Attestation Governance

GRC SIG Update for Attestation SIG
August 29, 2023

What is Governance?

GRC SIG Charter: CCC Governance Risk & Compliance Special Interest Group - Charter.pdf

1. **Articulating the desired state of a system (or, alternatively, forbidden states), as well as specifying the actions to be taken if/when an out-of-policy condition is detected.**
2. Measuring the state of the system (e.g., through monitoring, sampling and/or periodic reviews).
3. Comparing the reported state of the system against the desired state.
4. Taking prescribed actions to bring the system back into compliance if/when an out-of-policy state or condition is detected.
5. Periodically testing effectiveness of Governance by triggering undesirable states and ensuring that the system responds in the expected way (e.g., by detecting and reporting the problem, self-correcting violations and/or terminating offending workloads).
6. In all steps above, documenting ("evidencing") all pertinent information and storing the evidence in a protected repository for a period of time required by the regulators.
7. Presenting the evidence from the previous steps to regulators, periodically and/or on-demand.

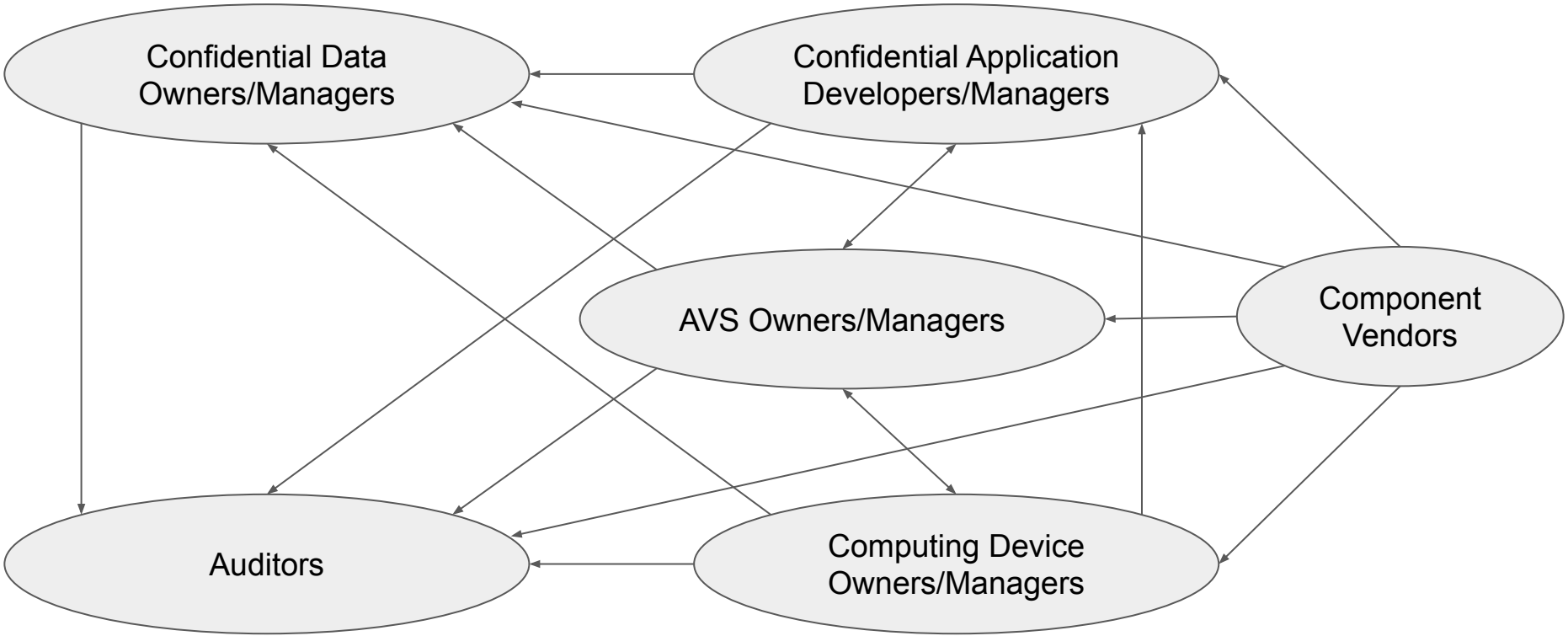
Current "Attestation Governance Patterns" document: Attestation Governance Patterns

The goal is to build patterns on top of Confidential Computing attestation mechanisms

Desired Properties of Attestation Governance Patterns

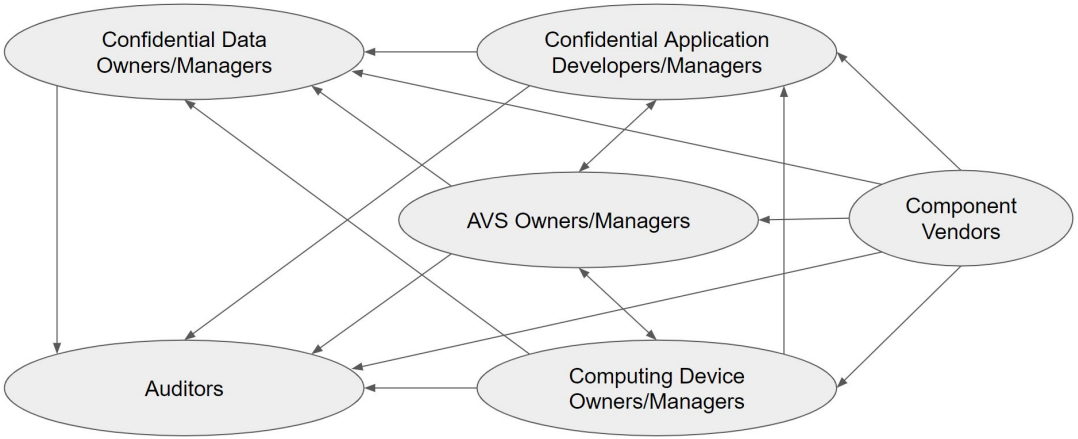
- Paving way to clearly documented expectations and reusable solutions
- Technology agnostic
  - TDX/SEV/SGX are technologies
  - Confidential Computing is a *kind* of technology
  - Protection of data-in-use is not
- Provider/vendor agnostic
- Widely applicable
  - AVS hosting: self/CSP/3rd party
  - Device ownership: self/CSP/3rd party
- Comprehensive
  - Covering key building blocks, interactions, services, processes, actors, responsibilities, …
  - Omissions create risk of ambiguity

Target Audiences and their Responsibilities to Each Other



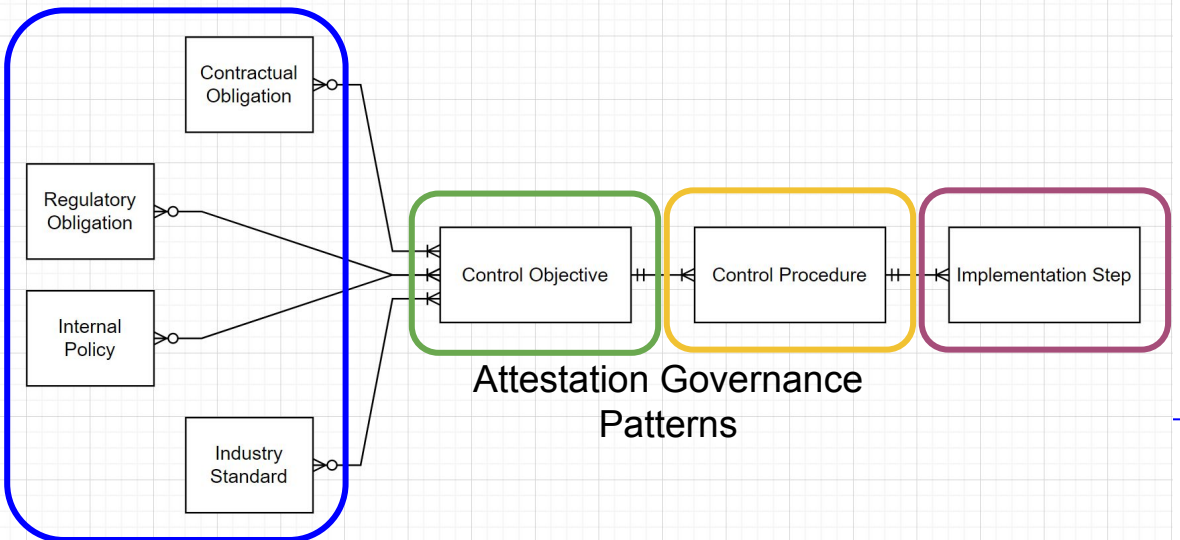
Target Audiences and their Responsibilities to Each Other

- The participants in the Confidential Computing space fall into several distinct categories
- These participants have unique responsibilities to each other
- Governance patterns must capture all these individual responsibilities and suggest effective and repeatable ways of addressing them



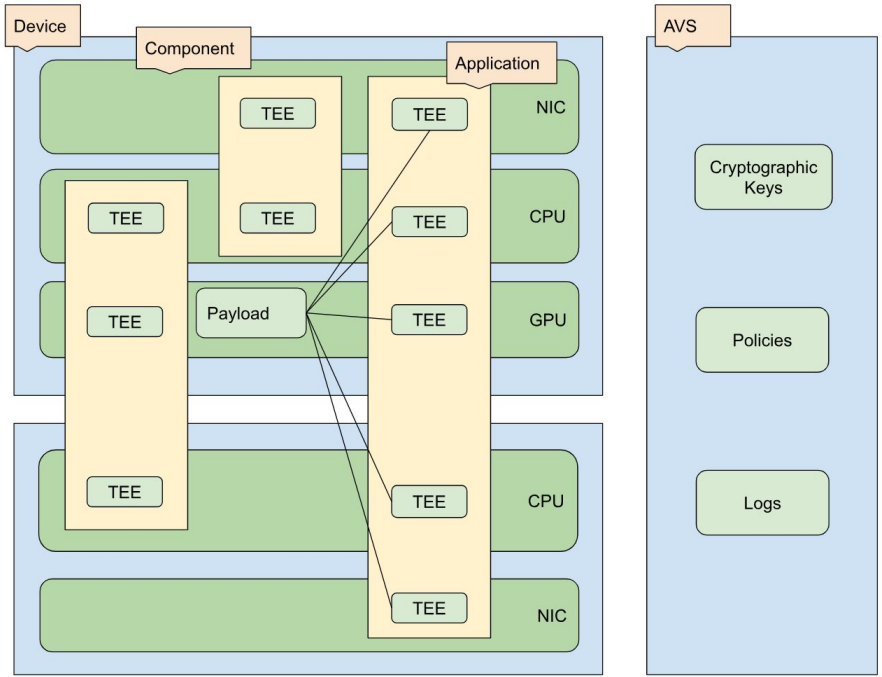
Regulatory Building Blocks: Entity-Relationship Diagram

- Control Specifications come from many sources
- Control Specifications compress down to Control Objectives
- Control Objectives expand to Control Procedures
- Control Procedures realized by Implementation Steps



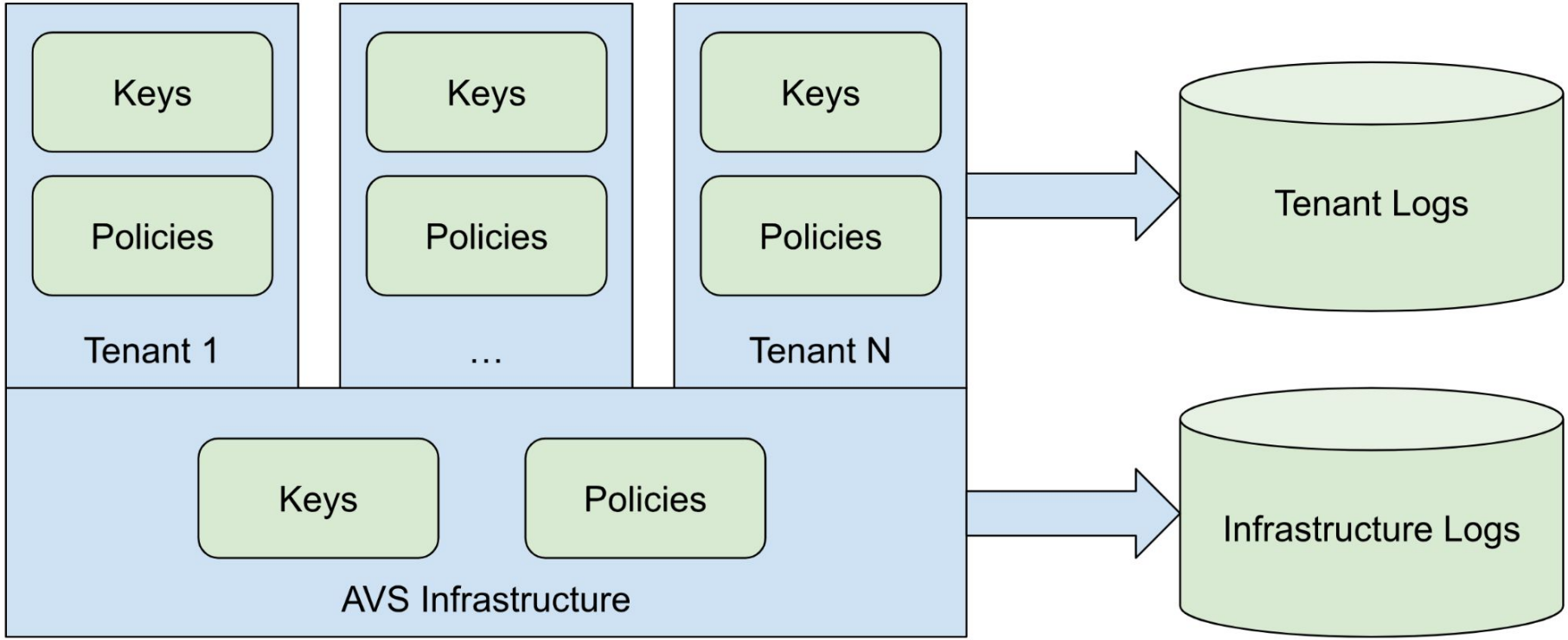
Device, Component, TEE, Payload, Payload Slice, …

- An Application (*) runs on one or more Devices
- An Application hosts a Payload, which comprises one or more Payload Slices
- A Device comprises one or more Components
- A Component hosts zero or more TEEs
- Payload Slices run inside TEEs (*)
- Each TEE executes a Payload Slice
- A {Payload Slice/TEE/Component} tuple is a standalone unit of governance
- The AVS comprises multiple governable entities
  - Policies (tenant & infrastructure)
  - Keys (tenant & infrastructure)
  - Logs



(*) The meanings of *Application* and *TEE* appears to be subtly different here from the CCC definition – need to reconcile

AVS Governable Entities

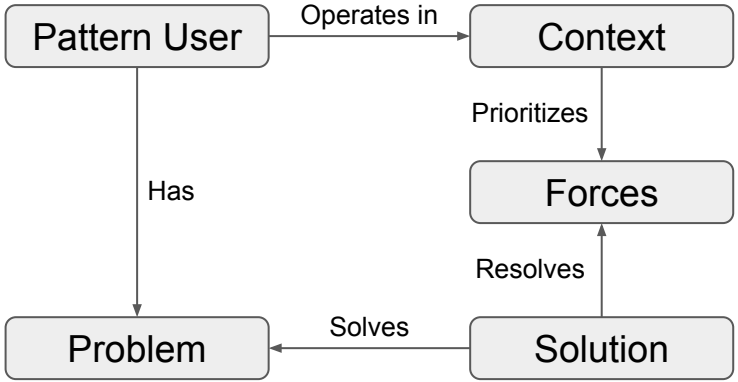


What is a “Pattern”?

A “Pattern” is a *Solution* to a *Problem* in a *Context*, shaped by *Forces*: Patterns

Required:

- **Context**: sets the stage where the Pattern takes places
- **Problem**: explains what the actual problem is
- **Forces**: describes why the Problem is difficult to solve
- **Solution**: explains the Solution in detail



Optional:

- **Resulting context** (a.k.a. “Consequences”): what happens when the Solution is implemented
- **Rationale**: describes the reason to use the solution
- **Related patterns**
- **Examples**

Patterns can be organized in Groups

Attestation Governance Patterns & Pattern Groups

1. Baseline Governance Patterns
   - Payload baseline governance
   - TEE baseline governance
   - Component (infrastructure) baseline governance
2. AVS Governance Patterns
   - AVS Tenant Governance
   - AVS Service Governance
   - AVS vs. Relying Party Governance
3. Downtime-Minimizing Deployment Governance Patterns
   - Payload Deployment Governance
   - TEE Deployment Governance
   - Component (Infrastructure) Deployment Governance