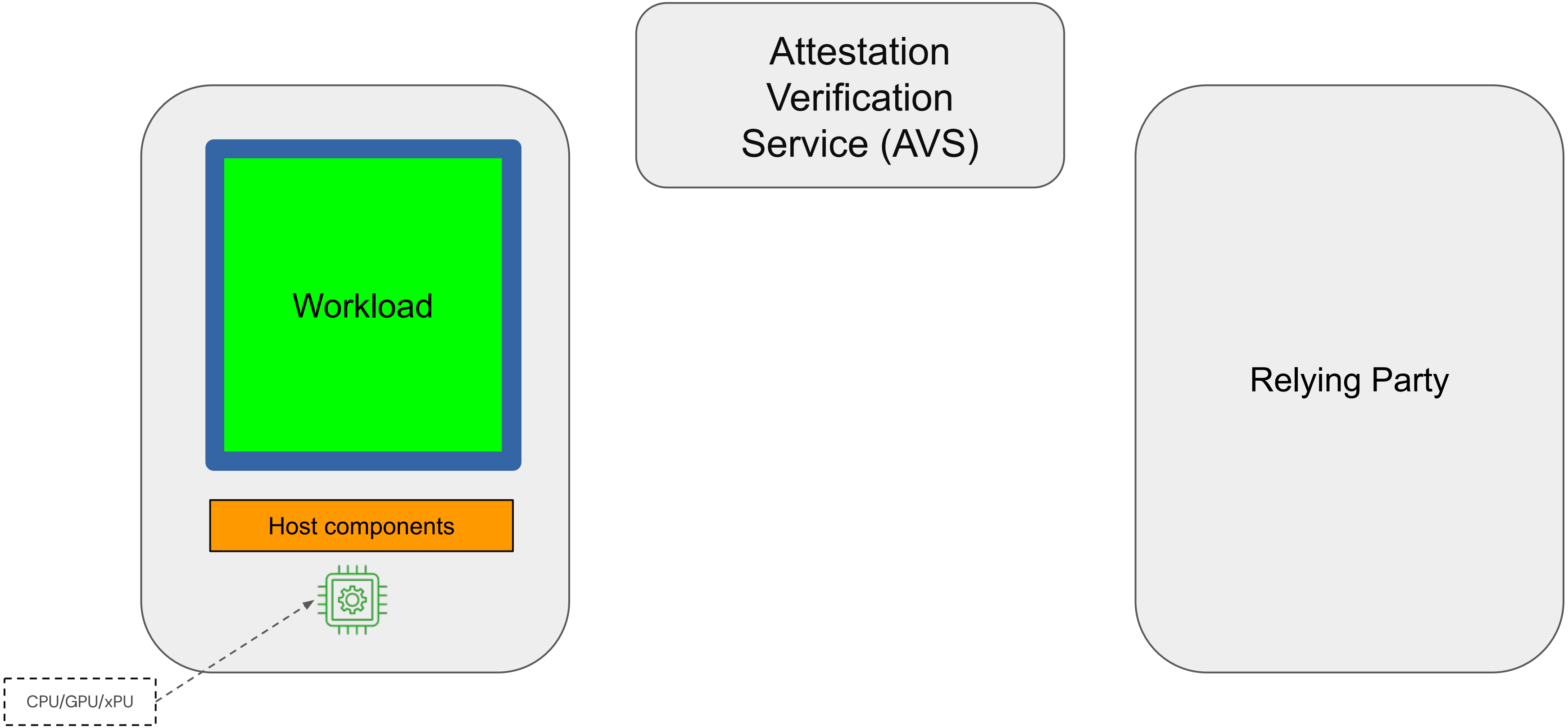
AVS choices

Mike Bursell, Executive Director
Confidential Computing Consortium

CONFIDENTIAL COMPUTING
CONSORTIUM

Components

Basic overview



Attestation Verification Service (AVS)

Workload

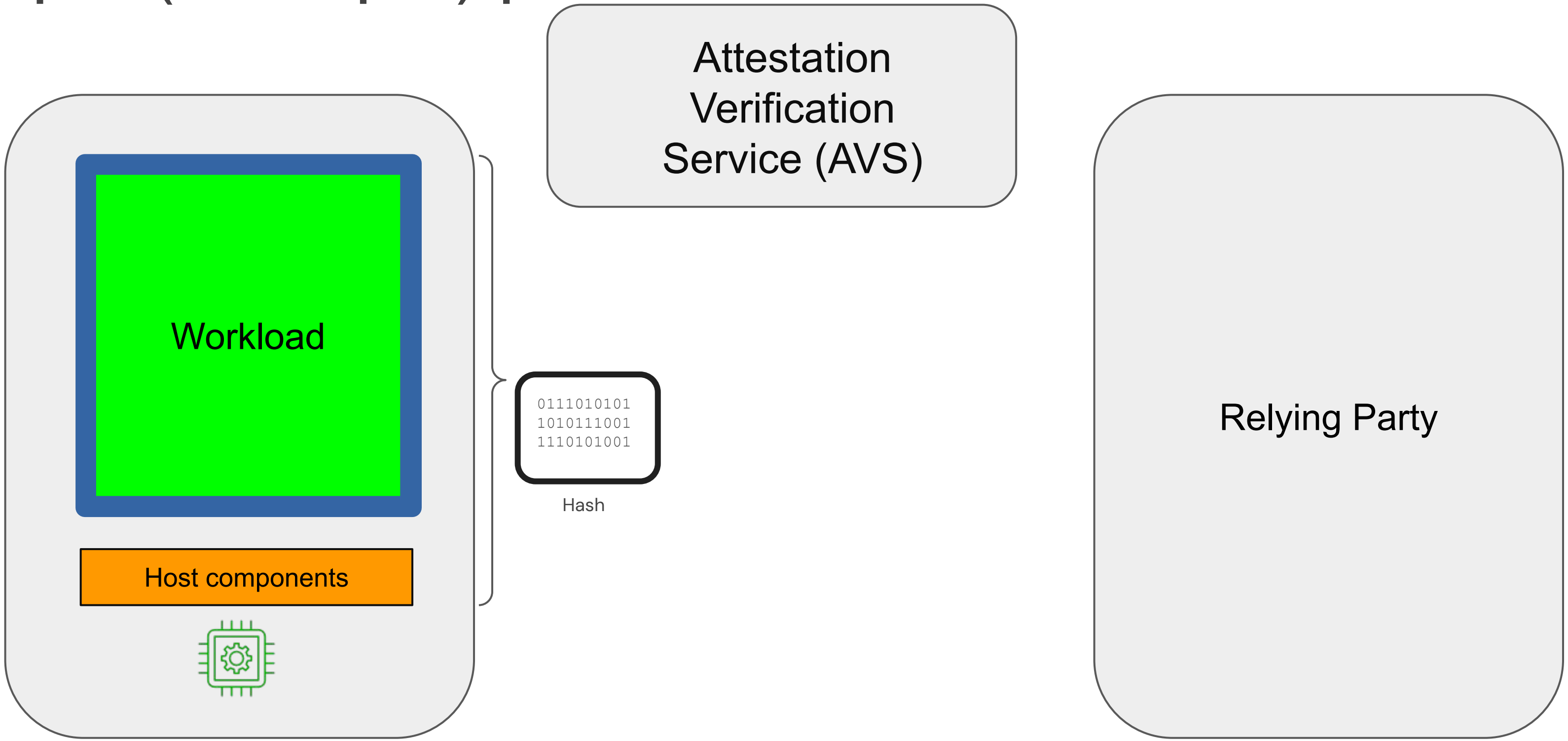
Host components

CPU/GPU/xPU

Relying Party

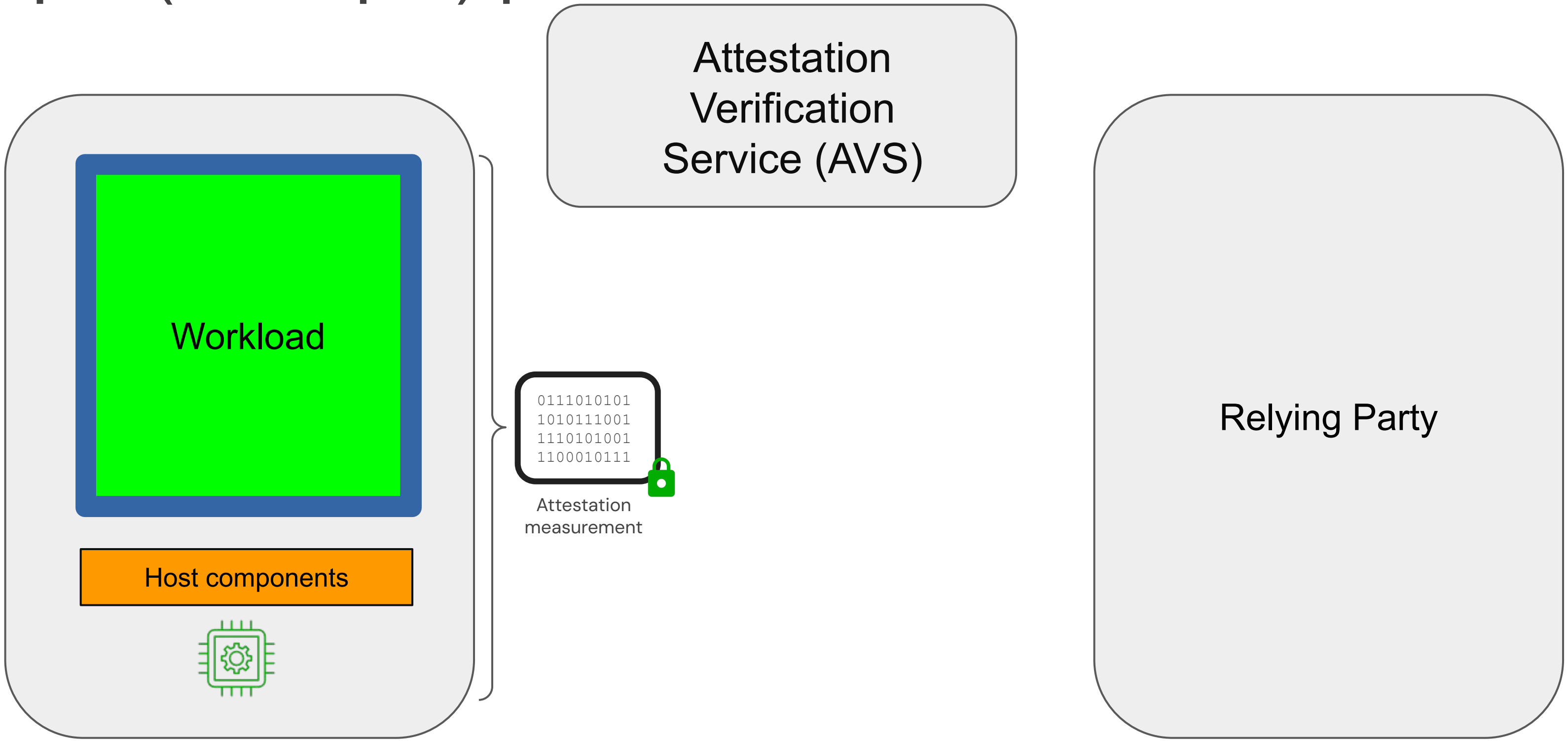
Process

Simple (example) process view



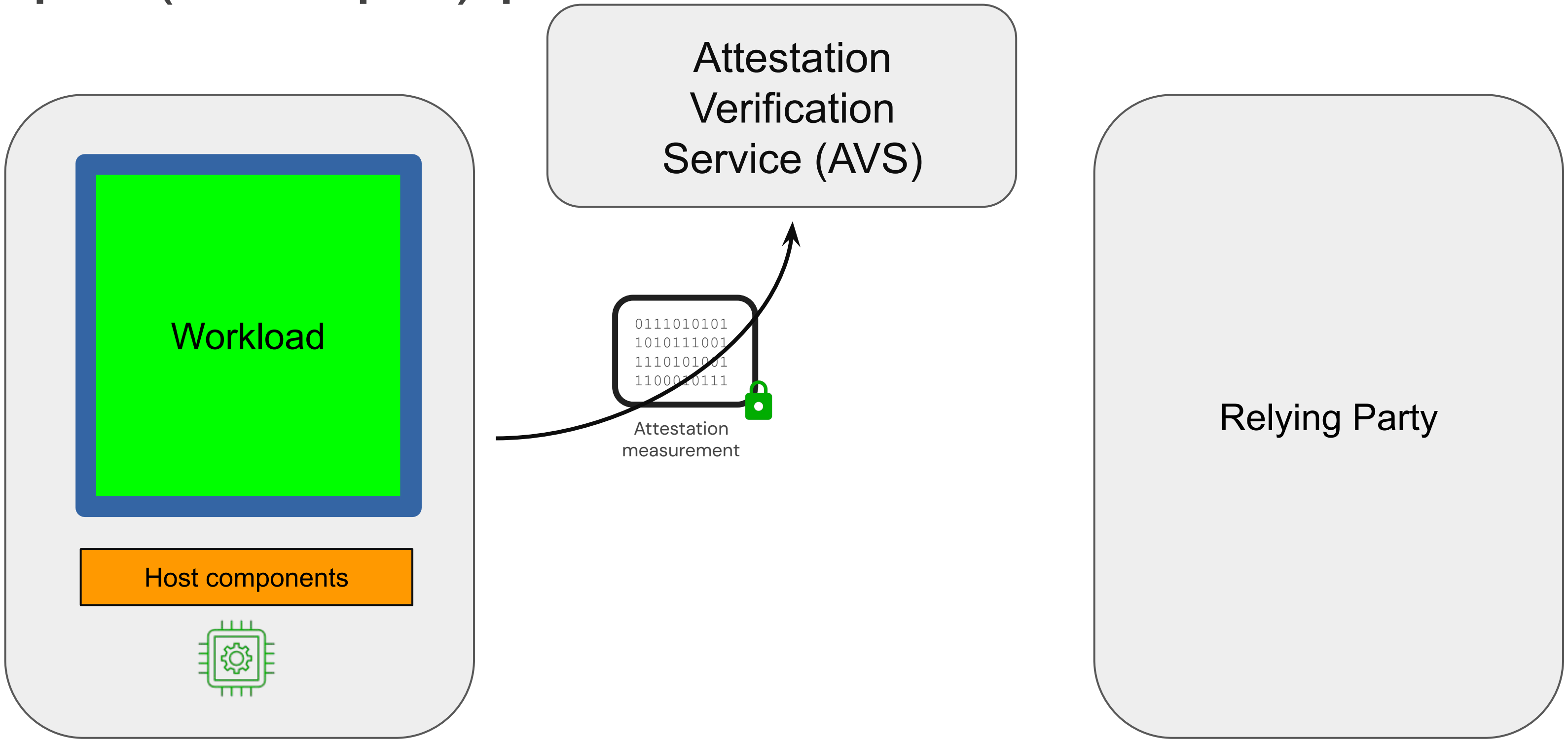
1. CPU creates cryptographic hash of workload and host components

Simple (example) process view



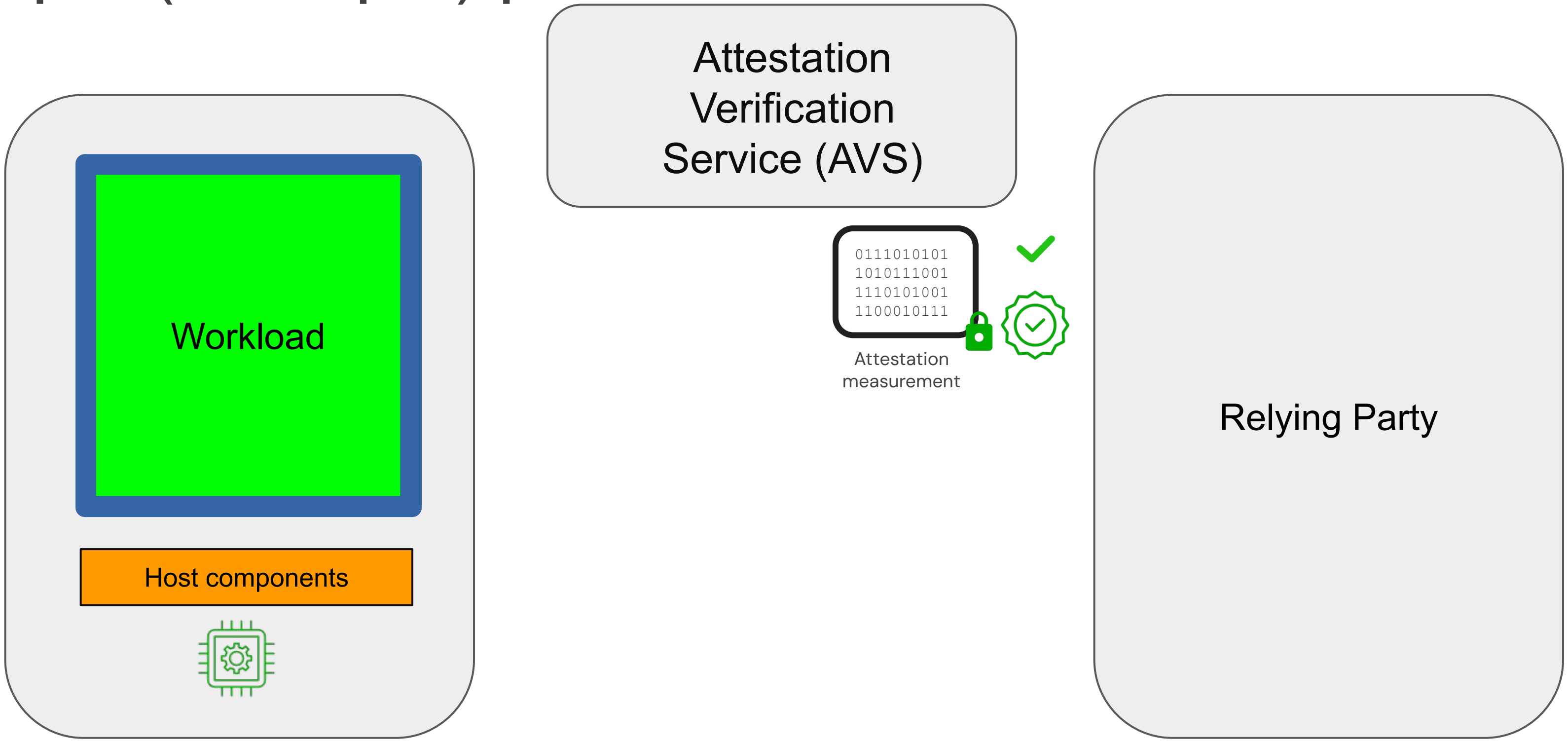
2. CPU combines CPU information with hash, signs all data

Simple (example) process view



3. Attestation measurement sent to AVS

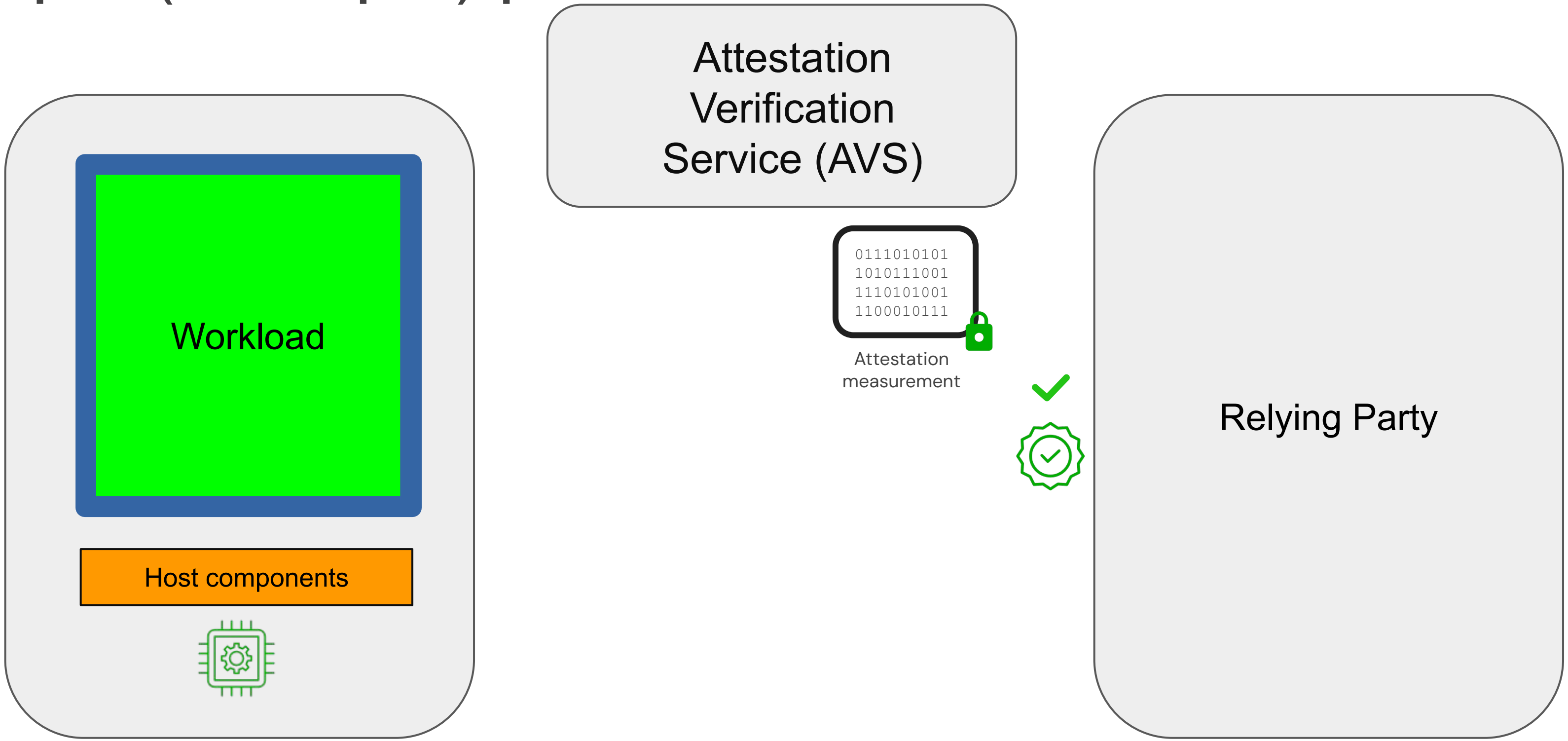
Simple (example) process view



4. AVS verifies Attestation measurement
4a. AVS optionally creates certificate

CONFIDENTIAL COMPUTING
CONSORTIUM

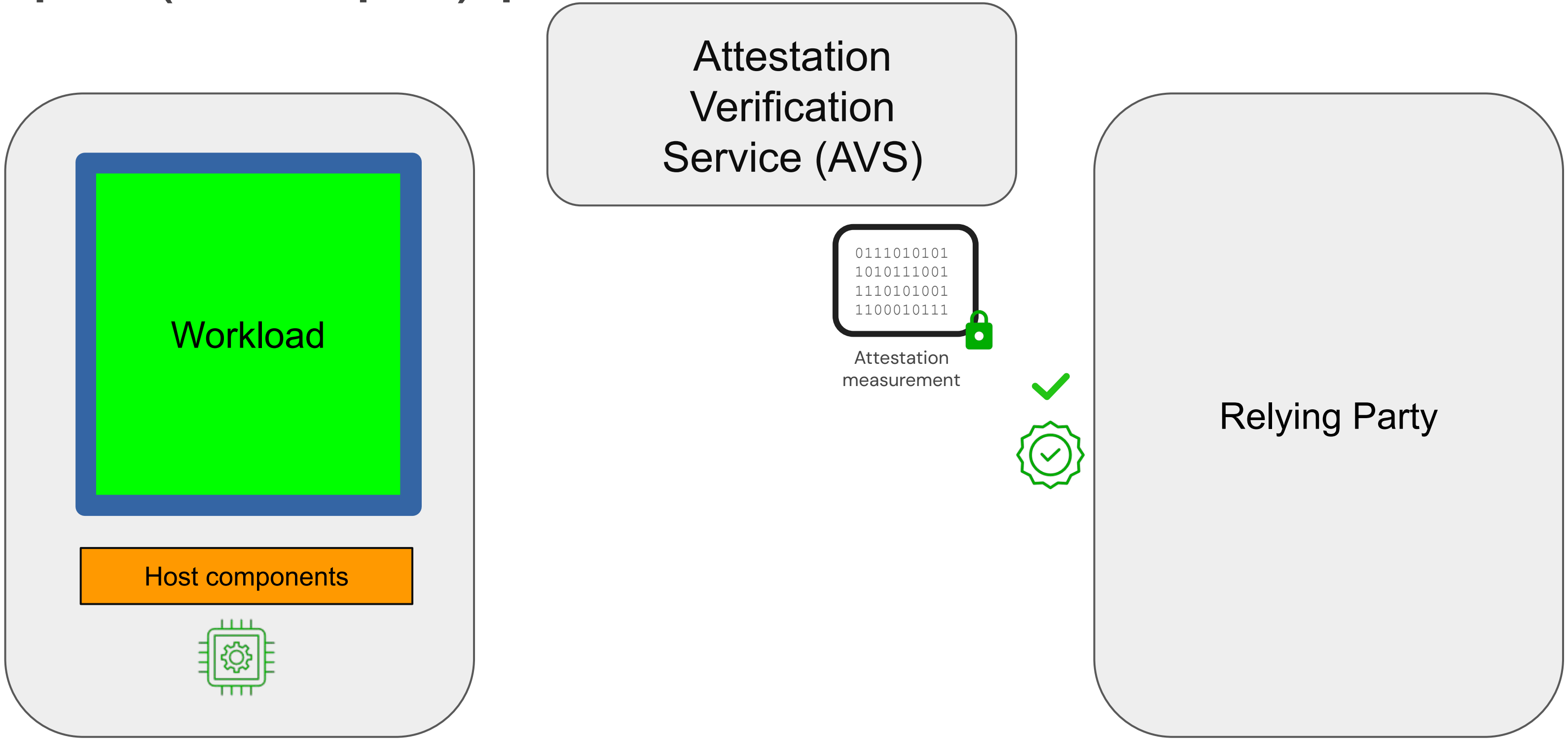
Simple (example) process view



5. AVS sends verification result (and optional certificate) to Relying Party
5a. AVS optionally sends Attestation measurement to Relying Party

CONFIDENTIAL COMPUTING CONSORTIUM

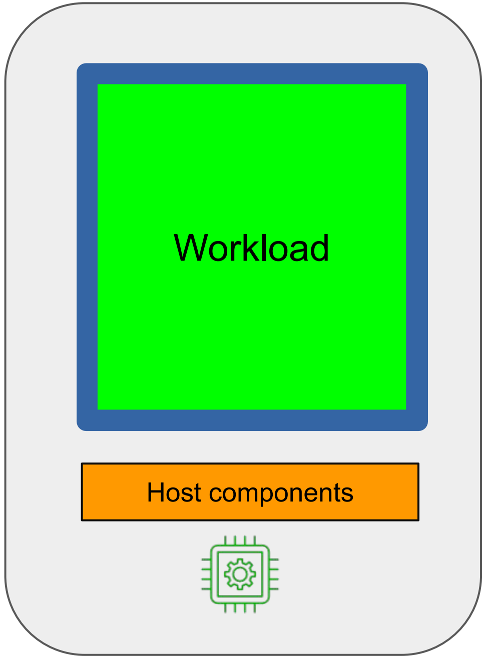
Simple (example) process view



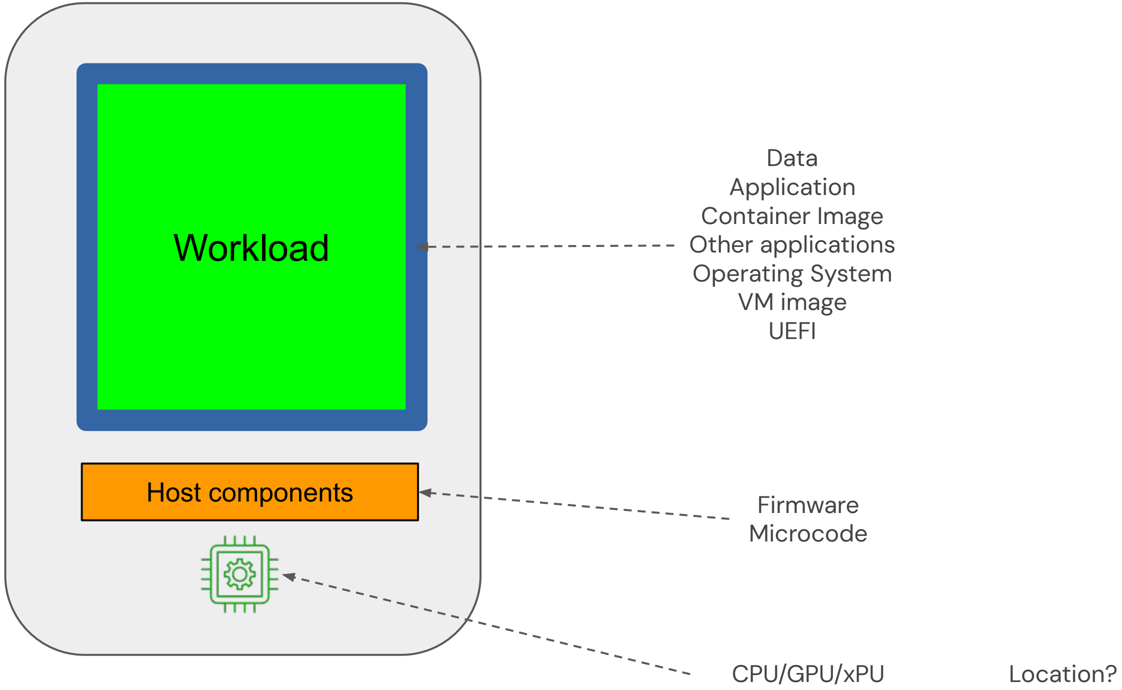
6. Relying Party happy with AVS result, workload considered “good”.

Host-side components

Host-side components

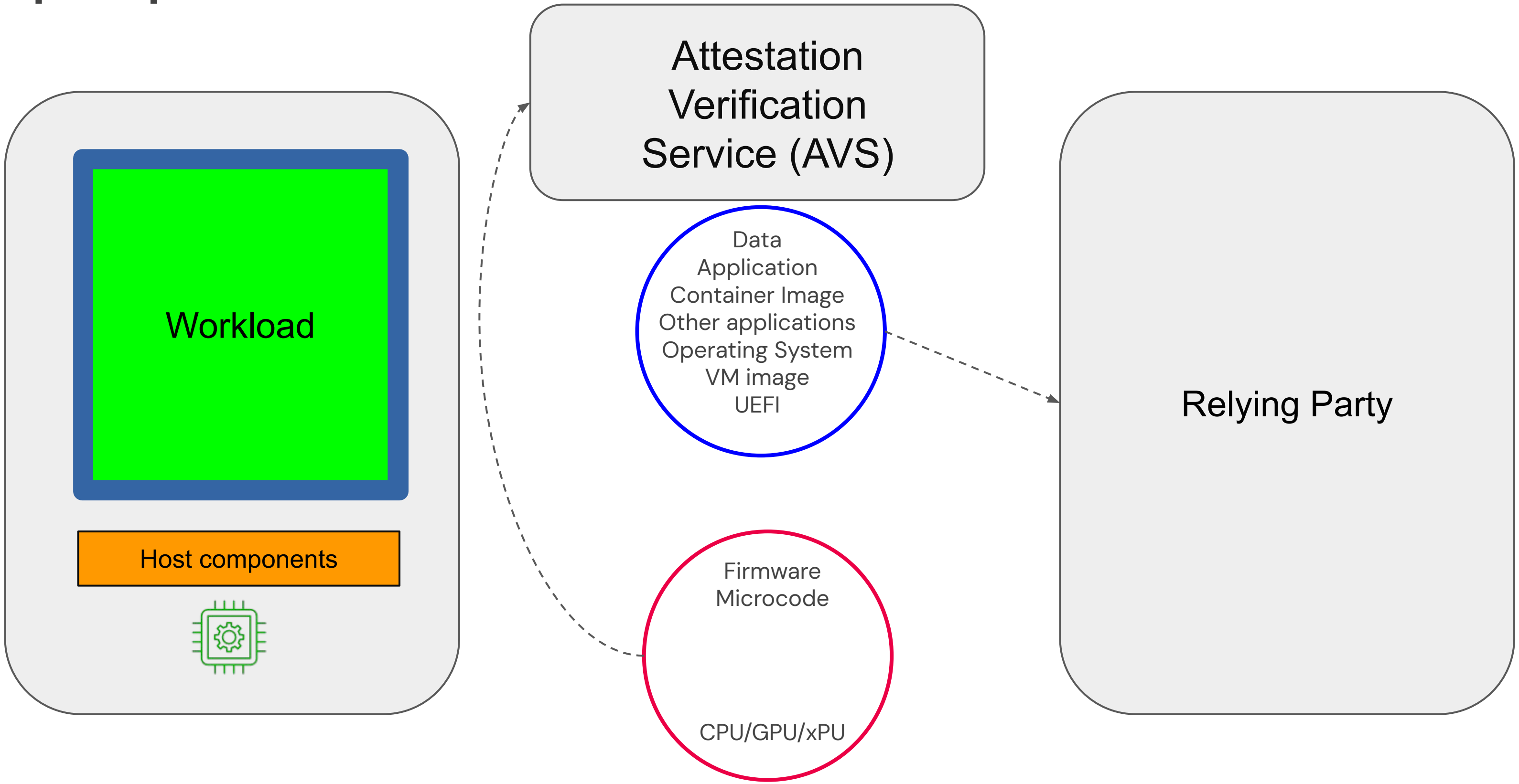


Host-side components



Which parties hold verification criteria?

Simple process view



Verification criteria

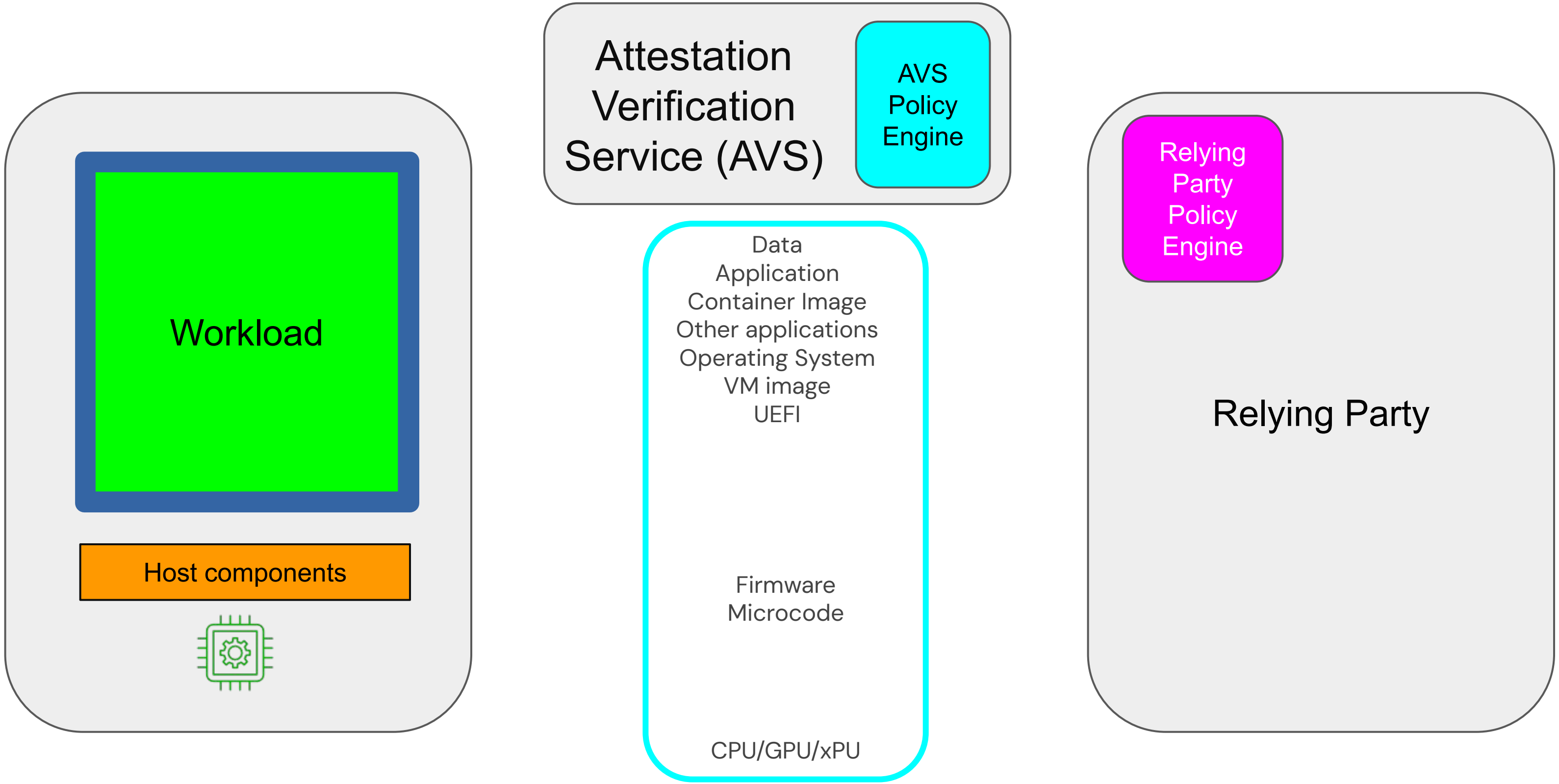
Relying Party specific	Data Application
May be shared between some Relying Parties	Container Image Other applications? Operating System VM Image UEFI?
Shared across multiple Relying Parties	UEFI? Firmware Microcode CPU/GPU/xPU

Policy application

- Relying party should **always** control policy for all components
  - The more granular the policy, the better
- Relying party may choose to delegate policy for some or all components or parts thereof
- Certificate signing significantly simplified if performed once
  - Much easier if policy is applied by one entity

Where is policy applied?

Policy option 1 - all policy applied at AVS



Attestation Verification Service (AVS)

AVS Policy Engine

Workload

Host components

Data
Application
Container Image
Other applications
Operating System
VM image
UEFI

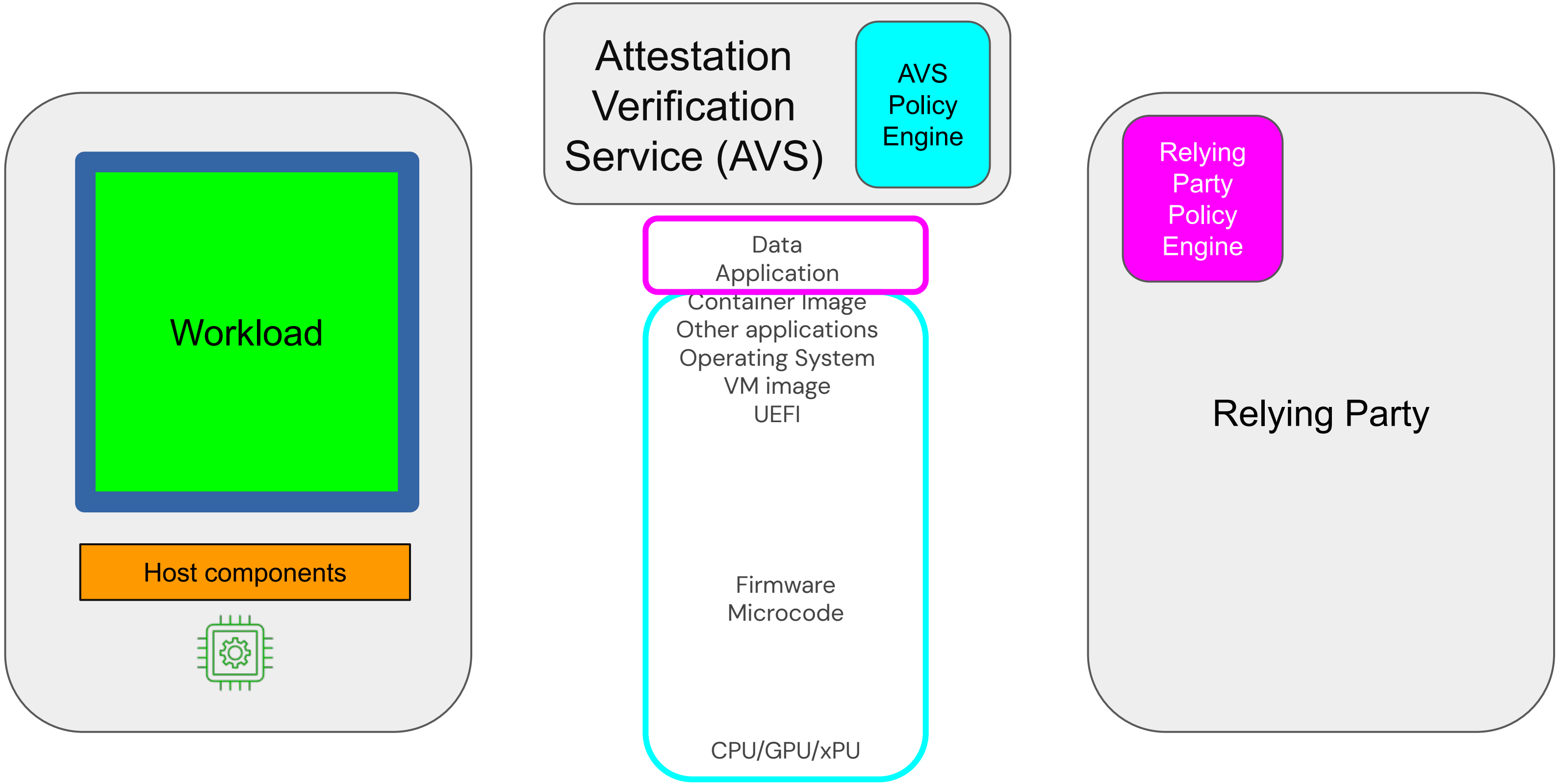
Firmware
Microcode

CPU/GPU/xPU

Relying Party Policy Engine

Relying Party

Policy option 2 - some policy applied by Relying Party



CONFIDENTIAL COMPUTING CONSORTIUM

Policy options

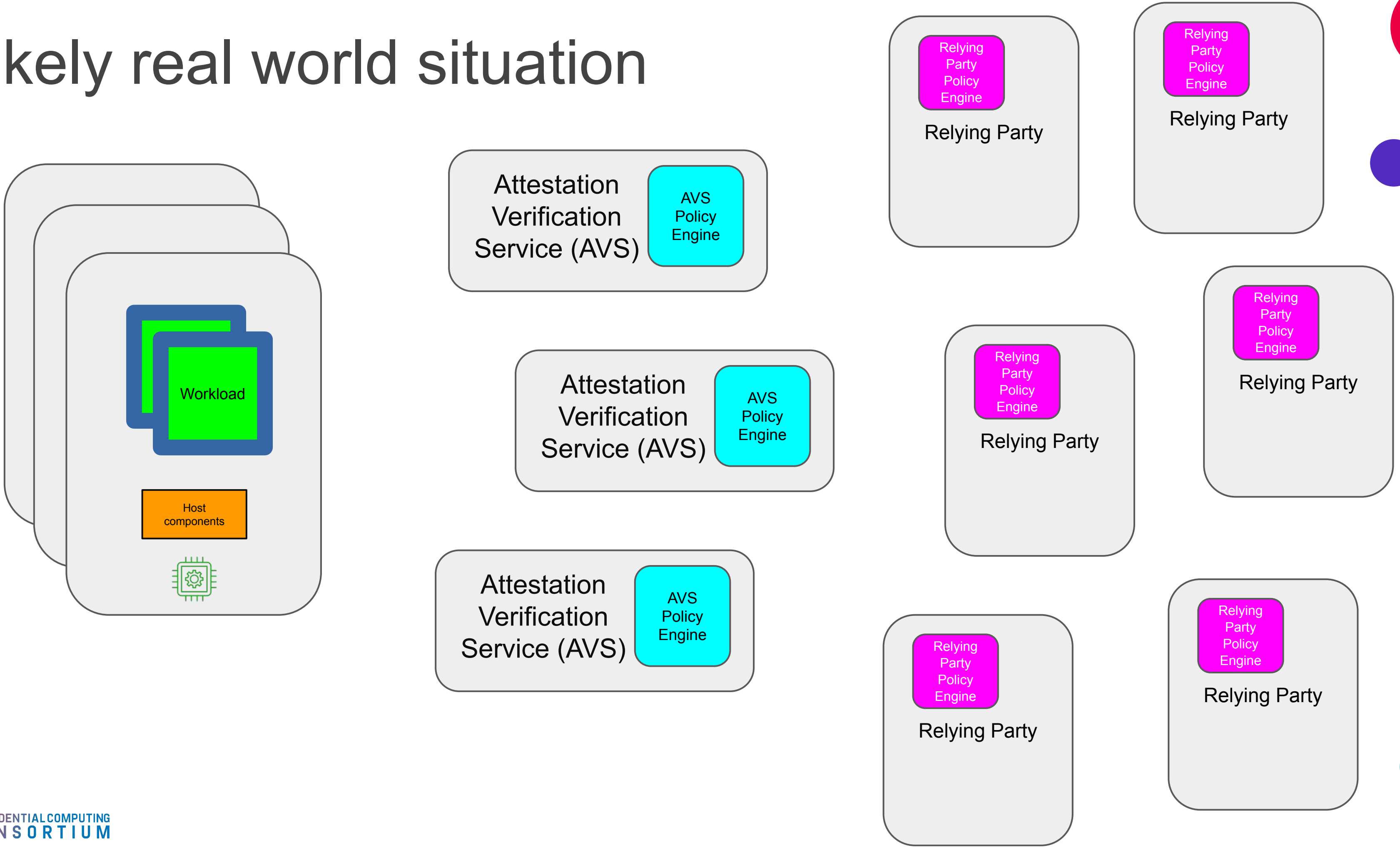
- Other options are possible and plausible
    - E.g. Relying Party owning policy around Container or VM Image
    - **NOTE:** UEFI may be an important policy point for some Relying Parties
    - **NOTE:** Firmware versions may be an important policy point for some Relying Parties
- Location is a possible addition to attestation information
    - No known stable protocol definitions for this
- Other additions?

Reasons for/against policy delegation

For delegation	Against delegation
Speed	Security
Cost of operation if run internally	Cost for verification
Certificate signing in one place	Integration complexity
	Management complexity
	Multiple AVS entities
	Complex trust relationships

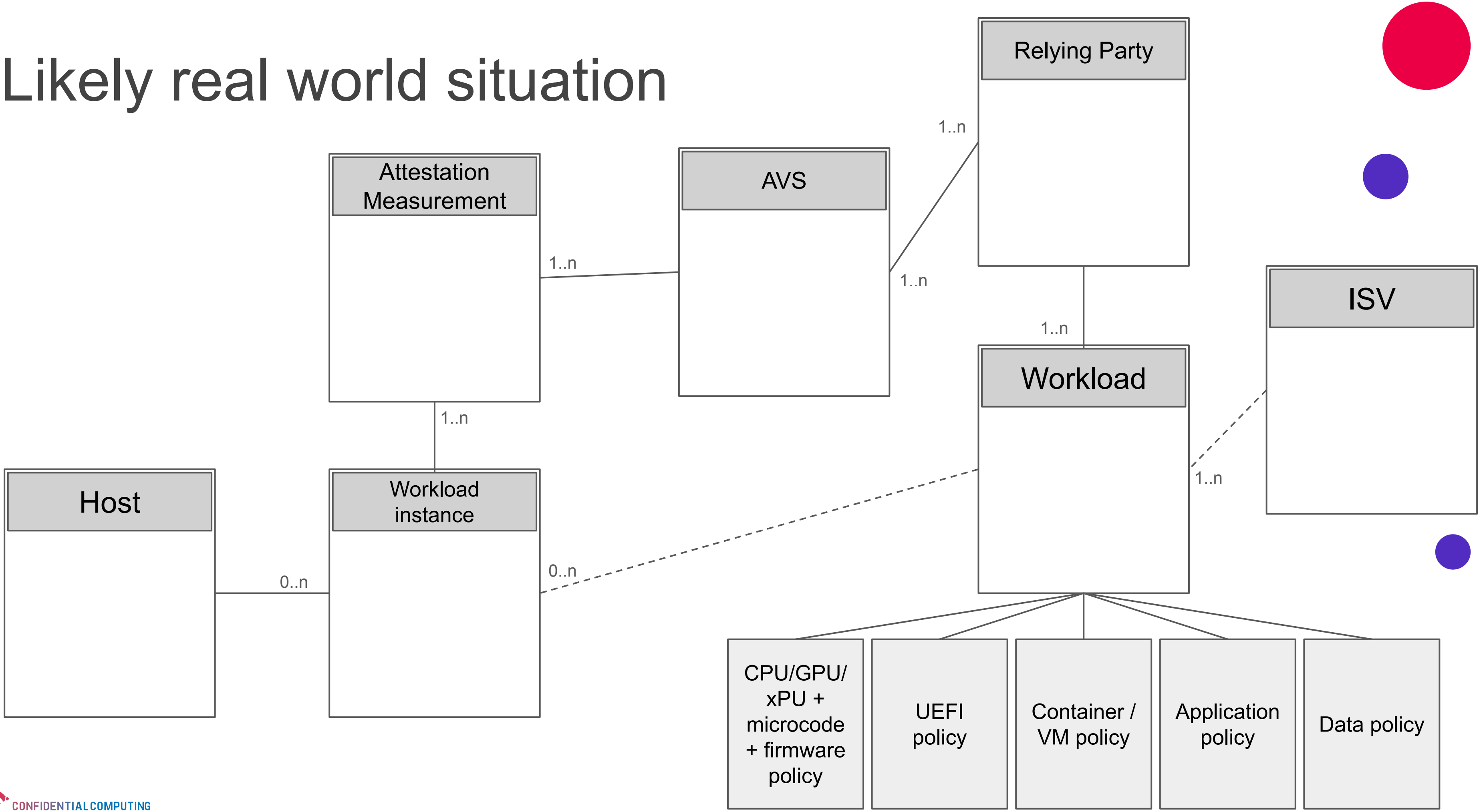
Why does this matter?

Likely real world situation


Workload
Host components
Attestation Verification Service (AVS)
AVS Policy Engine
Attestation Verification Service (AVS)
AVS Policy Engine
Attestation Verification Service (AVS)
AVS Policy Engine
Relying Party Policy Engine
Relying Party
Relying Party Policy Engine
Relying Party
Relying Party Policy Engine
Relying Party
Relying Party Policy Engine
Relying Party
Relying Party Policy Engine
Relying Party
Relying Party Policy Engine
Relying Party

CONFIDENTIAL COMPUTING CONSORTIUM

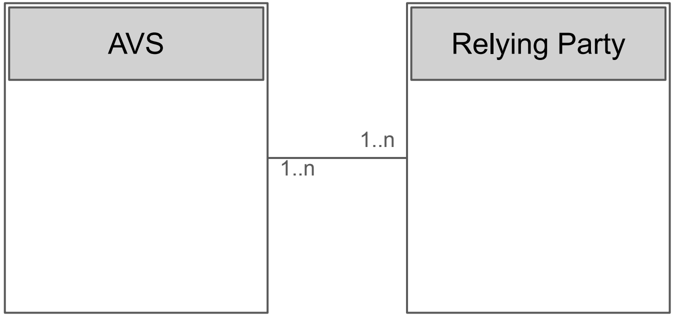
Likely real world situation



CONFIDENTIAL COMPUTING CONSORTIUM

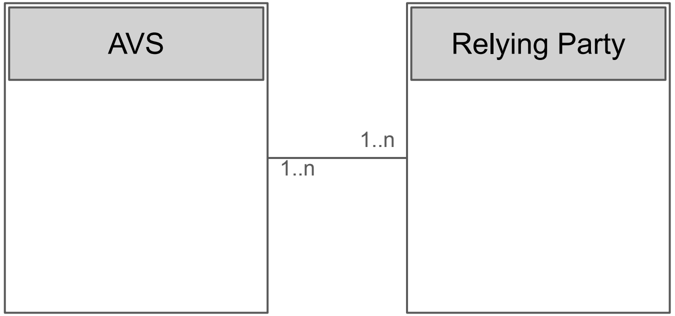
Likely real world situation

- Each Relying Party has multiple workloads
- Each Relying Party uses multiple Attestation Verification Services
- Each Attestation Verification Service is used by multiple Relying Parties



Likely real world situation

- Each Relying Party has multiple workloads
- Each Relying Party uses multiple Attestation Verification Services
- Each Attestation Verification Service is used by multiple Relying Parties



IMPLIES:

Significant management burden for Relying Parties

Other outstanding questions

- Charging model
- Trust establishment from Relying Party to Attestation Verification Services
  - What might be appropriate bodies to run an AVS?
- Policy management standards
- Revocation processes
- ISV’s place in the process
- Service Level Agreement expectations
  - Performance
  - Uptime
  - Fail-over

Possible AVS operators

Org. type	Comments
CSP / system operator	Removes isolation assurance from system; “marking own homework”
ISV (workload creator)	May not be core business; proliferation of AVS instances
Government / regulator	Specific to jurisdiction or sector; strong trust within scope; may not be trusted by others
Not-for-profit	Charging model must be explicit and guaranteed; jurisdiction may affect trust
Silicon vendor	Unlikely to support other vendors; unlikely to support policies?
Integrator	Consolidation of ISVs; likely to be trusted by larger Relying Parties
Certificate Authority	Global; have company-internal options; charging model likely to differ from existing
OEM/OHM	Close to microcode/firmware; unlikely to support other vendors? Unlikely to support higher-level component policies?
Internal	…

CONFIDENTIAL COMPUTING CONSORTIUM

Questions?

ConfidentialComputing.io