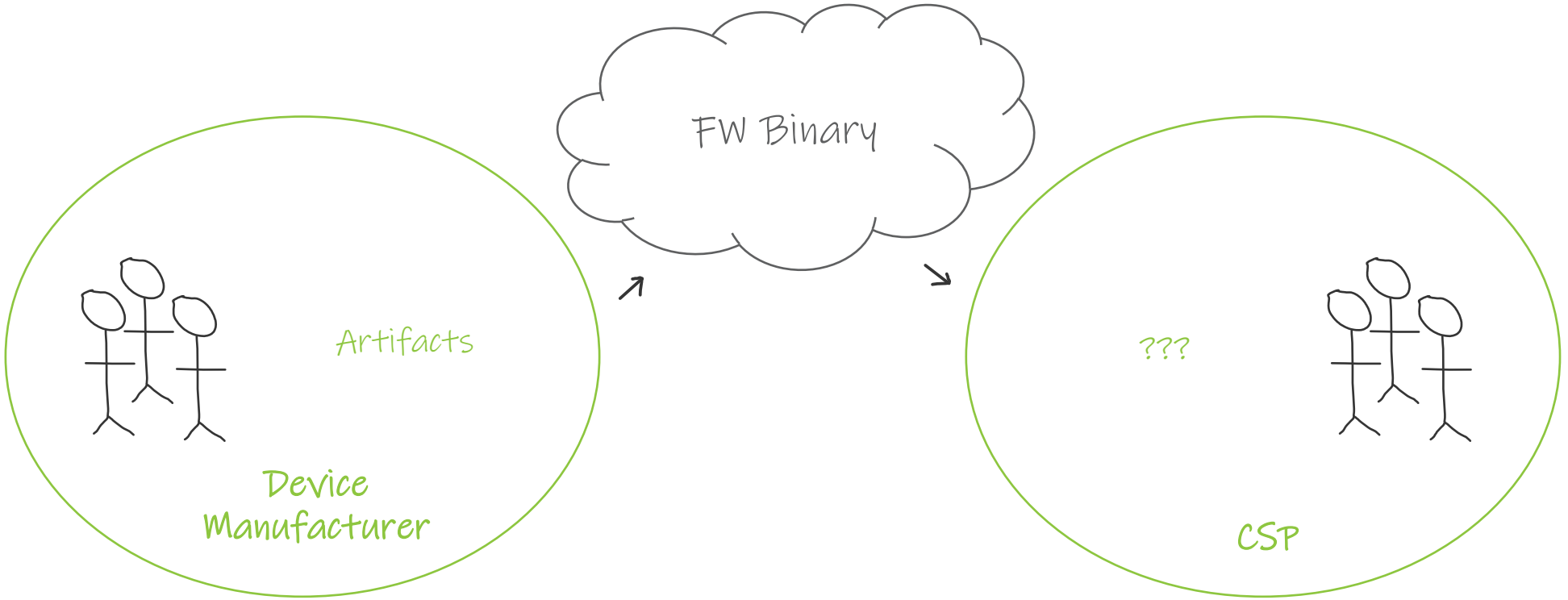
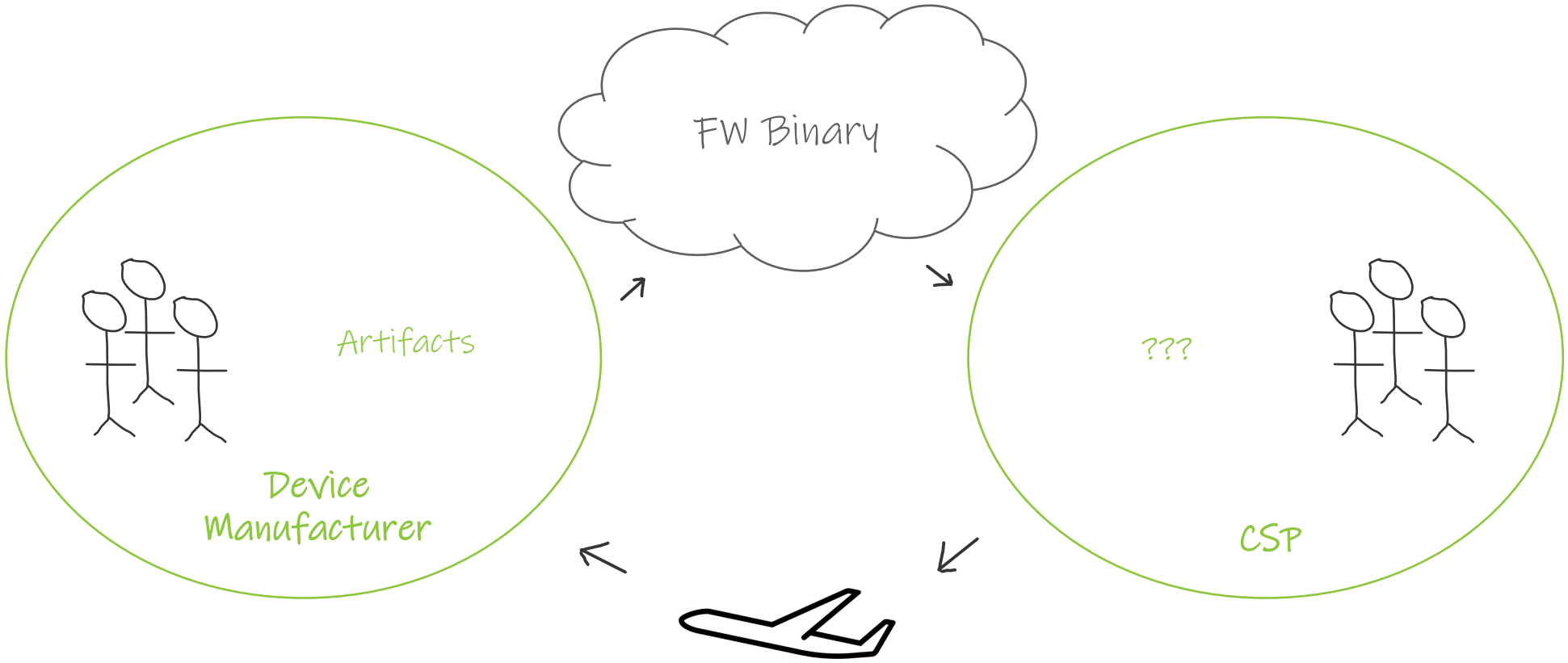
Supply Chain Auditing

Bryan Kelly [Microsoft], Bharat Pillilli [Microsoft],
Andres LC [Google]

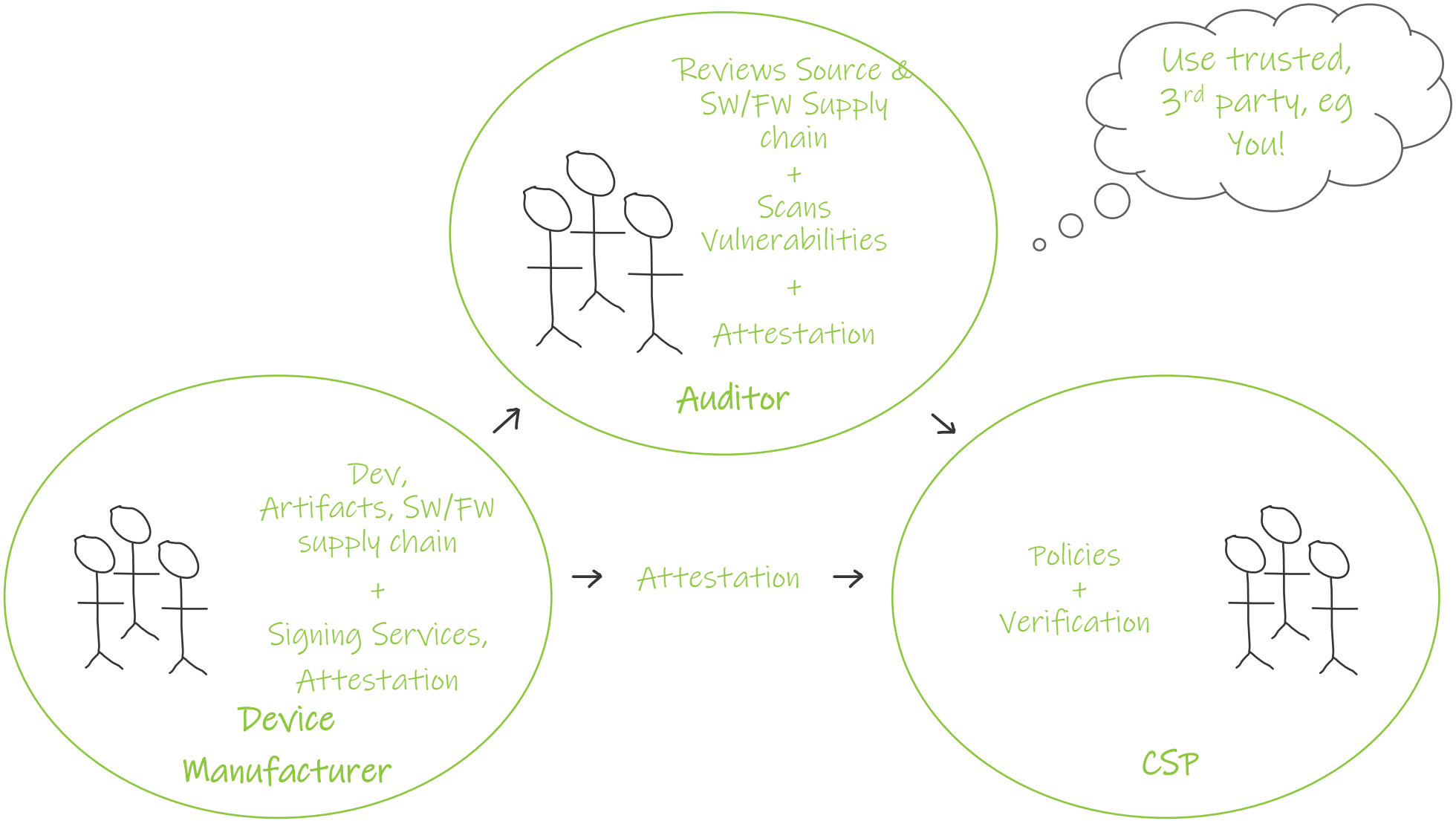
Traditional Model



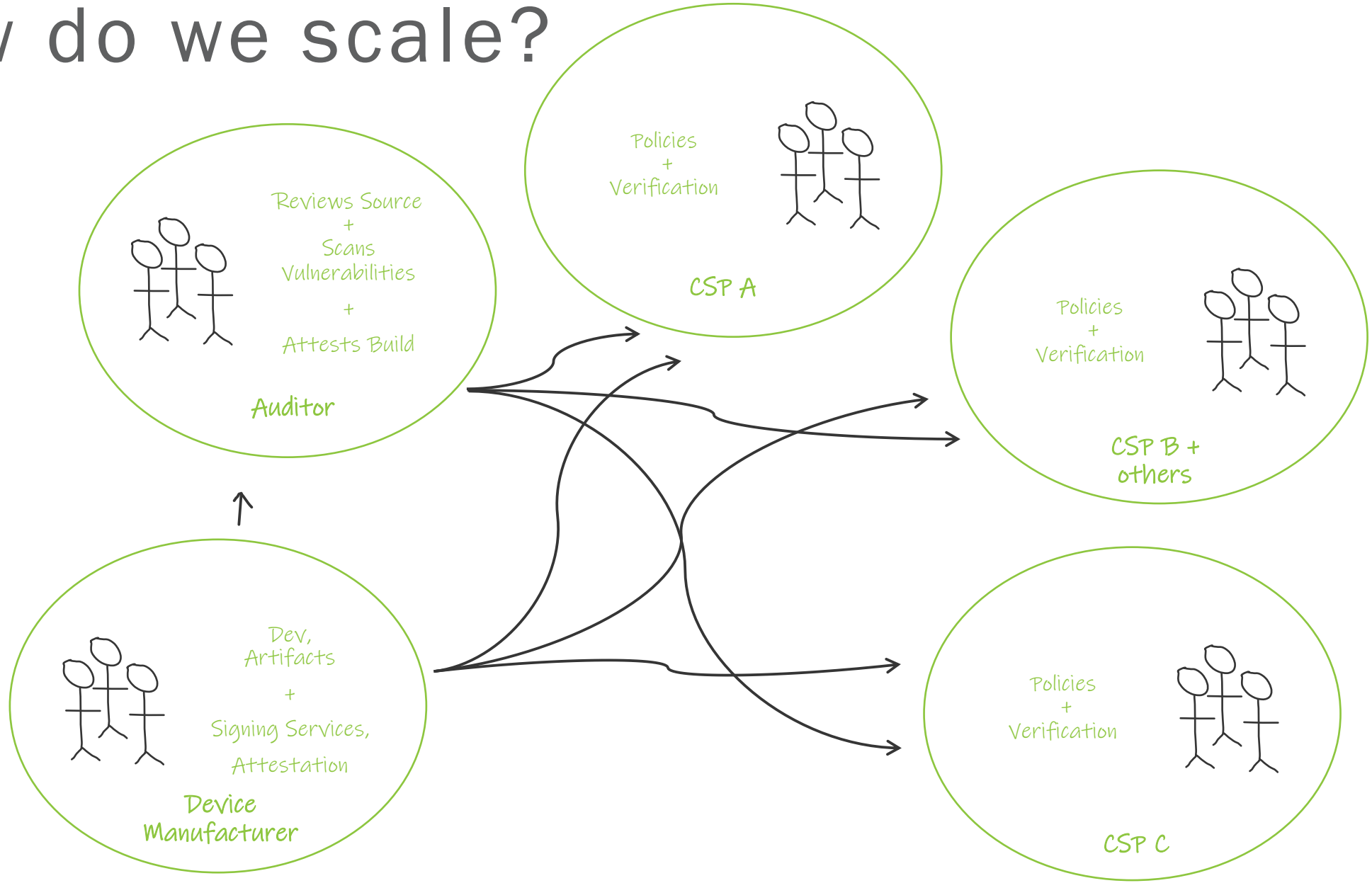
CSP point-in-time review model



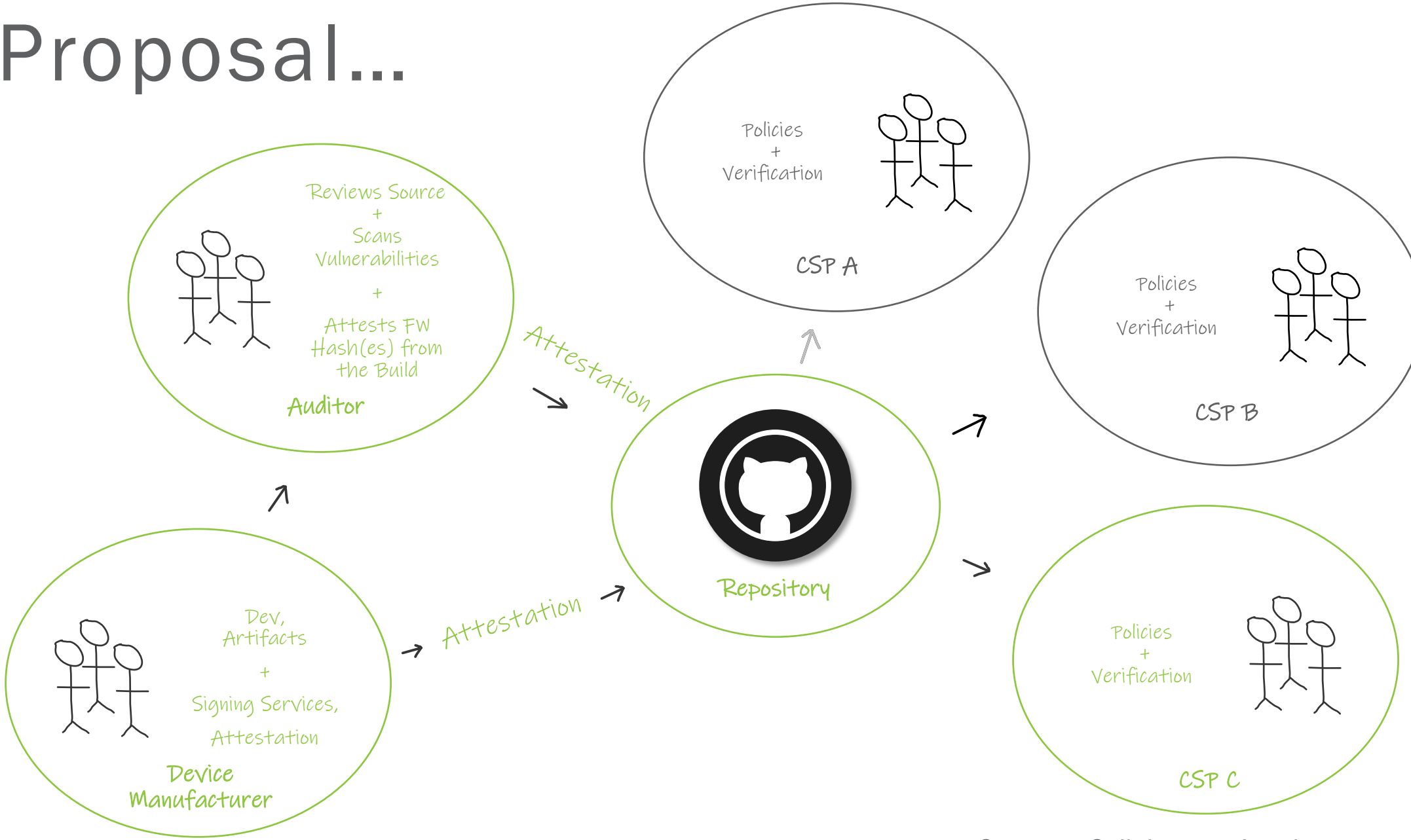
Standardize Supplier Audit



How do we scale?

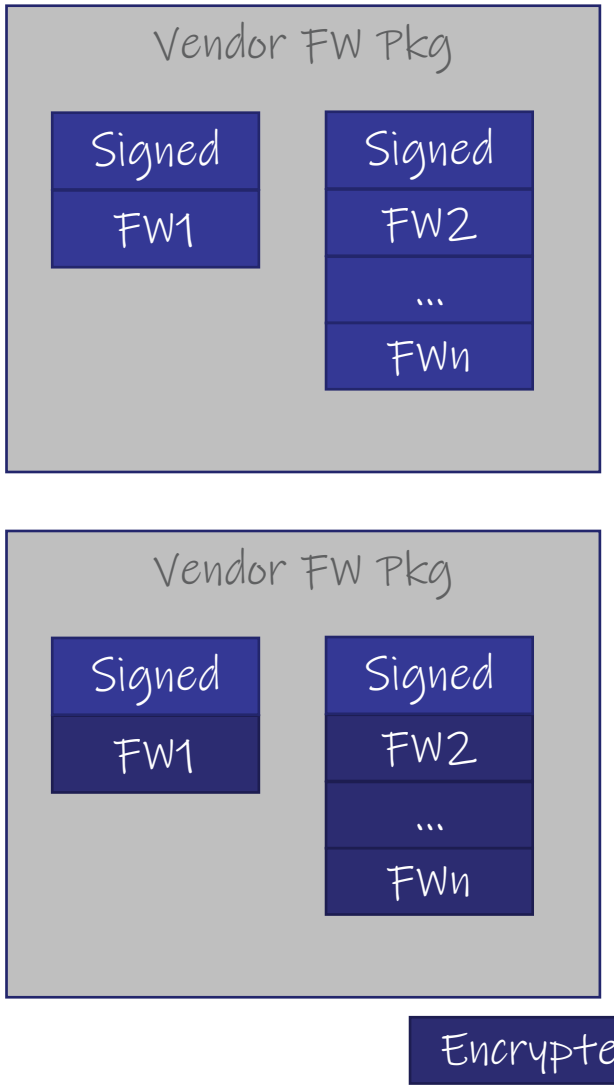


Proposal...


Reviews Source
+
Scans Vulnerabilities
+
Attests FW Hash(es) from the Build
Auditor
Attestation
Policies
+
Verification
CSP A
Policies
+
Verification
CSP B
Repository
Dev, Artifacts
+
Signing Services, Attestation
Device Manufacturer
Attestation
Policies
+
Verification
CSP C

What to account for?

- **Handling Encrypted FW**
  - SBOM from MANUFACTURER & AUDITOR must reflect encrypted & plain-text hashes
- **Vendor FW Dependencies**
  - E.g. Security FW to Power Management FW
- **CSP specific releases** (for prototype or CSP specific scenarios)
- **Reproduceable builds**
  - Auditor must have the ability to do a build & generate the hash => tool chain
- **Auditor Review Expectation**



How to account for? -> SBOM

- Complex & Dynamic Supply Chains
- Need Transparency and information on firmware objects
- Machine readable/interpretable and partly human readable!
- Dependencies b/w Vendor FW releases to CSP internal FW releases & deployments
- Many SBOM formats – what to pick?
- Based on NIST guidance: SPDX or SWID
- Recommended format: SWID (enabling potential transition to CoSWID in future)

Auditor Review Expectations

- Code Security Assessment (as specified in OCP spec)
  - Discovery of built-in and hard-coded credentials
  - Identifying memory safety issues
  - Deprecated and insecure encryption options
  - Trust-boundary violations,
  - Input validation failures
  - Any open or recently closed CVEs in first or third party code
  - Compiler, toolchain options (aslr, stack canaries, etc)
- Audit review output must be in SWID SBOM in a machine-readable format
- Profiles/Levels of Audit

Next steps

- Specification 1.0 release before OCP'22
- Finalize the SBOM and formats
- Work with Auditors to define profiles/levels of audits

Q&A