PoC Configuration Diagram

This diagram illustrates the data flow and component interaction of the Keylime-based Remote Attestation PoC:

Component	Description
Rust-based Agent	Runs on client, collects PCRs and IMA logs, signs data using TPM
TPM 2.0 (STMicro)	Stores keys, provides quote (attestation evidence)
Secure Boot	Ensures boot chain integrity before OS loads
IMA	Monitors file integrity and provides runtime measurements
Python-based Registrar	Stores node credentials and public keys
Python-based Verifier	Validates quotes, policies, and IMA measurements
Python-based Tenant	Manages policy provisioning and attestation requests
UUID	Fixed: 11111111-1111-1111-1111-111111111111
TPM NV Index	Defined: 0x1500016

All components communicate over secure channels. Logs and policies are synchronized and verified to maintain platform integrity.