Device Attestation, Confidential Identity, and Generic vTPM Support in Trustee

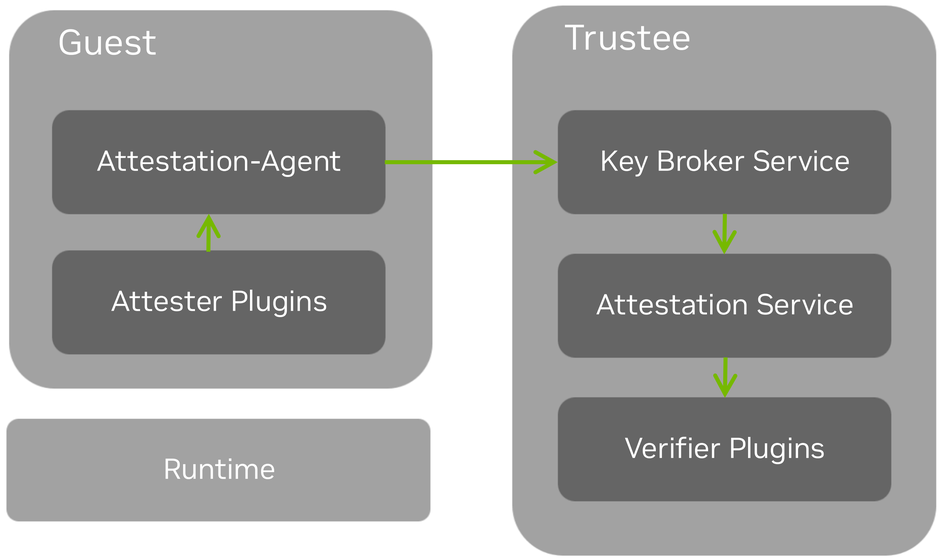
Tobin Feldman-Fitzthum | OC3 2026

Agenda

- Introduction to Trustee
- Attesting Devices
- Confidential Identity
- Generic Confidential vTPM Attestation

Trustee

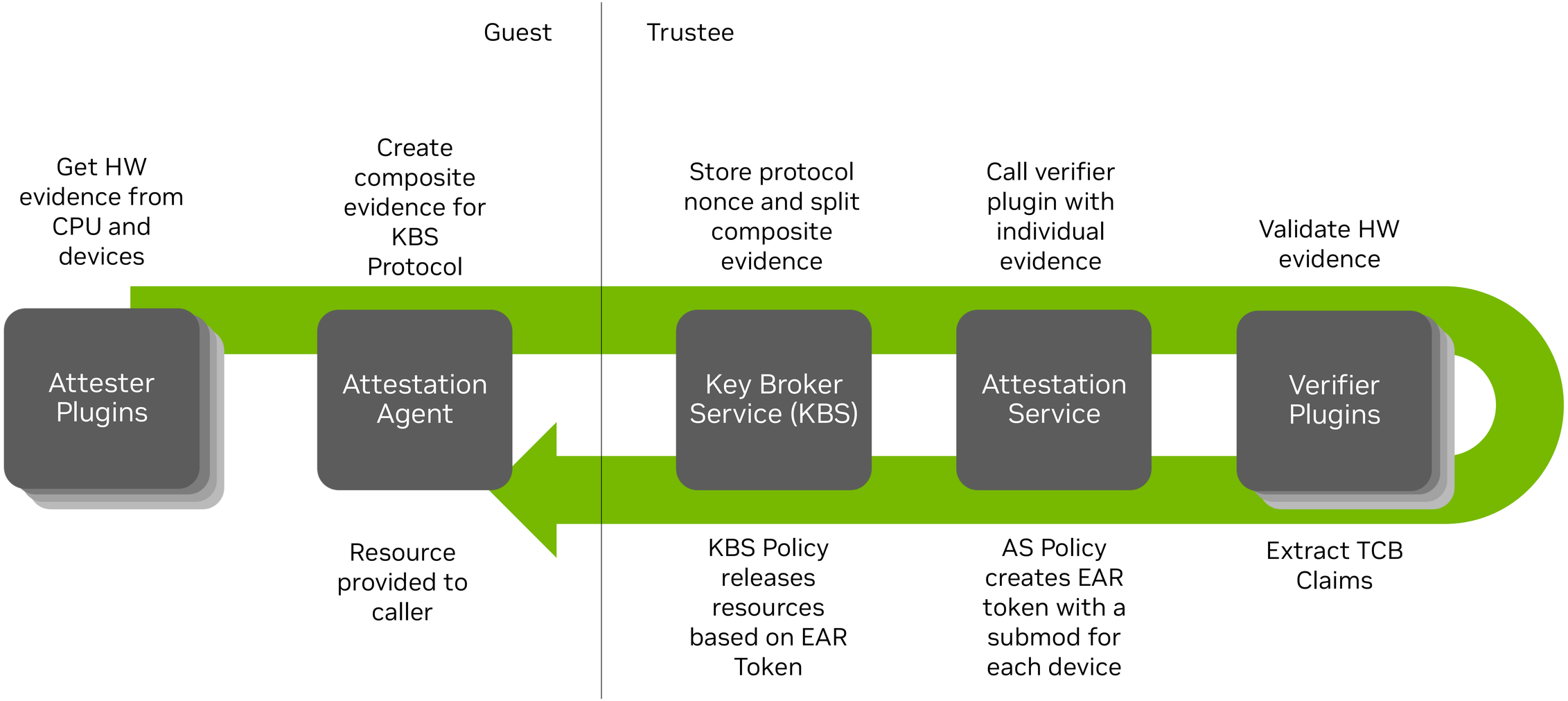
- Open source attestation project
- Balancing rigor, ease of use
- Pluggable
- Broad platform support
  - SNP, TDX, SGX, CCA, IBM SE, CSV, DCU, (v)TPM, Azure, NVIDIA



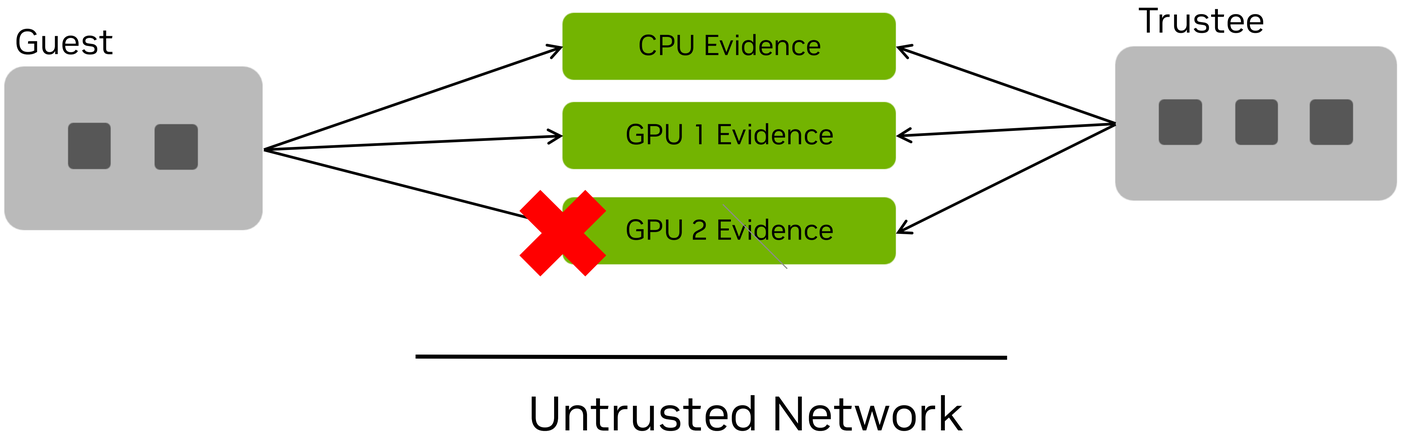
https://github.com/confidential-containers/trustee
https://confidentialcontainers.org/docs/attestation/

```
git clone https://github.com/confidential-containers/trustee
cd trustee && docker compose up
```

Attestation Flow

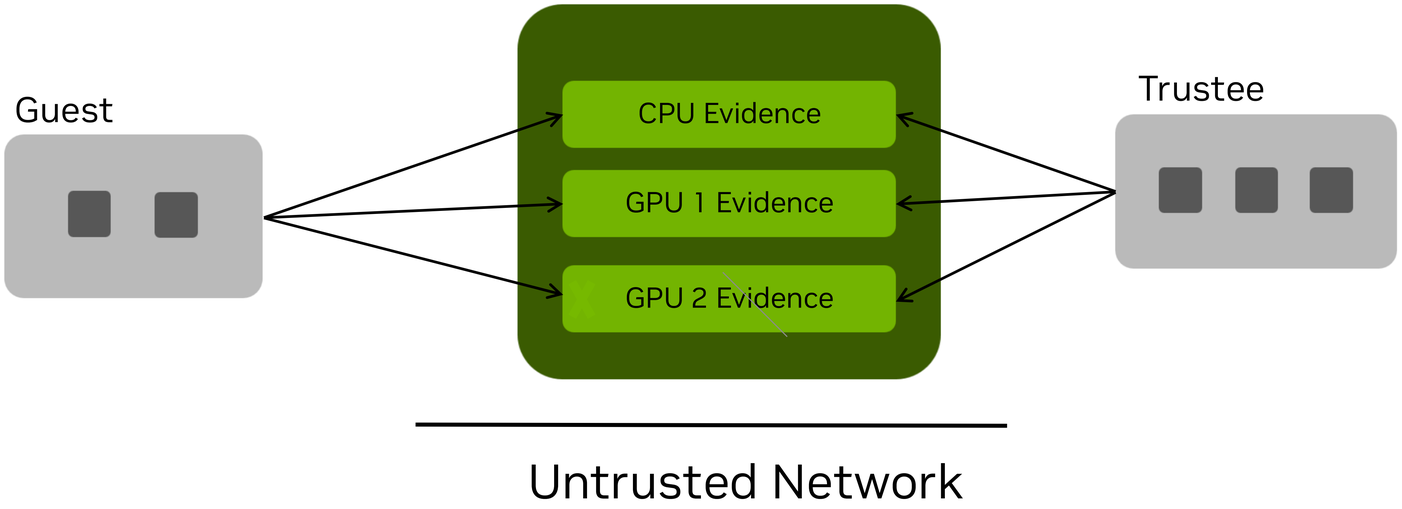


(Without) Composite Evidence



If device evidence is not bound together, a MITM can remove or replace a device in transit

Composite Evidence



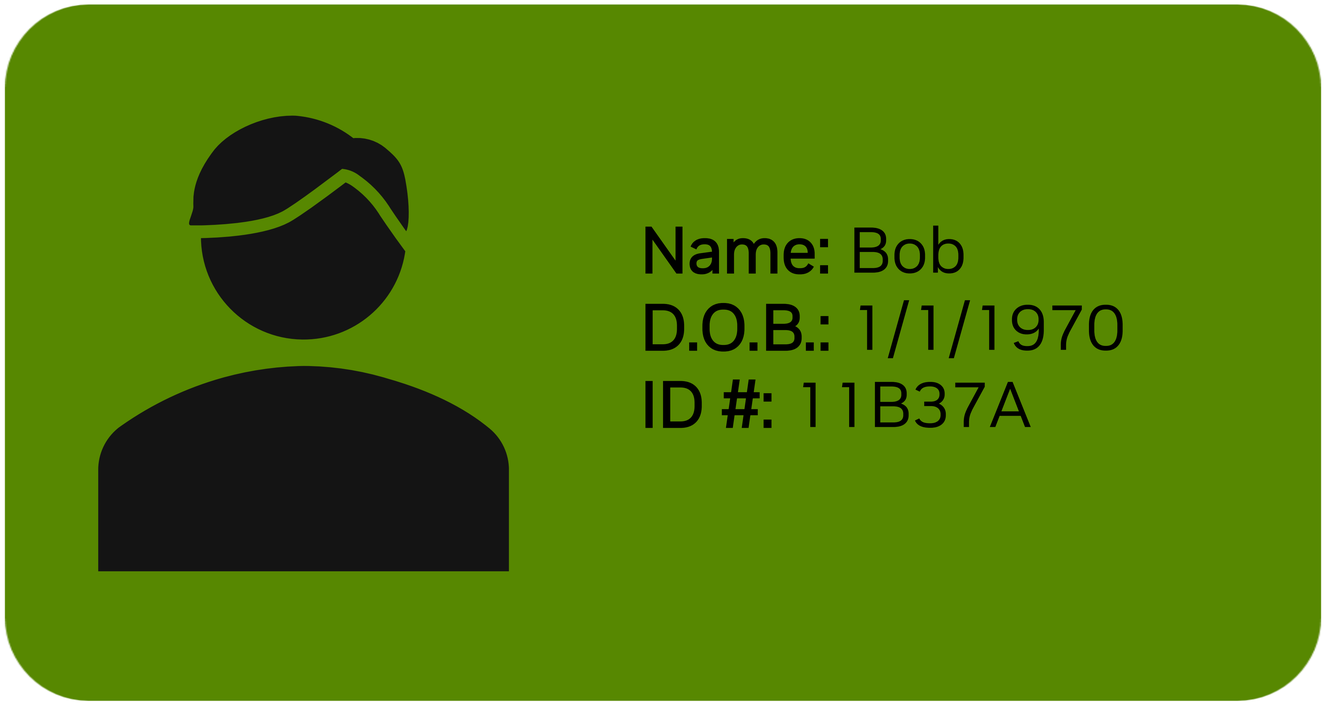
Additional devices are bound to the primary device (CPU) via report data.

Multi-Device Attestation

- Composable
- Transparent to the user
- NVIDIA Hopper and Blackwell GPUs support with SPT and MPT (including PPCIE)

What is Identity?

Who are you?
What are you?



Strings

Bound to your physical identity

Part of a system

Made up of many identifiers

Explicit or Implicit

Confidential Identity

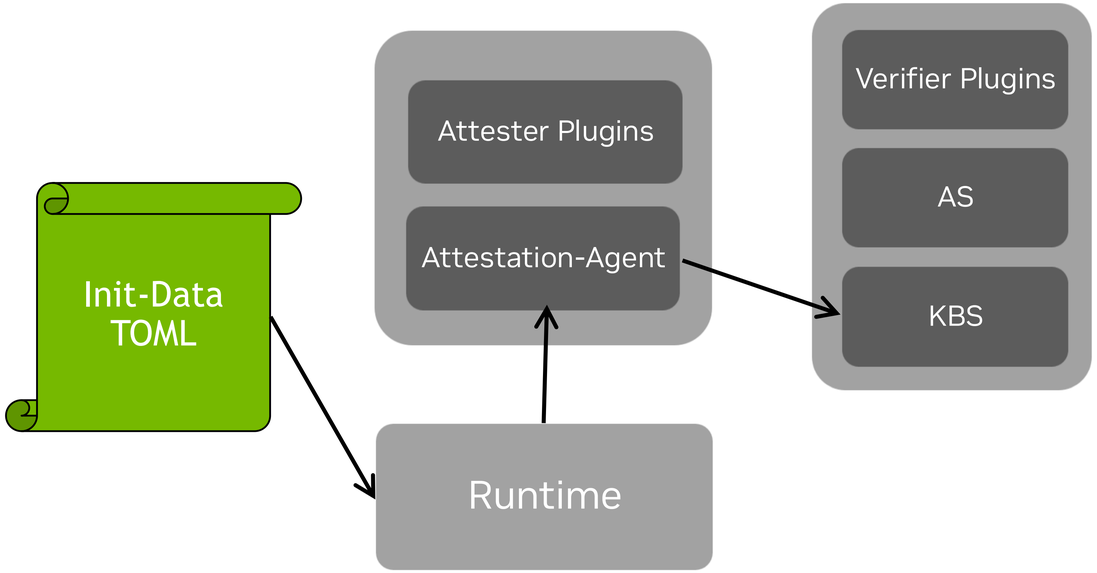
- Not all identifiers can be backed by HW evidence
- HW-specific identifiers vs generic identifiers
- Context loss
  - Hashes
  - Trust boundaries

Init-Data

- Specification for expressive guest configuration
- Based on *hostdata | mrconfig*

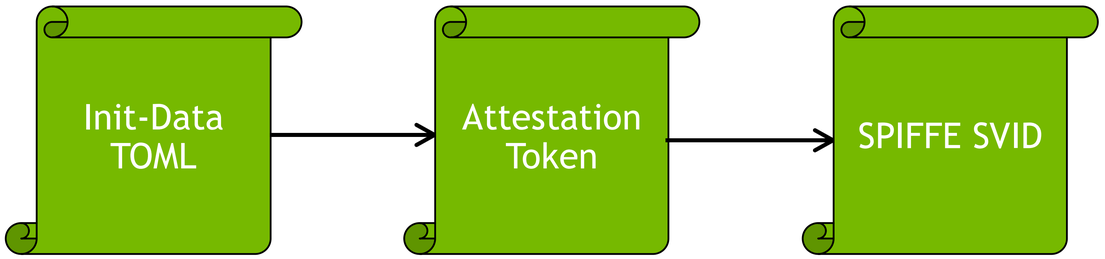
- Init-Data flows from user, to runtime, to guest, to Trustee

- Init-Data plaintext is bound to hardware measurement by Attestation Agent and Trustee

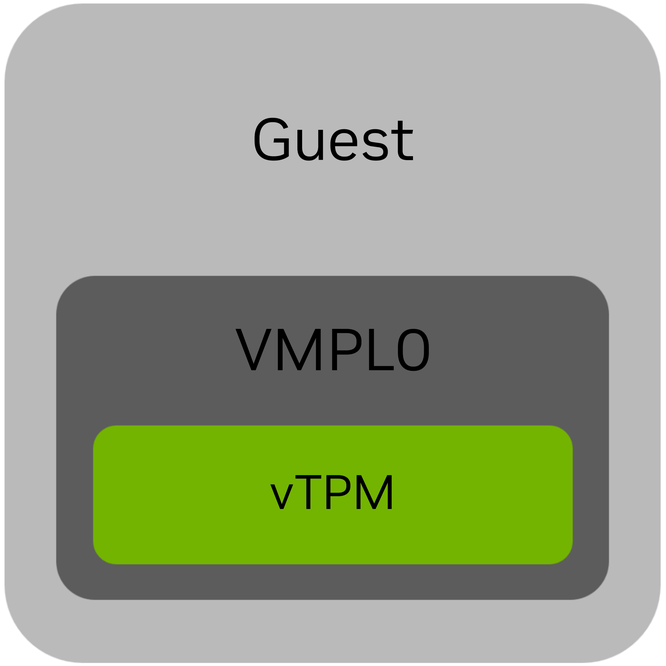


Validated Identifiers

- An extension to the EAR token
- Extracted from Init-Data by Attestation Service policy
- If a validated identifier is set, it must reflect the workload
- Generic

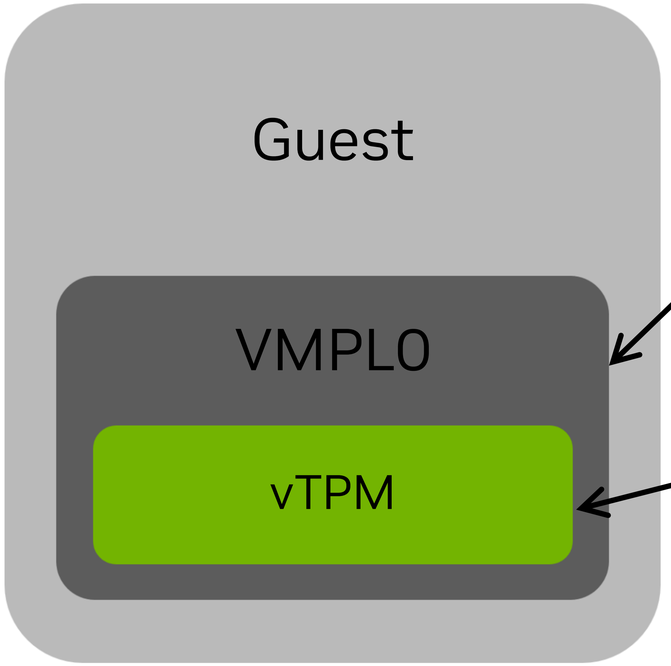


Generic vTPM Support



- vTPMs can be emulated inside the guest in plane 0.
- There are many combination of guest, paravisor, and vTPM
  - SVSM vTPM on SNP, Azure vTPM on TDX, non-confidential vTPM, TPM
- Can we attest all of these generically

Generic vTPM Support



Create an attester for each paravisor. This returns HW evidence (VMPL0) plus claims bound to the HW evidence

Use a generic TPM attester based on TPM quotes

Check the binding of 1) and 2) via policy. The quote should be signed by a public key bound to the VMPL0 evidence

Trustee

- Attestation has moved past one CPU
  - Complex guests with many devices
  - Complex workloads with many guests

- In open source, all these advancements compound

https://github.com/confidential-containers/trustee
https://confidentialcontainers.org/docs/attestation/

#confidential-containers-trustee in CNCF Slack Workspace

```
git clone https://github.com/confidential-containers/trustee
cd trustee && docker compose up
```