Microsoft

Azure vTPM Attestation and Binding

Mike Stunes
Microsoft, Modern VM & Migration
July 29, 2025

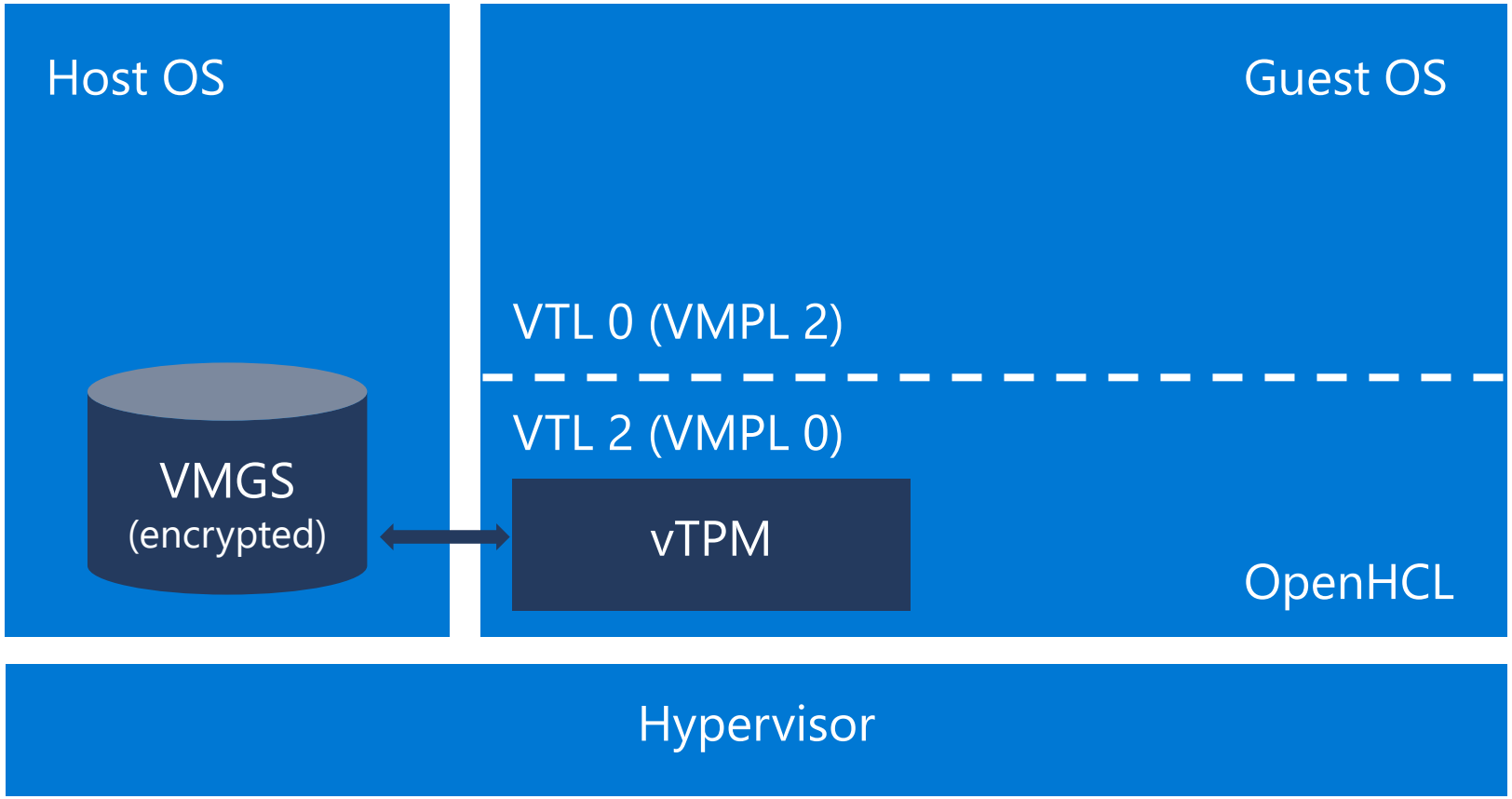
Scenario

- Binding vTPM evidence to CVM platform evidence
- How do I prove that a vTPM lives in a CVM?

Context

- TPM Quote: sign PCR state or other data with a key from the vTPM
- Azure VMs get endorsement key (EK) and attestation key (AK) provisioned in their vTPM
  - (Primary encryption/signing keys in endorsement hierarchy)
- CVM contains paravisor layer that provides vTPM

Context: CVM vTPM



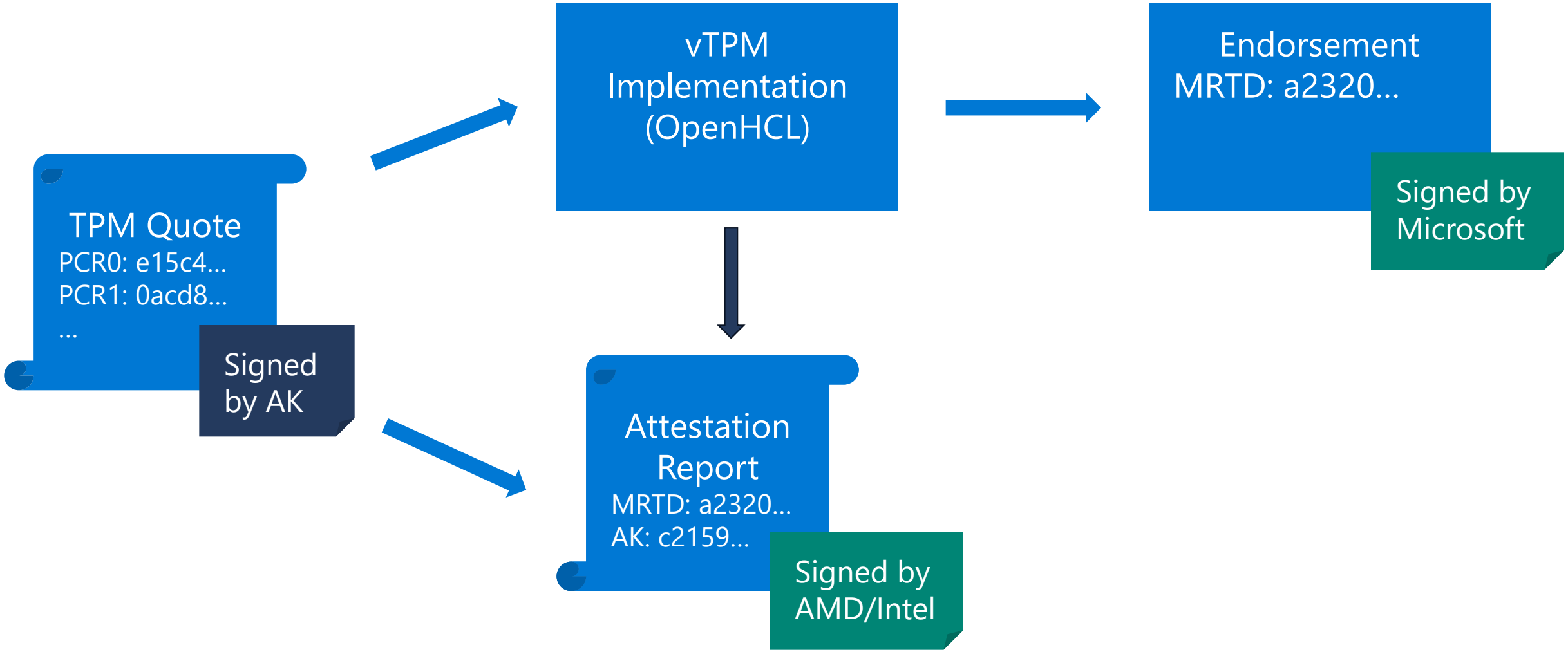
Simplified from [OpenHCL Architecture Diagram]

Scenario, restated

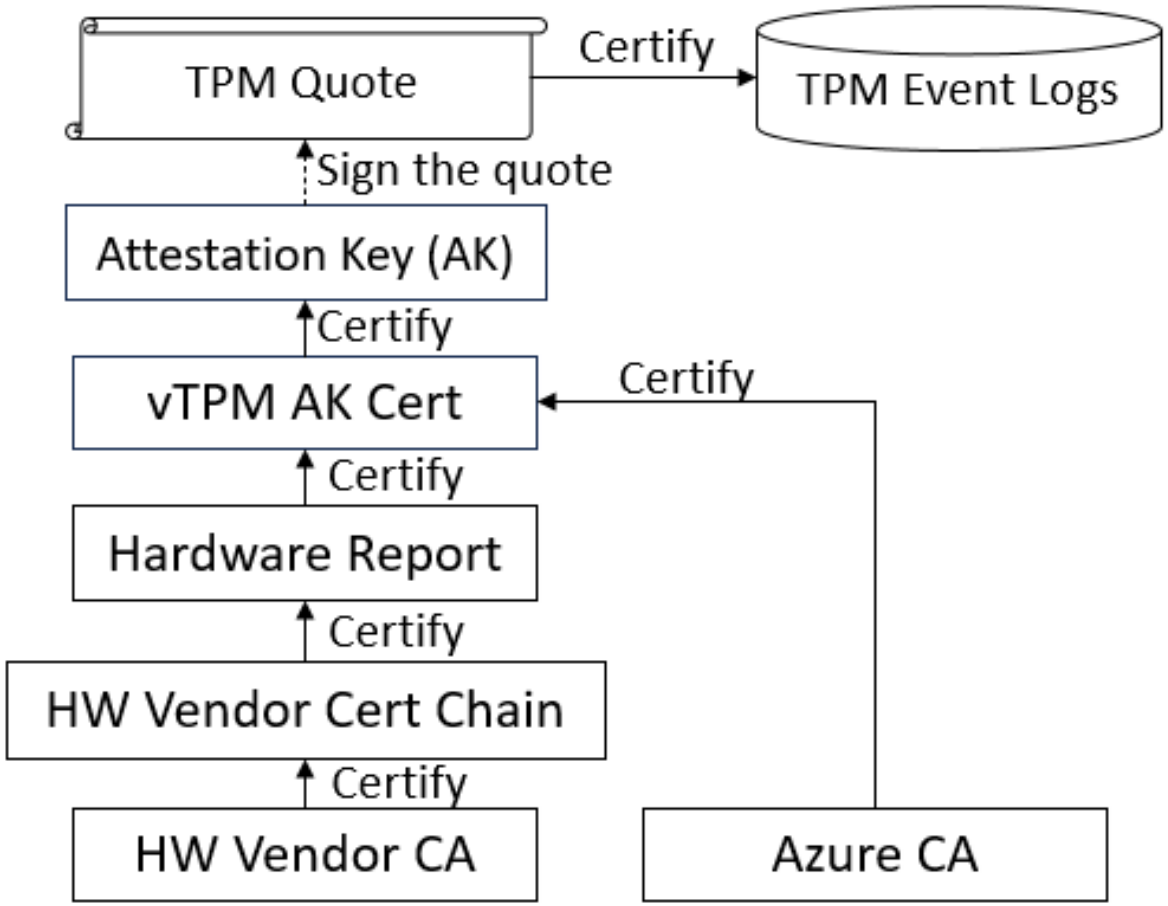
If I sign data or a TPM quote:

- How do I prove that the TPM is in a CVM?
- How do I prove that the TPM is trustworthy?
- What are my roots of trust?

vTPM Chain of Trust



vTPM Chain of Trust



Attestation Report NVRAM Index

Azure vTPM provides a way to get a hardware attestation report

Saved in TPM NVRAM index that guest OS can read

```
pub struct IgvmAttestRequest {
    /// Header (unmeasured)
    pub header: IgvmAttestRequestHeader,
    /// TEE attestation report
    pub attestation_report: [u8; ATTESTATION_REPORT_SIZE_MAX],
    /// Request data (unmeasured)
    pub request_data: IgvmAttestRequestData,
    // Variable-length [`runtime_claims::RuntimeClaims`] (JSON string) in raw bytes will be
    // appended to here.
    // The hash of [`runtime_claims::RuntimeClaims`] in [`IgvmAttestHashType`] will be captured
    // in the `report_data` or equivalent field of the TEE attestation report.
}
```

Source: OpenVMM GitHub

Attestation Report NVRAM Index, cont'd.

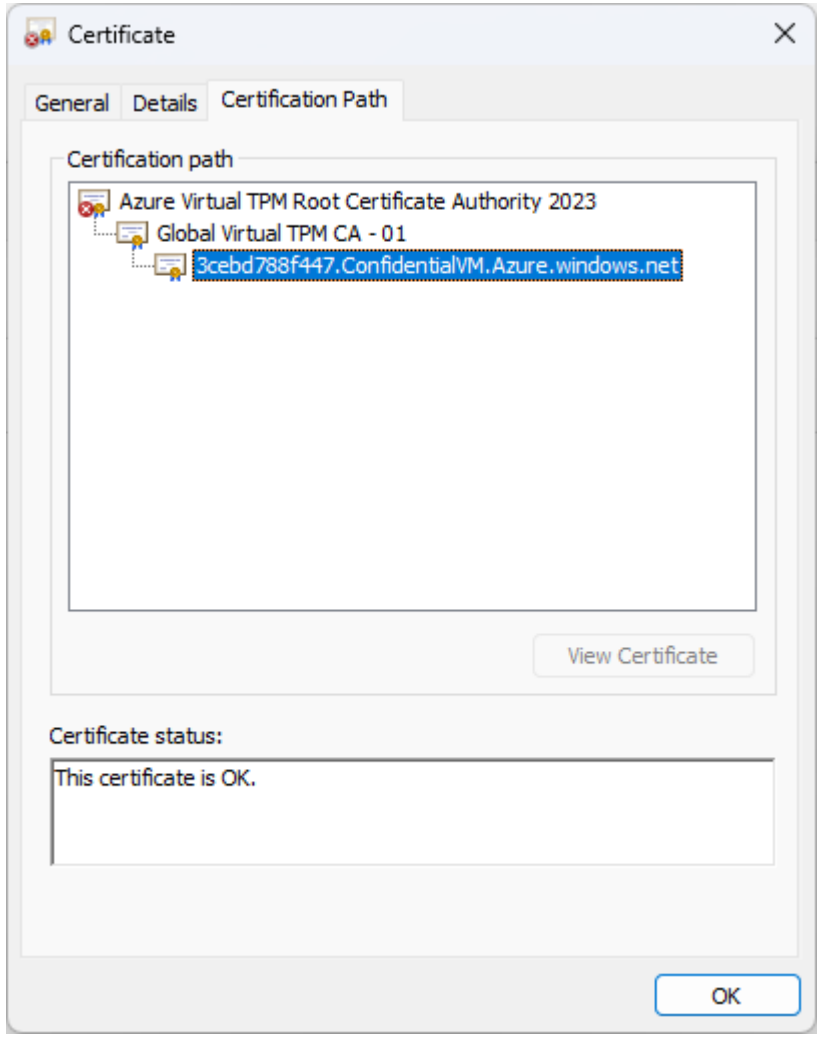
User data in attestation report includes AK and EK

```
{
  "keys": [
    {"kid": "HCLAkPub", "key_ops": ["sign"], "kty": "RSA", "e": "AQAB", "n": "whWaug..." },
    {"kid": "HCLEkPub", "key_ops": ["encrypt"], "kty": "RSA", "e": "AQAB", "n": "pEtMPA..." }
  ],
  "vm-configuration": {
    "console-enabled": true,
    "secure-boot": true,
    "tpm-enabled": true,
    "vmUniqueId": "A32769B7-885D-4B76-AE5A-64AD81ECC2C3"
  },
  "user-data": "0000..."
}
```

User can write additional data to TPM NVRAM; reflected in attestation report (up to 64 bytes)

AK Certificate

- Azure VMs have AK signed by Azure Virtual TPM CA
- Cert is available in TPM NVRAM
- Link to CA bundle



Resources

- OpenHCL Code: https://github.com/microsoft/openvmm
- OpenHCL Public Website: https://openvmm.dev
- Azure TDX public preview (DCesv6)
- Intel Trust Authority Client Tutorial
- Example attestation code
  - https://github.com/Azure/cvm-attestation-tools/
  - https://github.com/Azure/confidential-computing-cvm-guest-attestation
- Microsoft Azure Attestation documentation
- CVM Guest Attestation Design documentation

Conclusion

- Key point: TPM is bound to CVM by including keys in attestation report
- Roots of trust:
  - Platform vendor (Intel, AMD) key: genuine CPU
  - Microsoft HCL signing key: properly implemented vTPM
  - Azure Virtual TPM CA: Compliant Azure CVM
- Open discussion: other patterns or approaches for vTPM attestation?