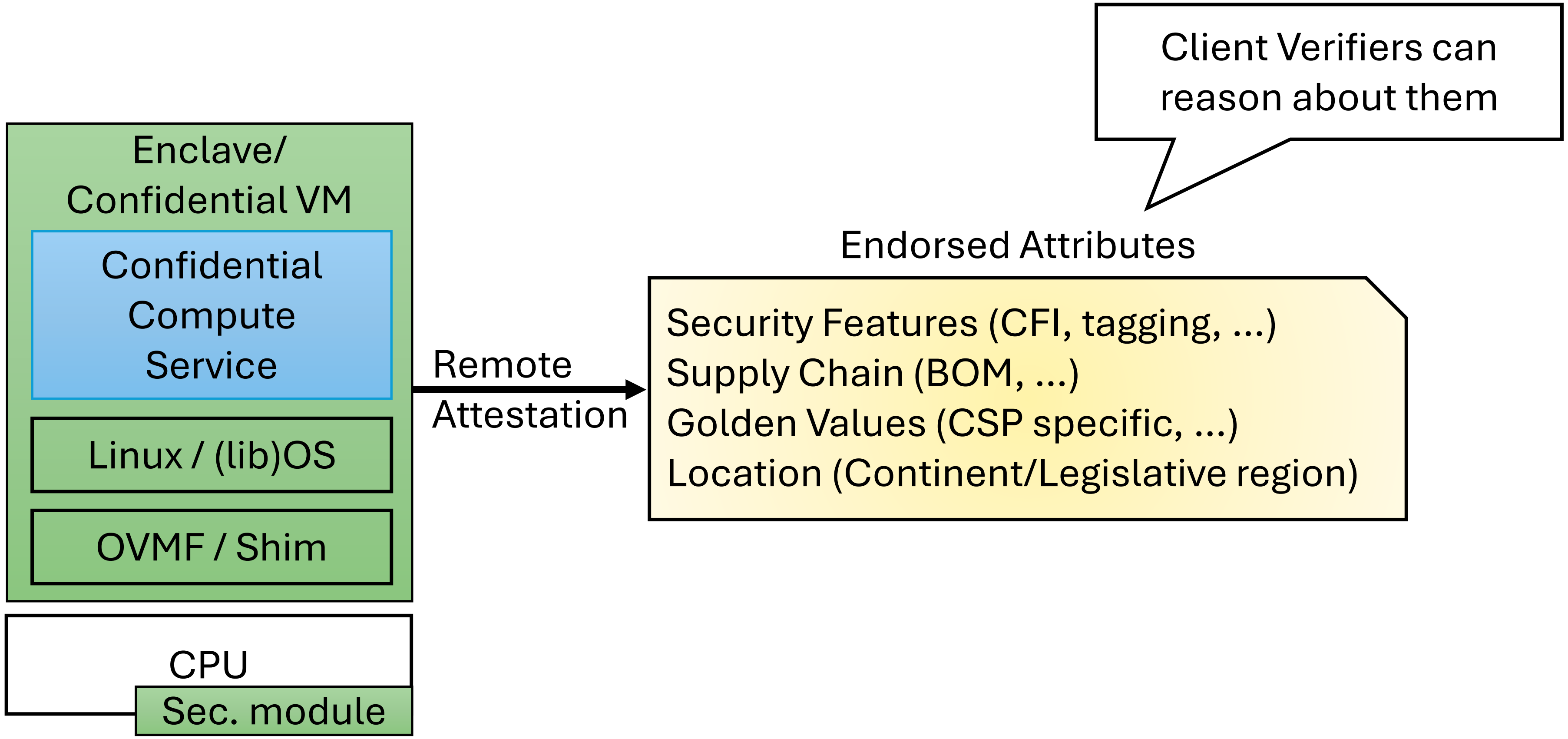
# Challenge: Building Trust in Confidential Compute Services



# Goal: Validate High-Level Attributes, not Low-Level Hashes

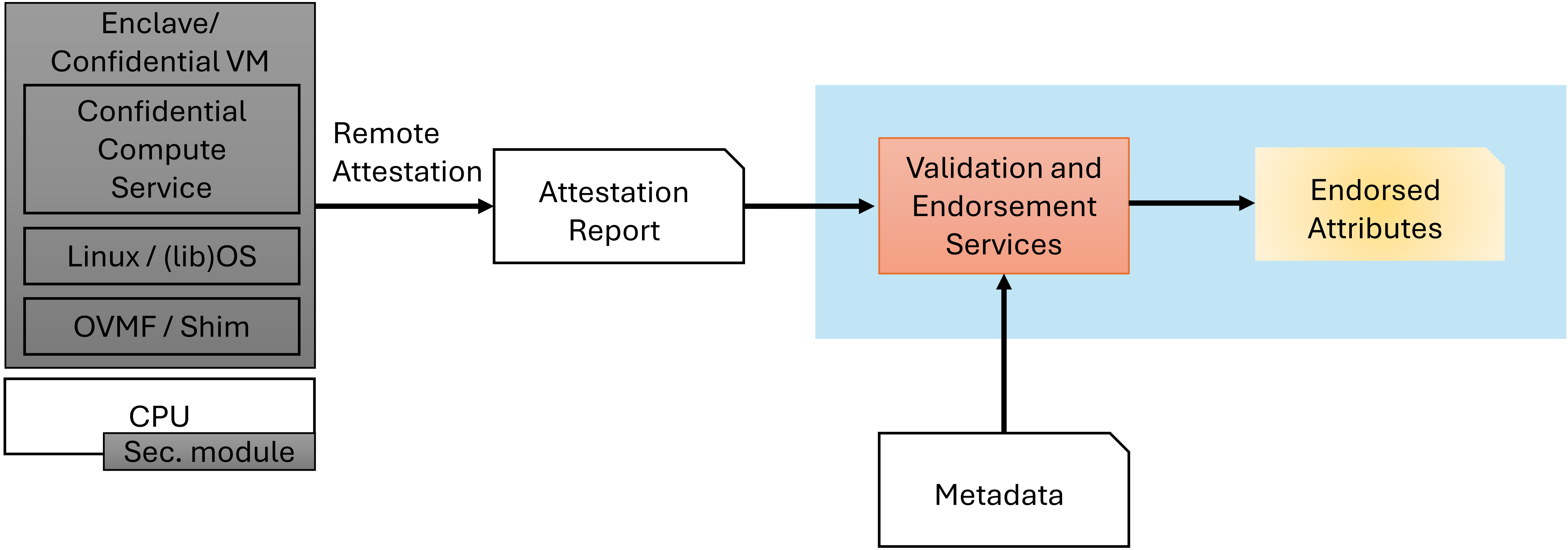

Enclave/
Confidential VM
Confidential Compute Service
Linux / (lib)OS
OVMF / Shim
CPU
Sec. module
Remote Attestation
Endorsed Attributes
Security Features (CFI, tagging, ...)
Supply Chain (BOM, ...)
Golden Values (CSP specific, ...)
Location (Continent/Legislative region)

# Goal: Validate High-Level Attributes, not Low-Level Hashes

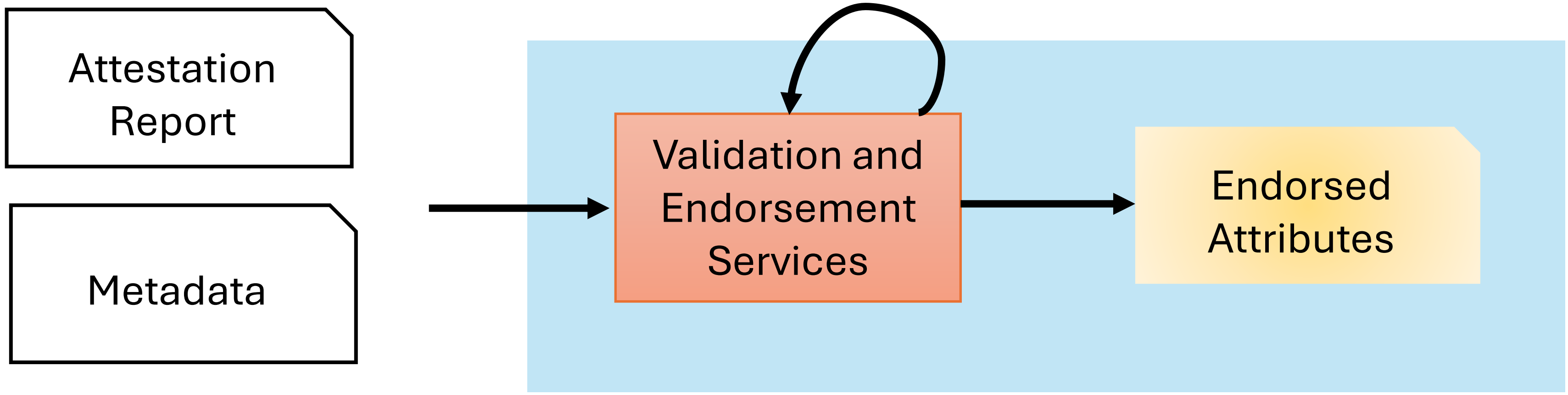


Security Features (CFI, tagging, …)
Supply Chain (BOM, …)
Golden Values (CSP specific, …)
Location (Continent/Legislative region)

# Our Proposal:
# Validation and Endorsement Services (VES)

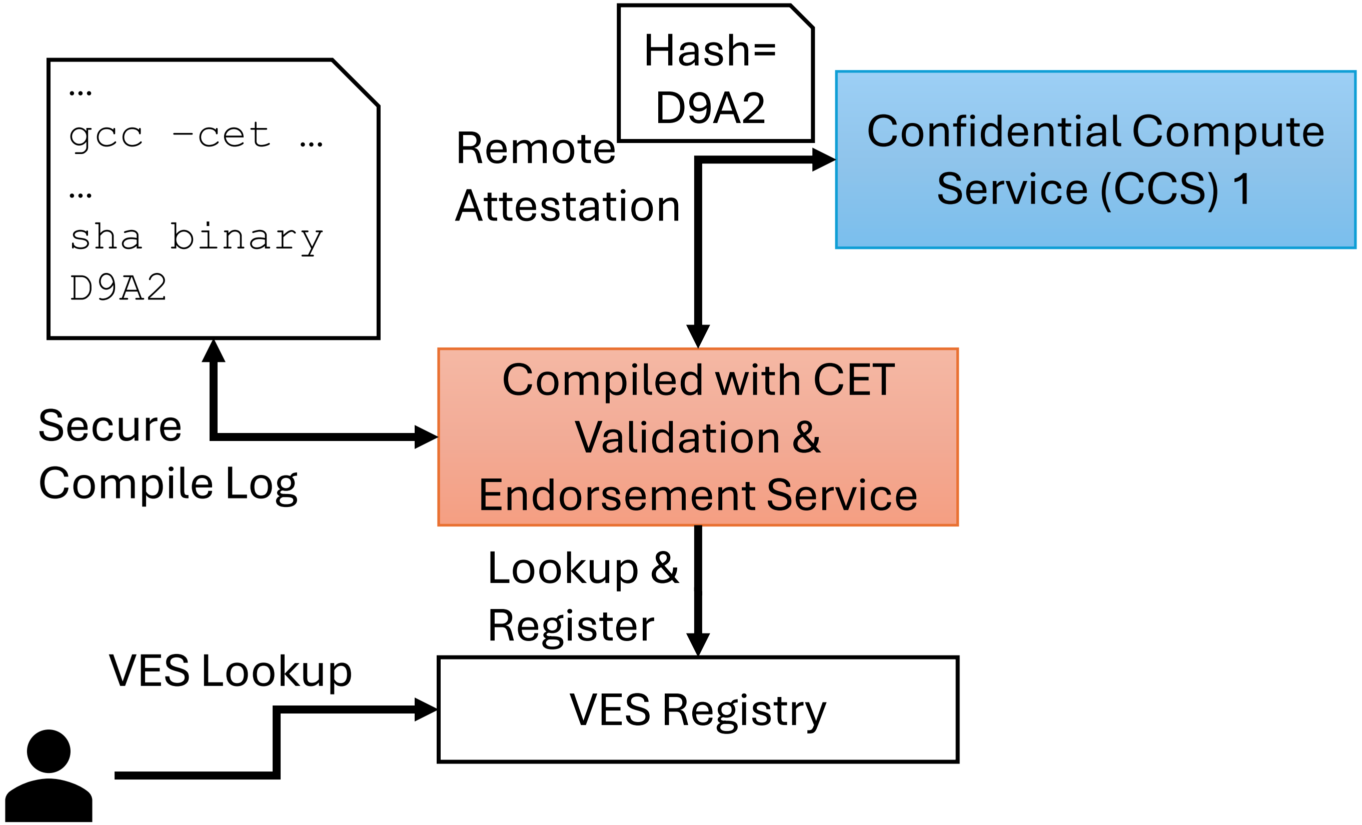


# Validation and Endorsement Services (VES)



- Validate Attribute of a Confidential Compute Service (CCS)
- Endorse Attribute of a CCS
- VES themselves are implemented as CCS -> expand trust transitively
- Trust rooted in Root VES

# CCS & VES Architecture



```
…
gcc -cet …
…
sha binary
D9A2
```

Hash=
D9A2

Remote Attestation

Confidential Compute Service (CCS) 1

Secure Compile Log

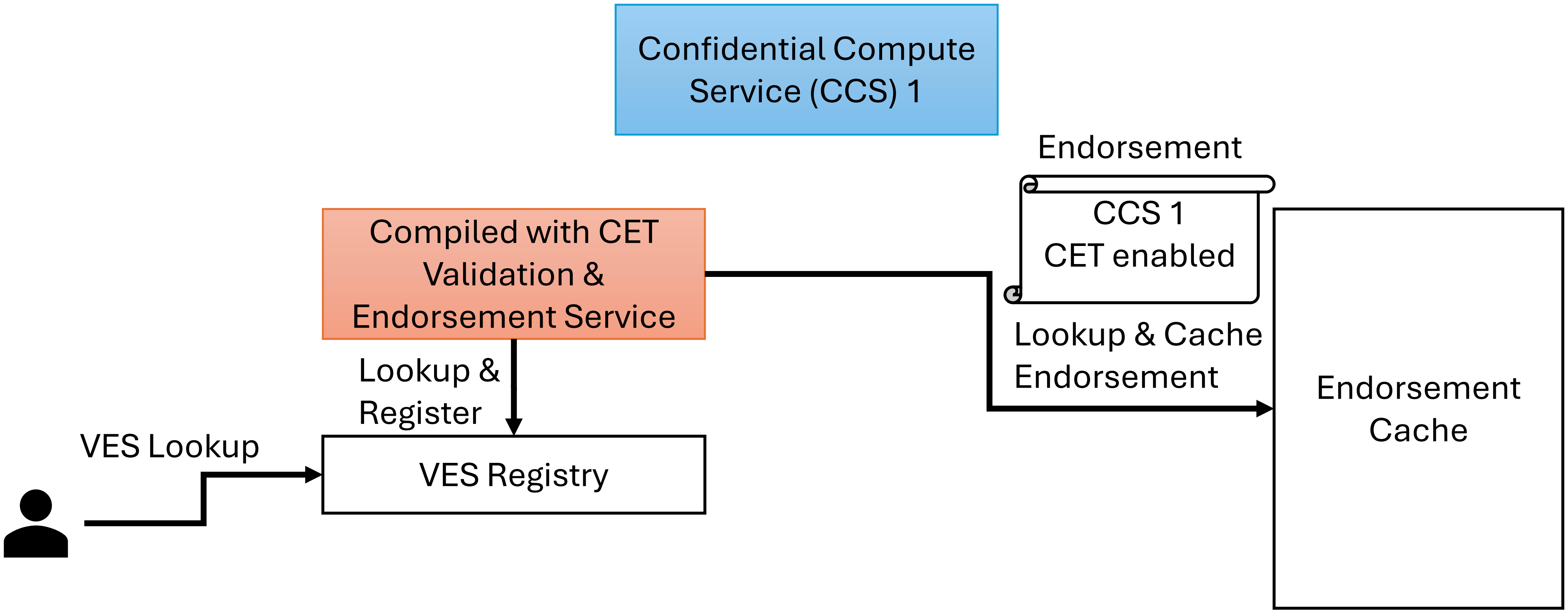
Compiled with CET Validation & Endorsement Service

Lookup & Register

VES Lookup

VES Registry

# CCS & VES Architecture



Confidential Compute Service (CCS) 1

Endorsement

CCS 1
CET enabled

Compiled with CET Validation & Endorsement Service

Lookup & Register

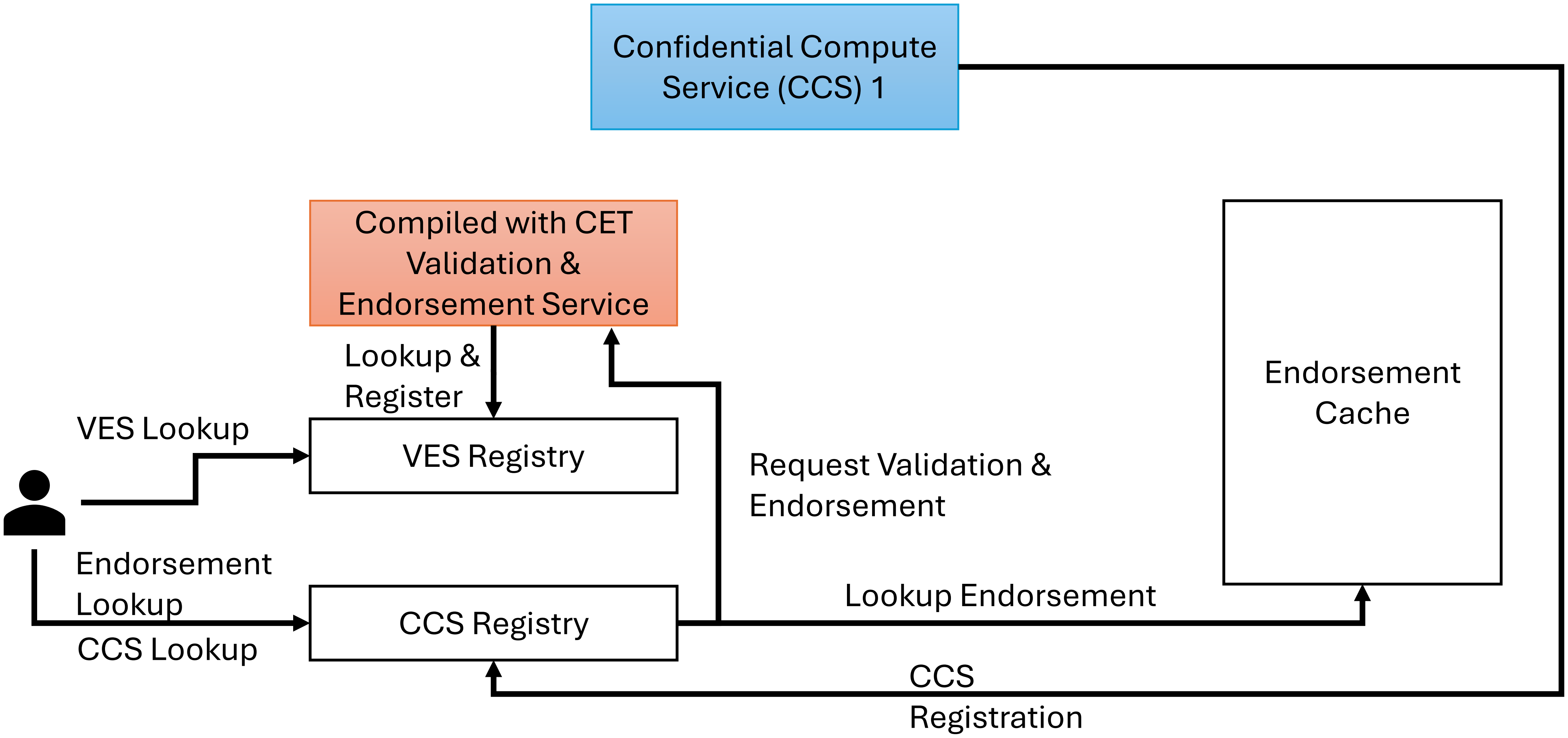
Lookup & Cache Endorsement

Endorsement Cache

VES Lookup

VES Registry

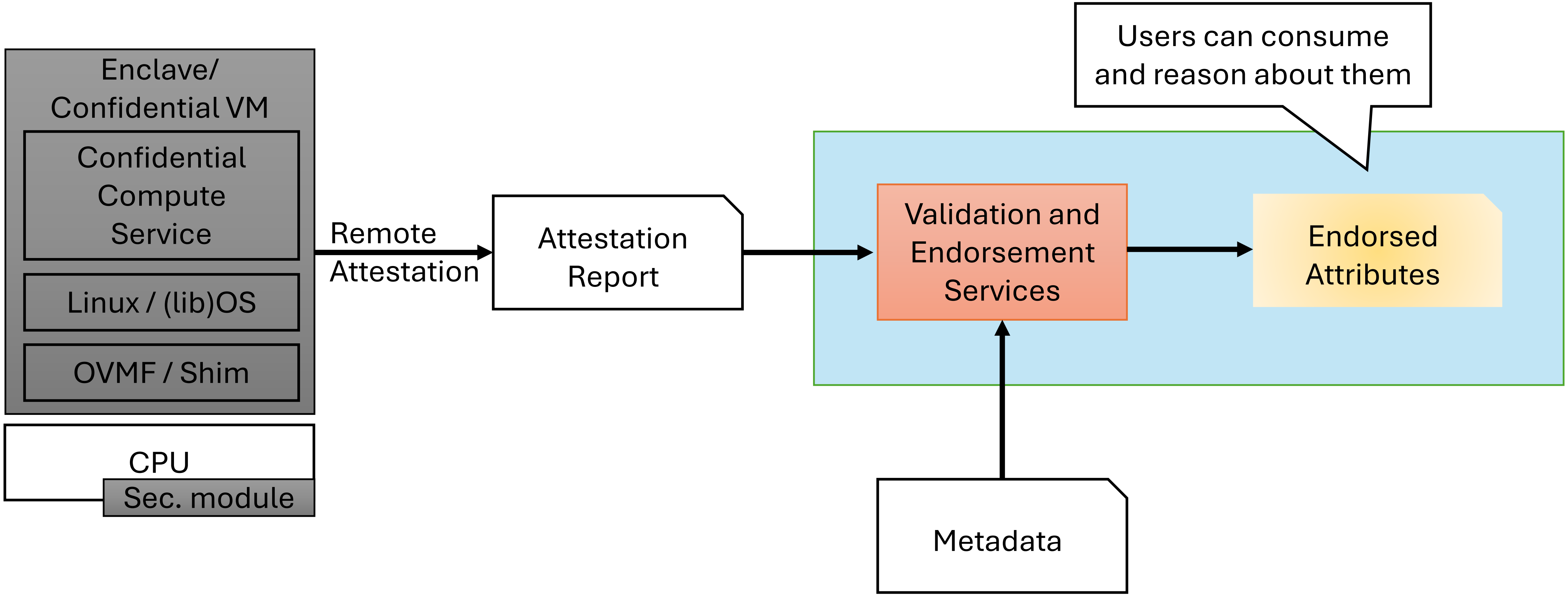
# CCS & VES Architecture



# Future Work and Challenges

- Consistency and validity of endorsements over long time
- What attributes are of the highest interest to endorse?
- Who could operate VESes and Registries?
  - Open-source vs. proprietary
  - What monetization model?

# Summary: Goal: Validate High-Level Attributes, not Low-Level Hashes



# Notices & Disclaimers

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

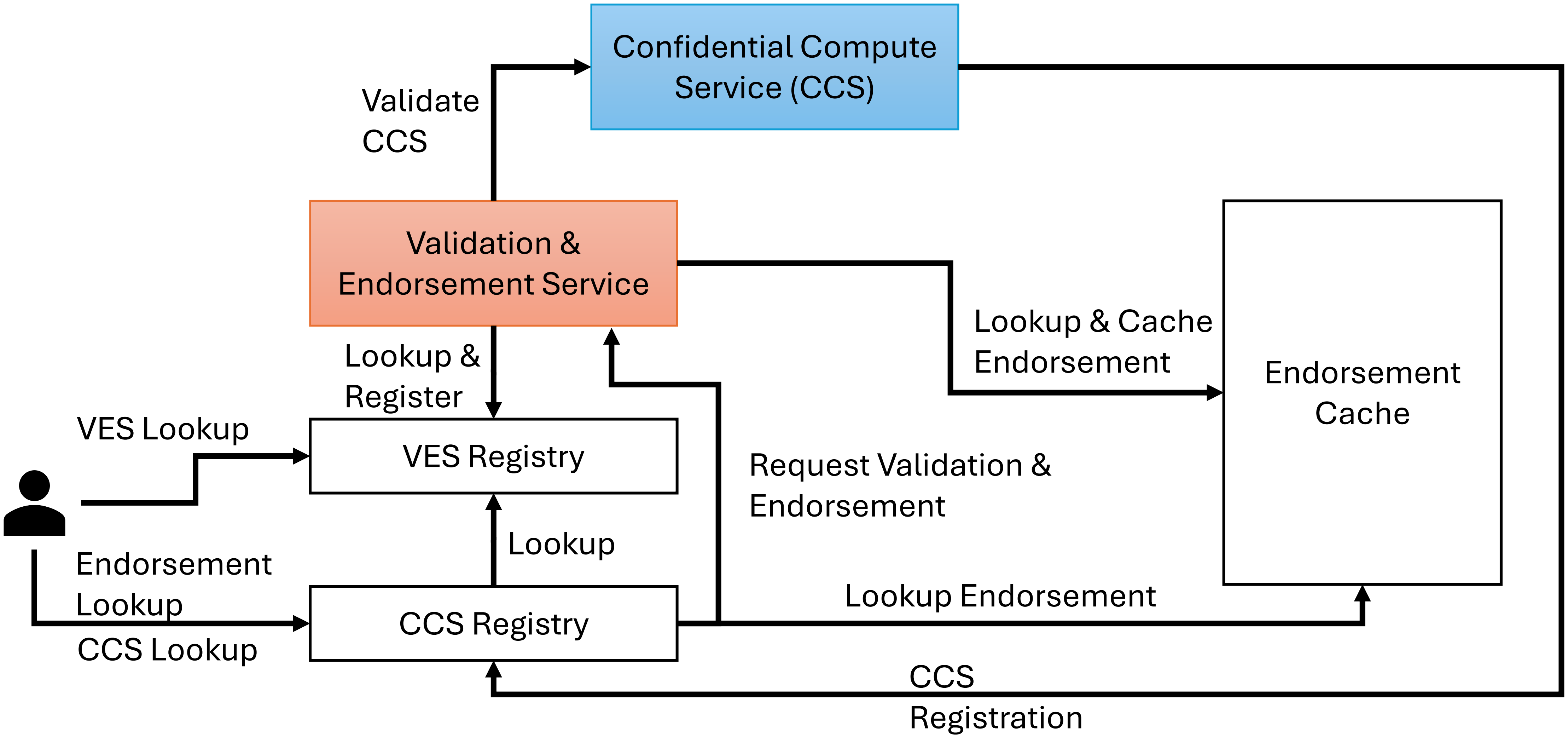
Your costs and results may vary.

© Intel Corporation.  Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries.  Other names and brands may be claimed as the property of others.

# Q&A

Contact:
anjovahldiek@gmail.com
marcela.melara@intel.com

# CCS & VES Architecture



# Sample VESes

- TEE Golden Values
  - Services is entrusted to know deployment specific hash values of OVMF/SHIM, Linux, …
- Supply Chain
  - Accesses external SigStore/DB to retrieve attested Bill of Materials (BOM)
- Secure Compilation
  - Accesses external SigStore/DB to retrieve compilation details (e.g., logs) to evaluate if compilation was performed with security flags
- Geo Location
  - Perform ping benchmarks to determine approximate location

# Threat Model

CCSes and VESes should:

- Run in a TEE to preserve confidentiality and integrity
- Perform link encryption (RA-TLS)

- Root VES requires out of band trust like a certificate authority

- Trusted: Crypto and TEEs