Attestation and Verification

Season 2: Shrinking The Elephant

sameo@rivosinc.com - LPC 2023

Rivos

Last Season Recap

Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment. (CCC whitepaper)

Protecting data in use is of limited value if you can't trust who generates and uses it

Last Season Recap

Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment. (CCC whitepaper)

Protecting data in use is of limited value if you can't trust who generates and uses it

Confidential Computing without attestation and verification is not confidential

Last Season Recap

Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment. (CCC whitepaper)

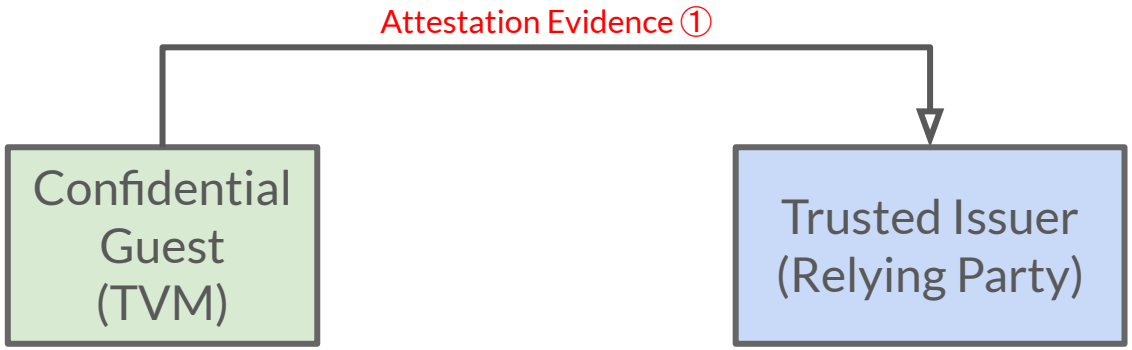
Protecting data in use is of limited value if you can't trust who generates and uses it

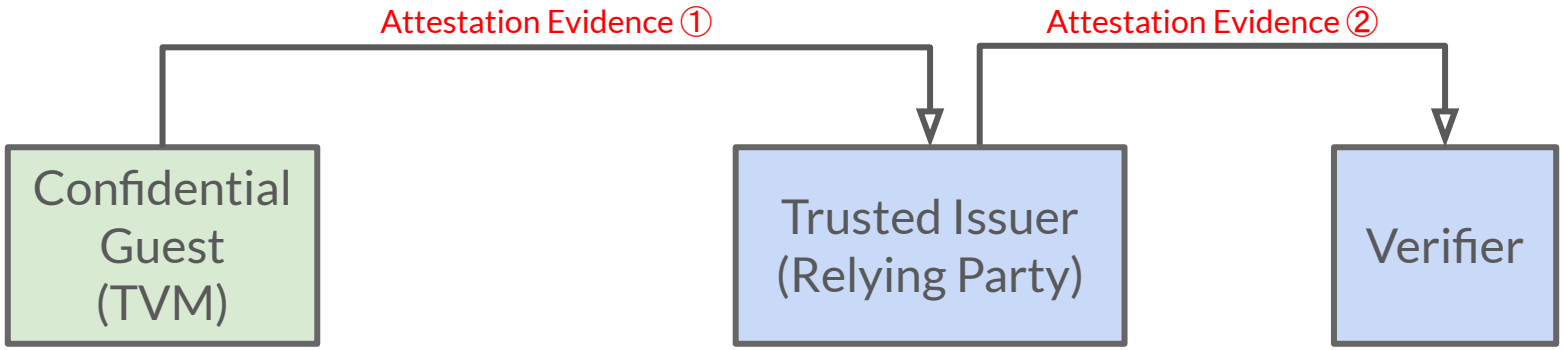
Confidential Computing without attestation and verification is not confidential

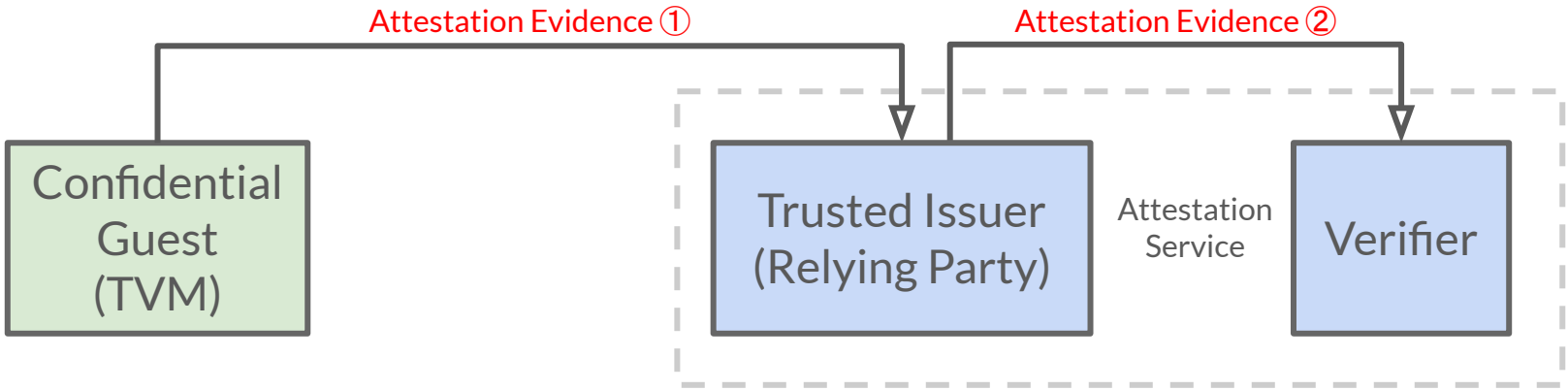
Interfaces, protocols, formats, and manufacturer interactions are very fragmented

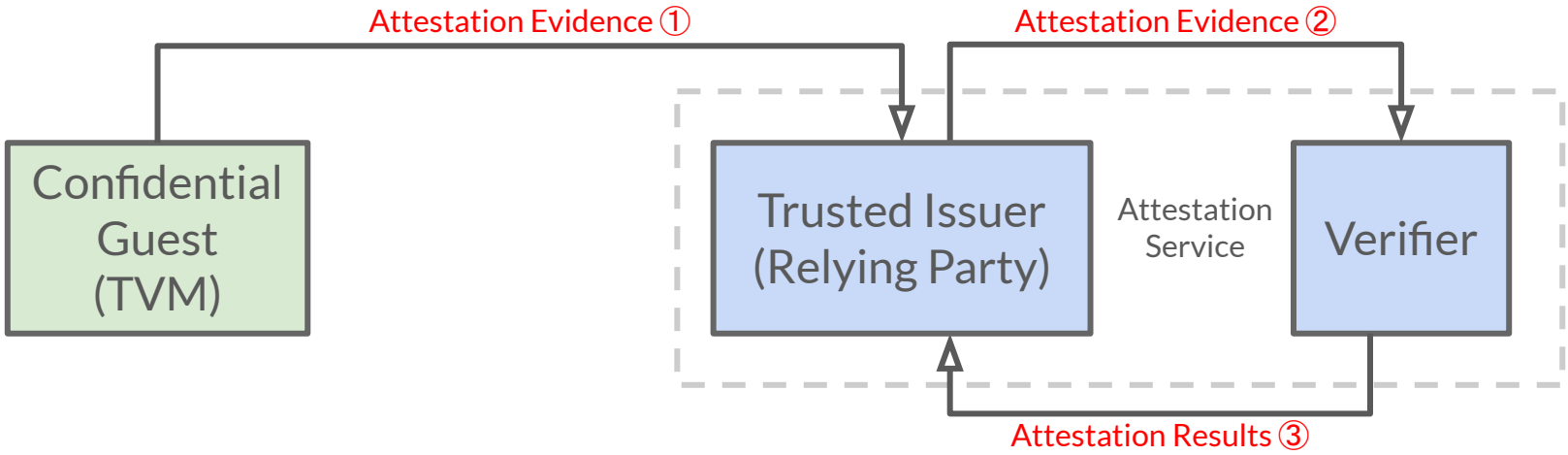
Plumbing an attestation evidence into an attestation service is very challenging

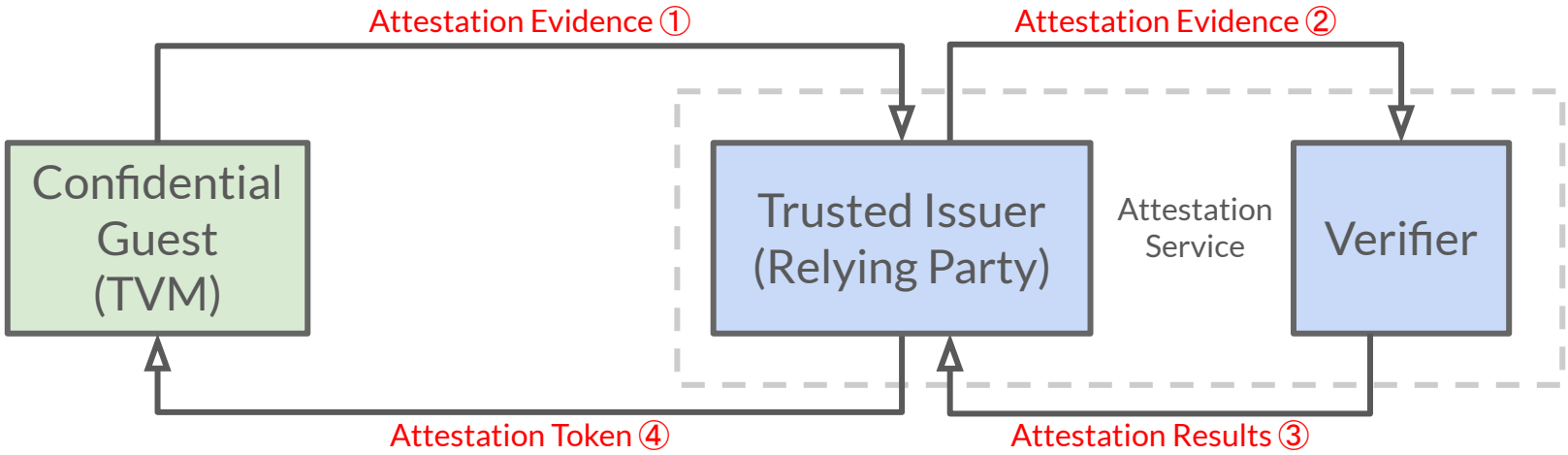
[1] e.g. Decryption key, AI model, etc

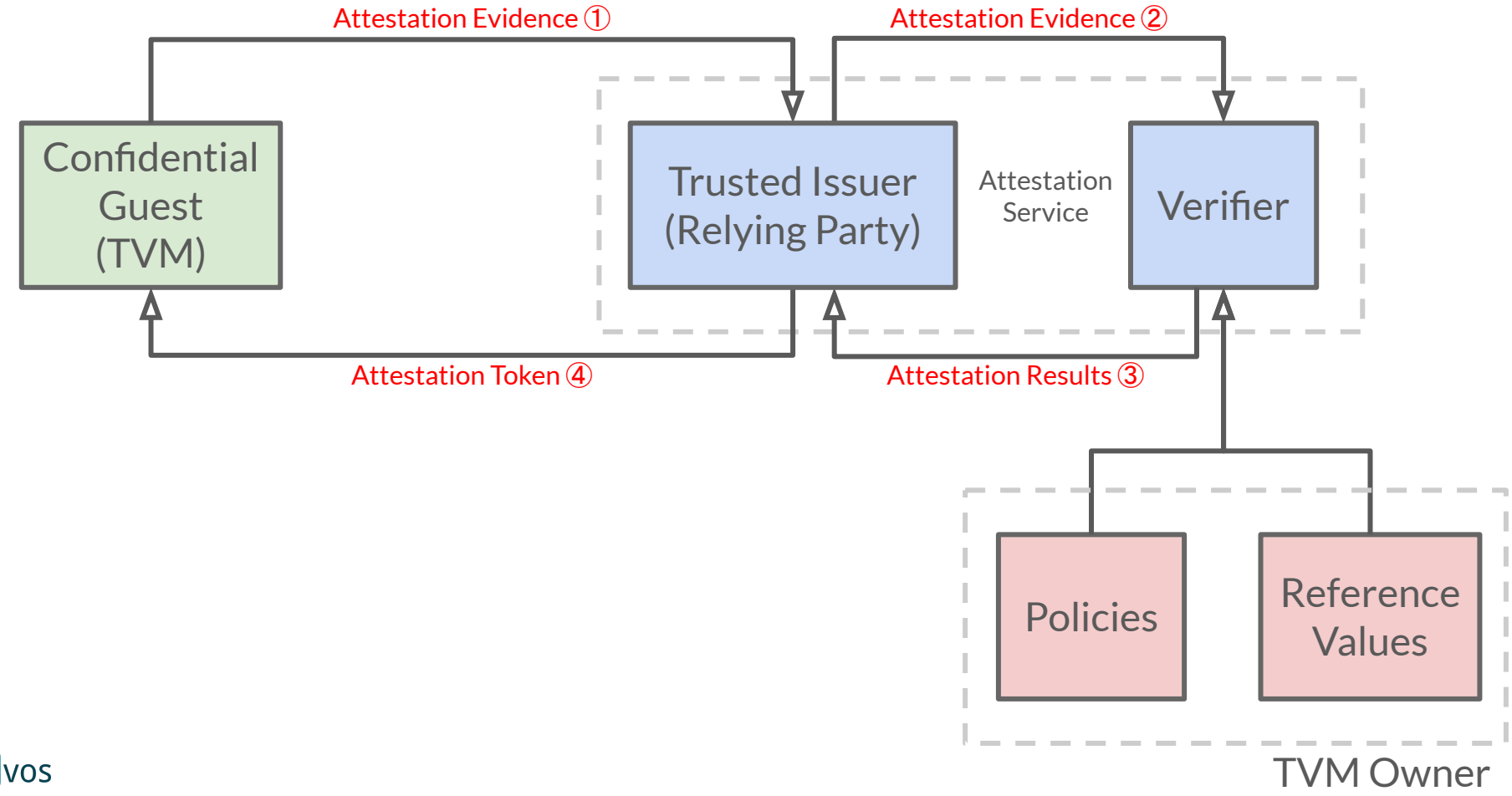

Attestation Evidence ①
Confidential Guest (TVM)
Trusted Issuer (Relying Party)

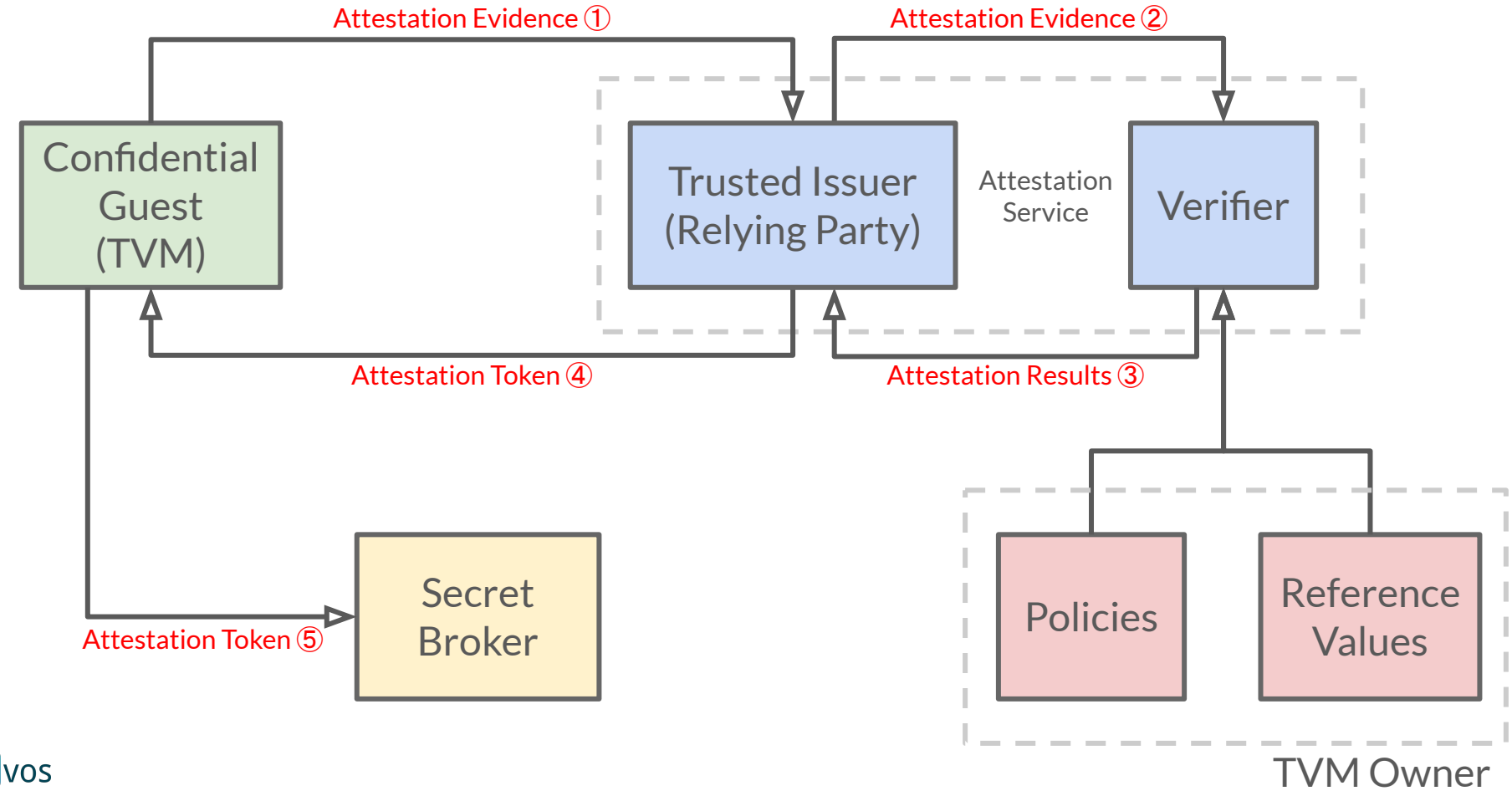

Attestation Evidence ①
Attestation Evidence ②
Confidential Guest (TVM)
Trusted Issuer (Relying Party)
Verifier

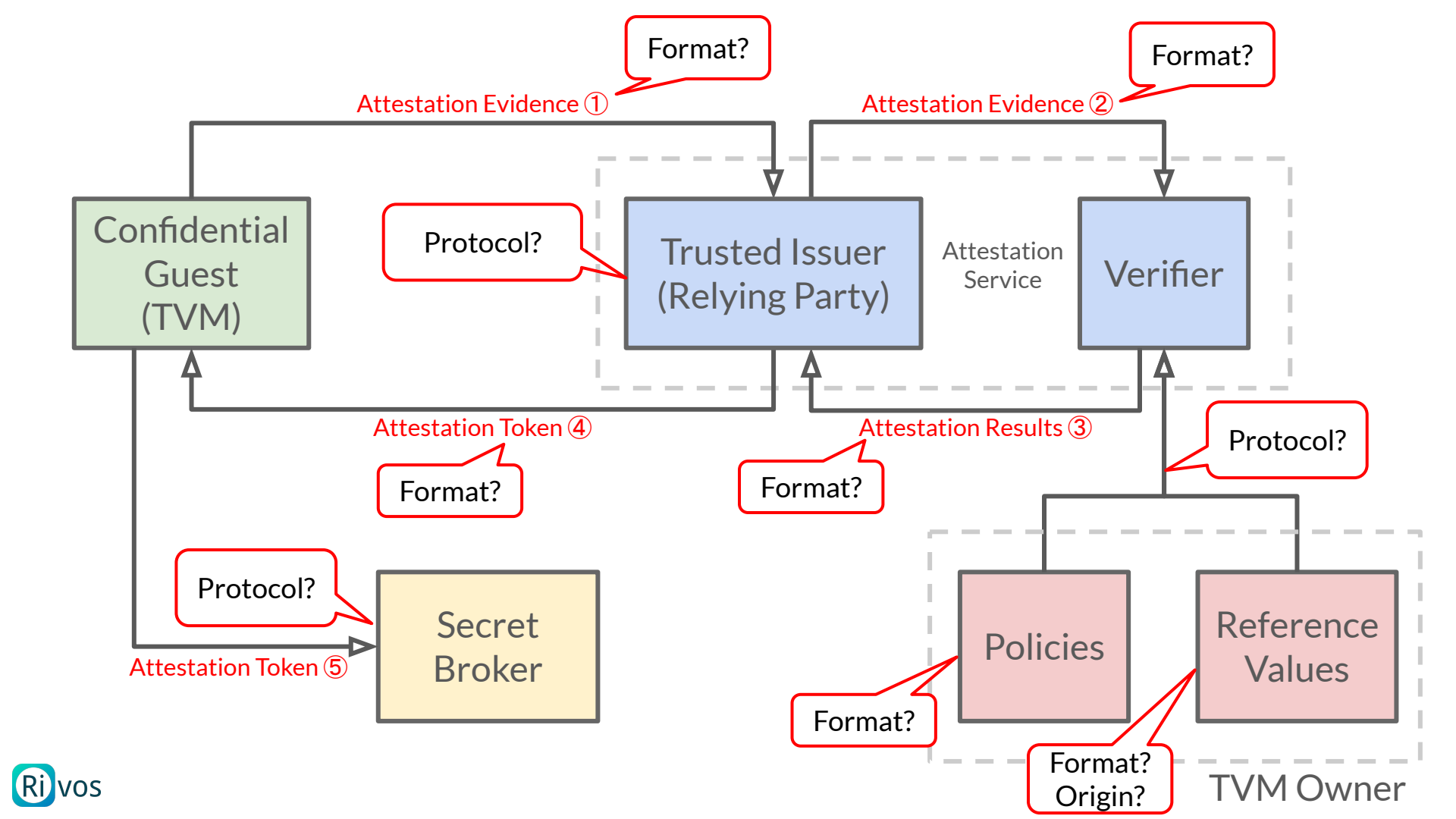

Attestation Evidence ①
Attestation Evidence ②
Confidential Guest (TVM)
Trusted Issuer (Relying Party)
Attestation Service
Verifier


Attestation Evidence ①
Attestation Evidence ②
Confidential Guest (TVM)
Trusted Issuer (Relying Party)
Attestation Service
Verifier
Attestation Results ③


Attestation Evidence ①
Attestation Evidence ②
Confidential Guest (TVM)
Trusted Issuer (Relying Party)
Attestation Service
Verifier
Attestation Token ④
Attestation Results ③

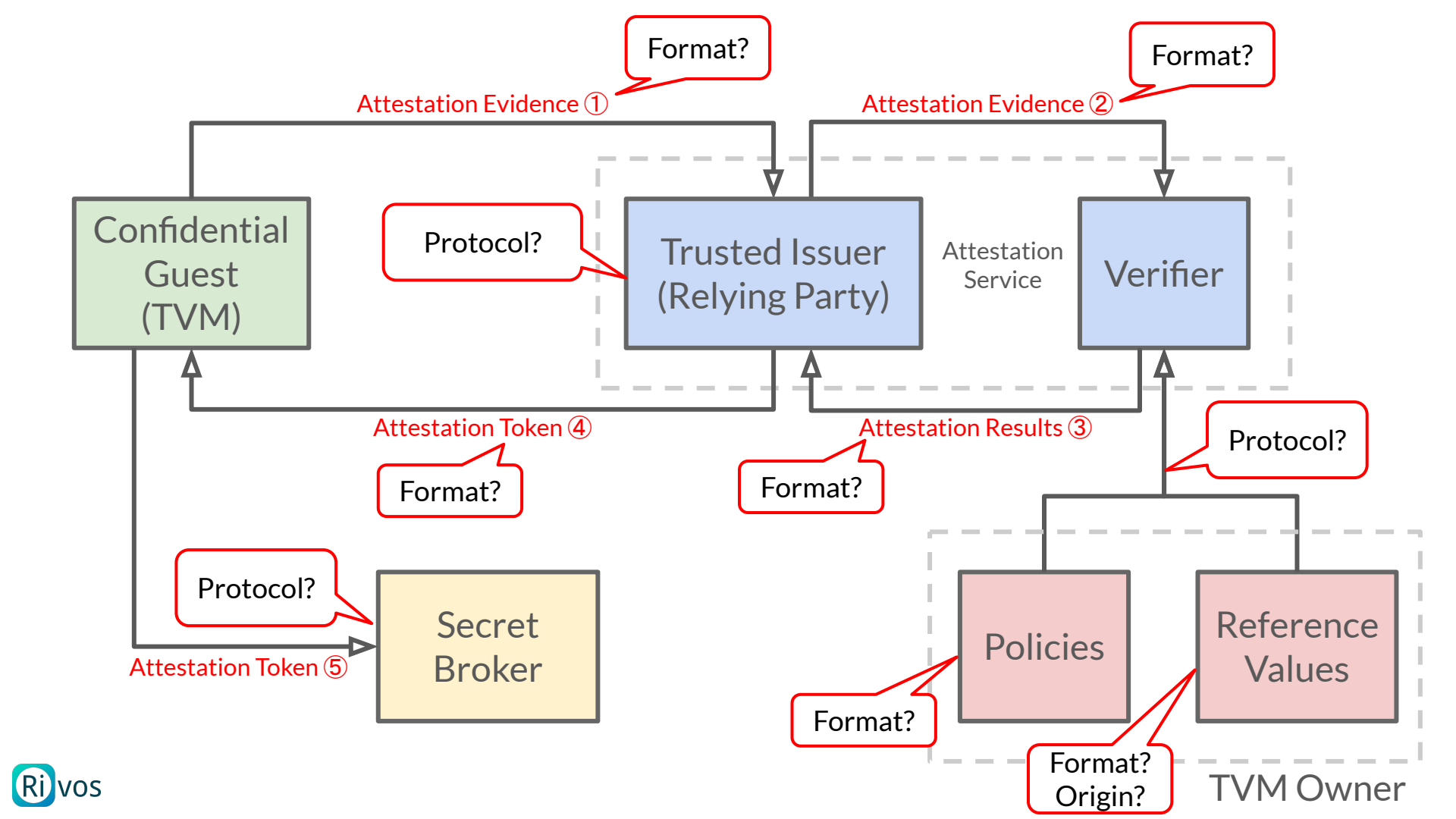

Attestation Evidence ①
Attestation Evidence ②
Confidential Guest (TVM)
Trusted Issuer (Relying Party)
Attestation Service
Verifier
Attestation Token ④
Attestation Results ③
Policies
Reference Values
TVM Owner

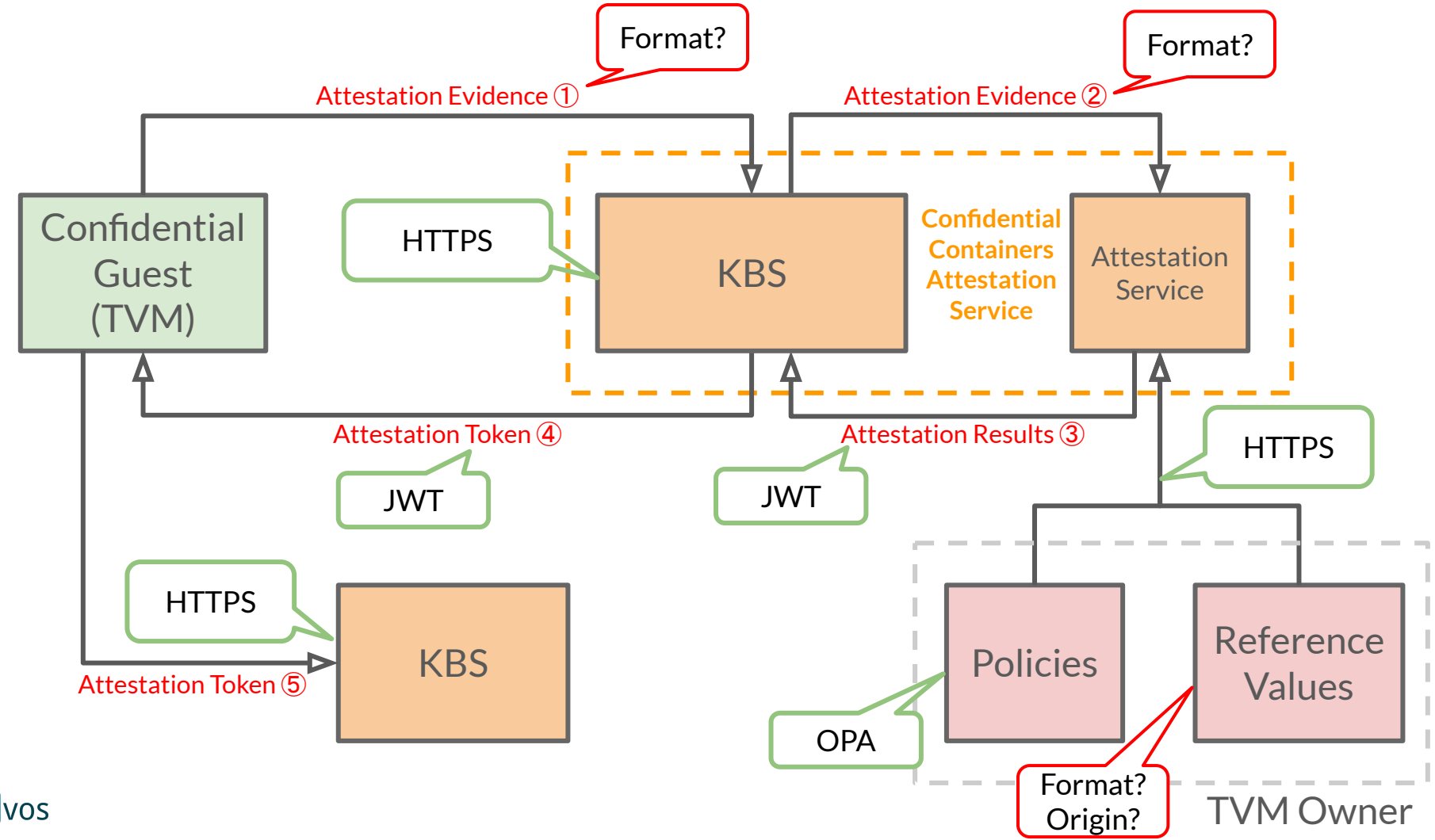

Attestation Evidence ①
Attestation Evidence ②
Confidential Guest (TVM)
Trusted Issuer (Relying Party)
Attestation Service
Verifier
Attestation Token ④
Attestation Results ③
Attestation Token ⑤
Secret Broker
Policies
Reference Values
TVM Owner


Format?
Attestation Evidence ①
Format?
Attestation Evidence ②
Confidential Guest (TVM)
Protocol?
Trusted Issuer (Relying Party)
Attestation Service
Verifier
Attestation Token ④
Format?
Attestation Results ③
Format?
Protocol?
Protocol?
Secret Broker
Attestation Token ⑤
Policies
Reference Values
Format?
Format? Origin?
TVM Owner
Rivos

Confidential Containers Attestation Service

- Complete open source attestation service
- Architecture agnostic
  - Support for all major attestation evidence formats (TDX, SEV, CCA, SGX, Azure, CSV)
  - Supports external verifiers (Intel Amber)
- Open formats and protocols
- https://github.com/confidential-containers/kbs


Format?
Attestation Evidence ①
Format?
Attestation Evidence ②
Confidential Guest (TVM)
Protocol?
Trusted Issuer (Relying Party)
Attestation Service
Verifier
Attestation Token ④
Format?
Attestation Results ③
Format?
Protocol?
Protocol?
Secret Broker
Attestation Token ⑤
Policies
Reference Values
Format?
Format? Origin?
TVM Owner
Rivos


Format?
Attestation Evidence ①
Format?
Attestation Evidence ②
Confidential Guest (TVM)
HTTPS
KBS
Confidential Containers Attestation Service
Attestation Service
Attestation Token ④
JWT
Attestation Results ③
JWT
HTTPS
HTTPS
KBS
Attestation Token ⑤
Policies
Reference Values
OPA
Format? Origin?
TVM Owner

Attestation Evidence Format

- tsm-configfs to converge userspace ABI
- Actual evidence format is still architecture specific
- Entity Attestation Token
  - Content is arch specific, format is standard
  - Please use that!
  - ARM CCA and RISC-V

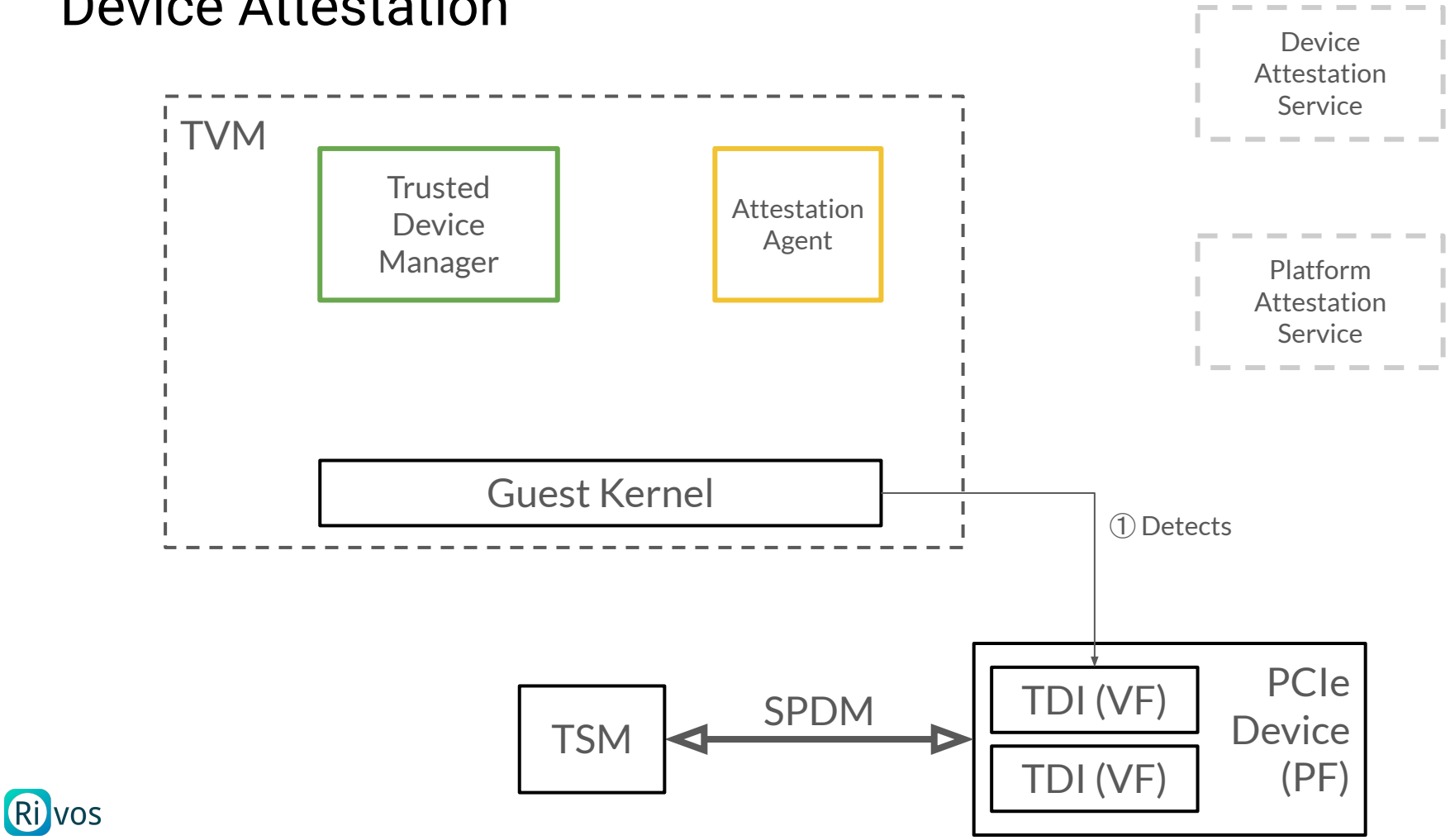
Reference Values

- IETF CoRIM for the format
- Link between supply chain and reference value provider

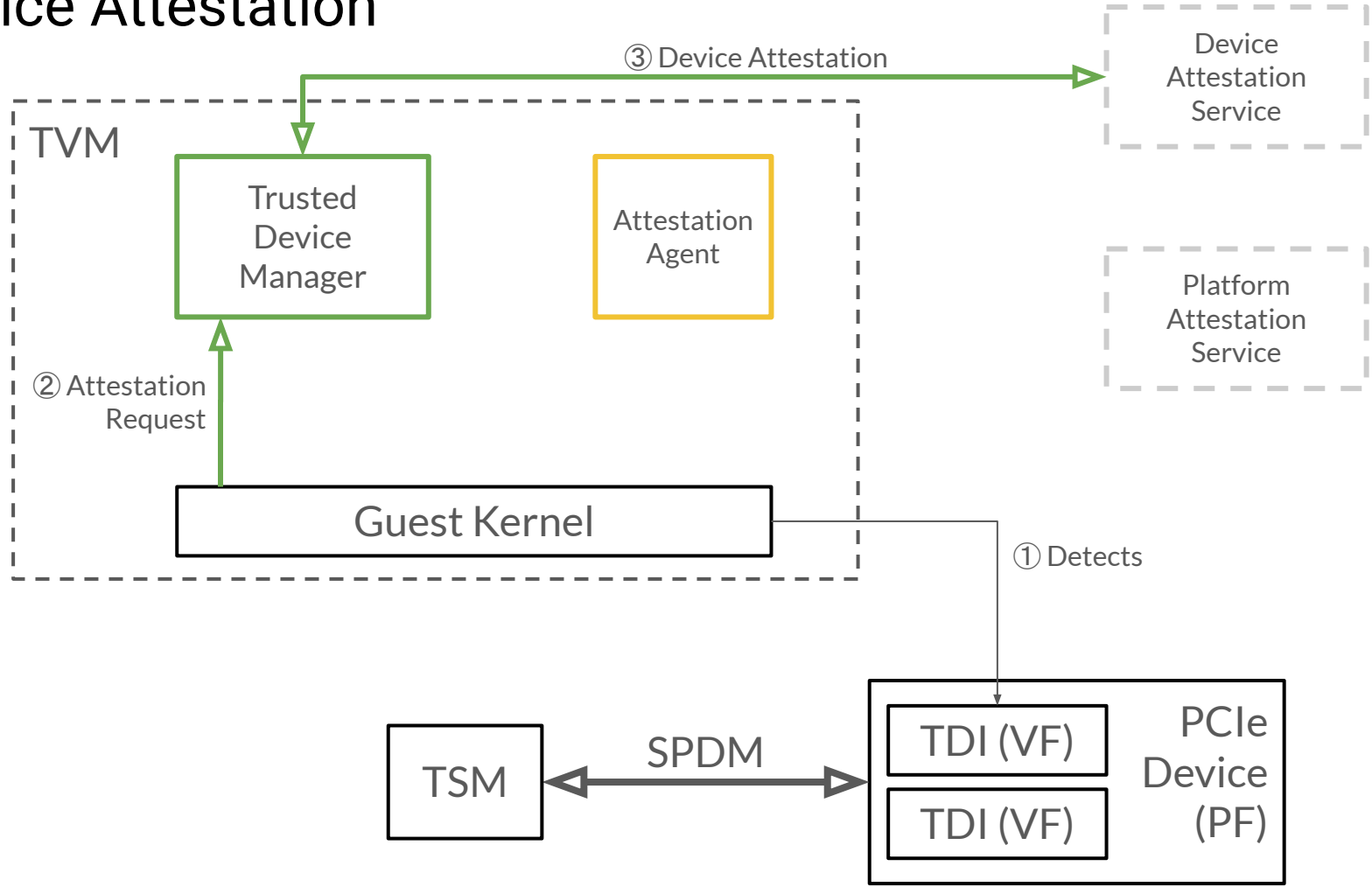
Device Attestation

- TVM must attest a device before accepting it
  - Kernel to offload device attestation to the Trusted Device Manager (TDM)
- Once accepted, the device is part of the TCB
  - Combined attestation: TVM attestation must include device attestation results

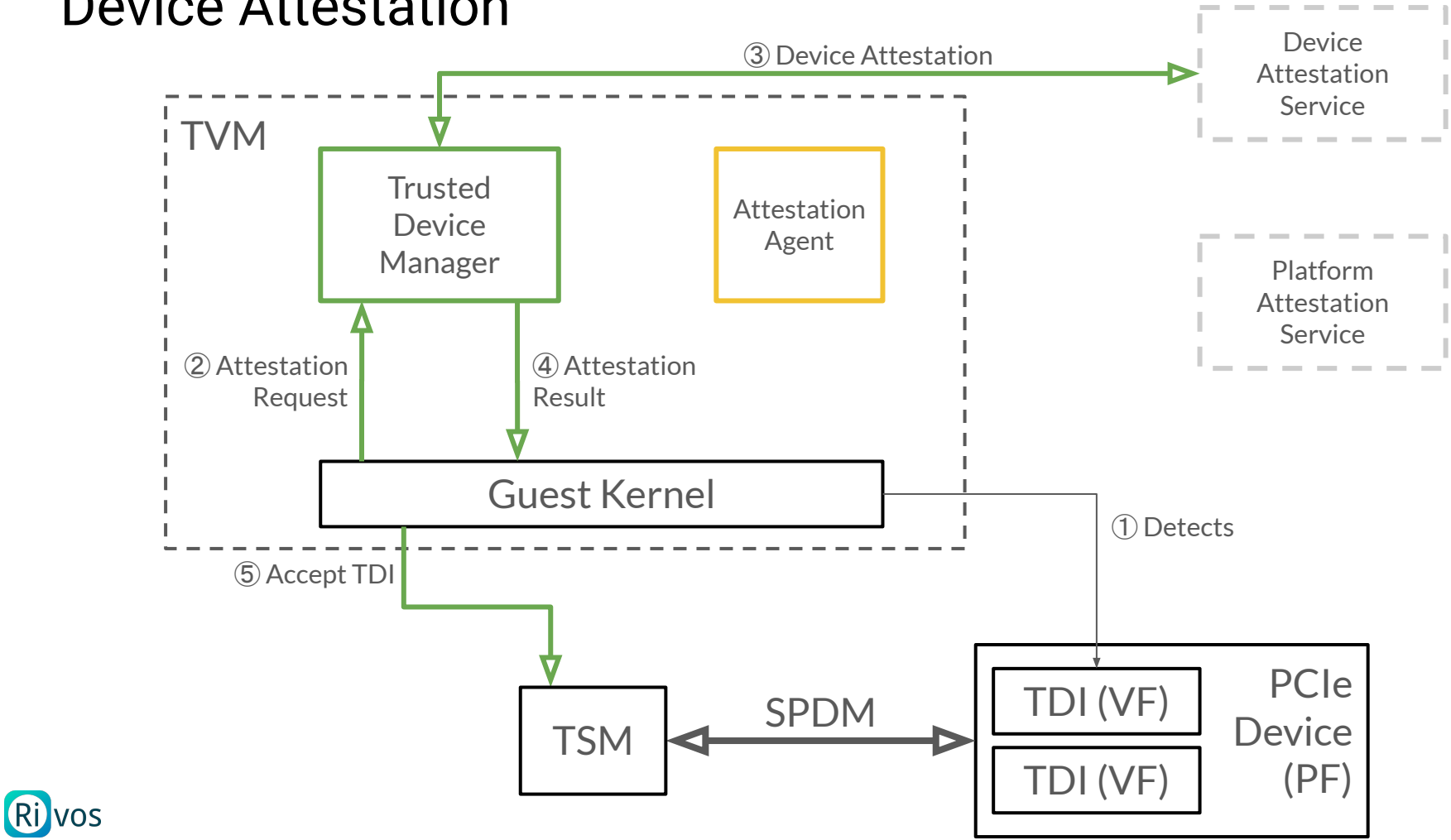
Device Attestation



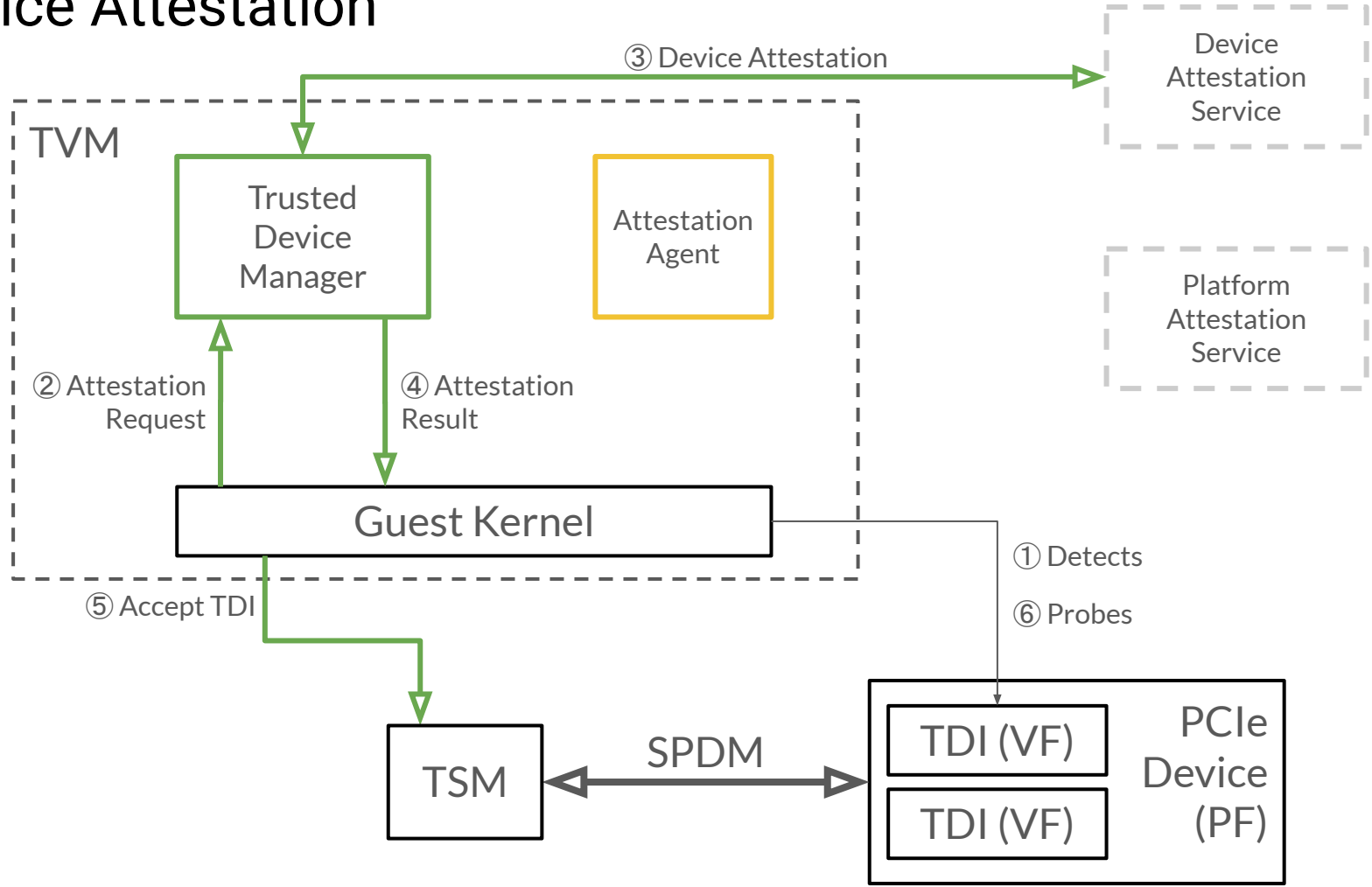
Device Attestation



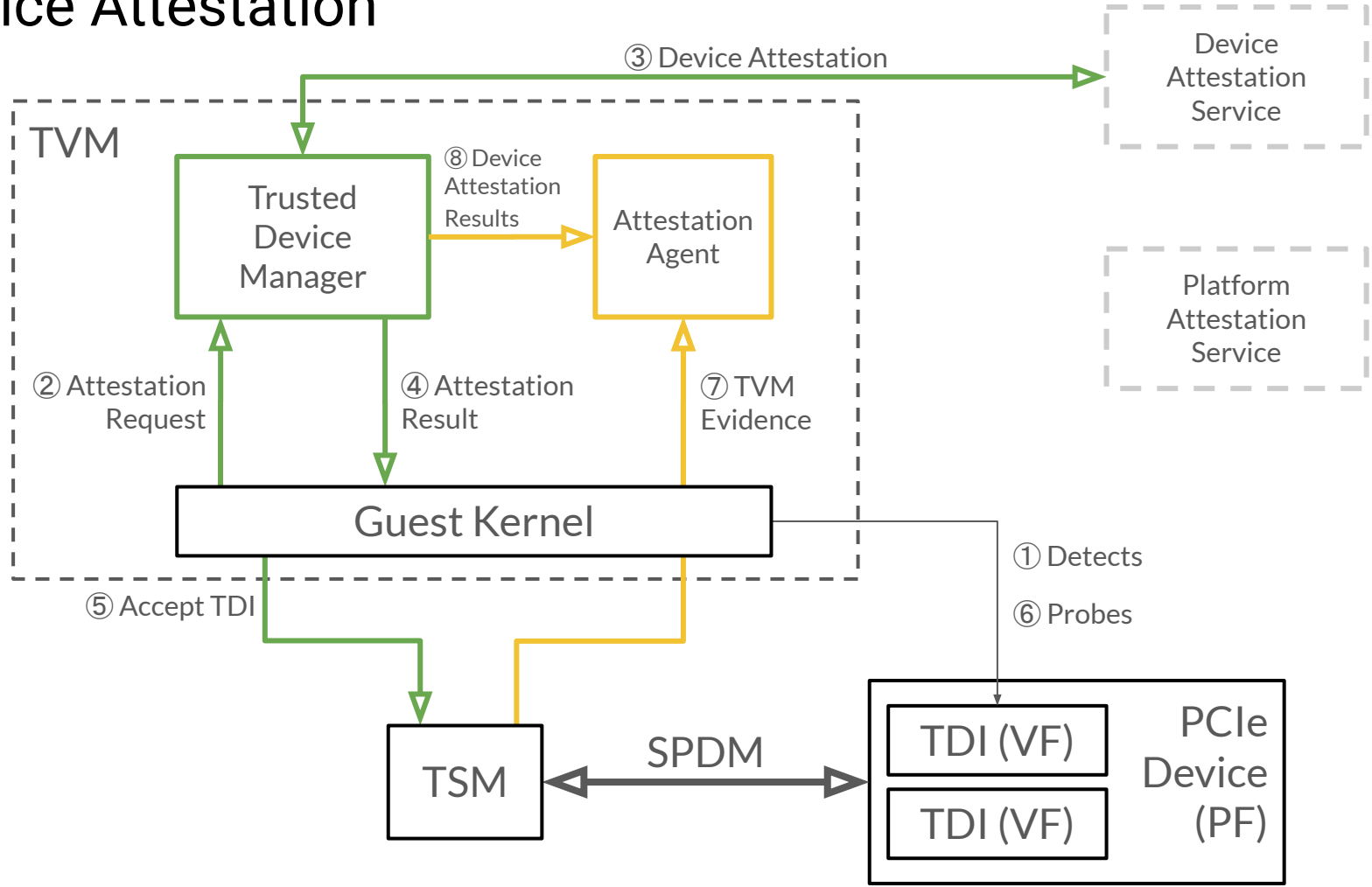
Device Attestation



Device Attestation

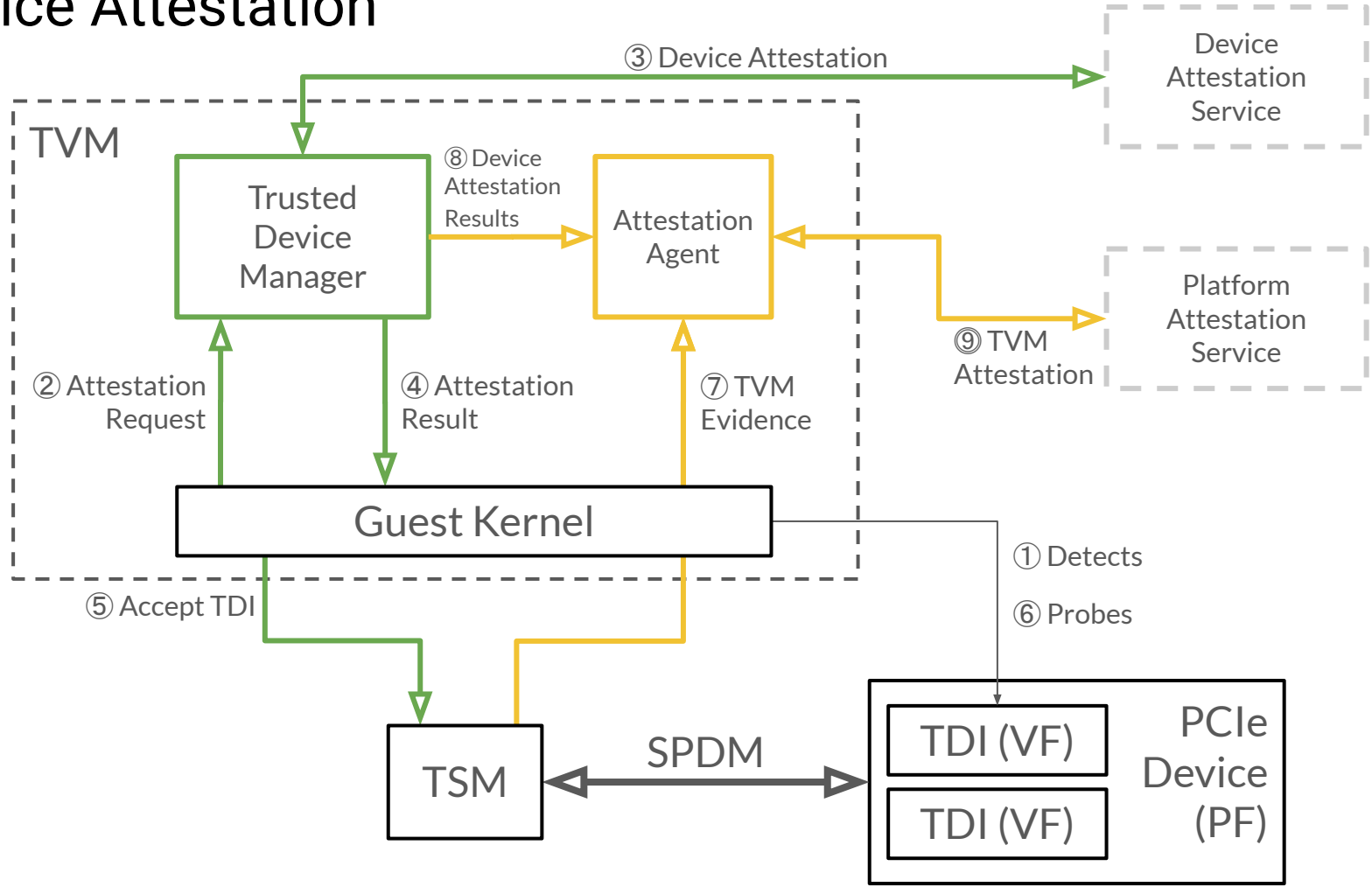


Device Attestation



Rivos

Device Attestation



Rivos