Enforcing the OpenSSF Ecosystem

carabiner

Enforcing the OpenSSF Ecosystem with AMPEL

carabiner

Hello, I’m @puerco! ✌️

- Software Engineer @ Carabiner
- Technical Lead on the Kubernetes Release Engineering team (SIG Release)
- Technical Lead of OpenVEX and Protobom (incubating in OpenSSF)
- SPDX Project Contributor

- I like to ride my bike around the world! 🚴

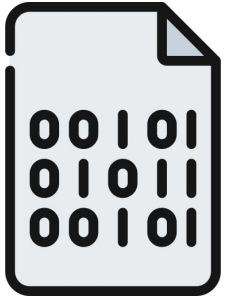
carabiner

carabiner
systems

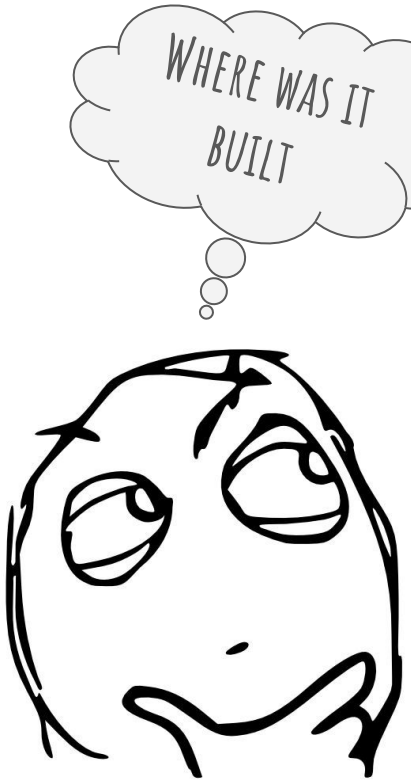
Supply Chain Transparency

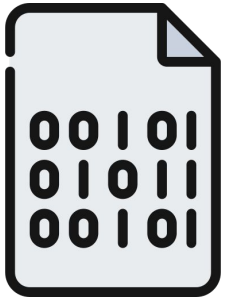
or, verifiable software consumption

carabiner

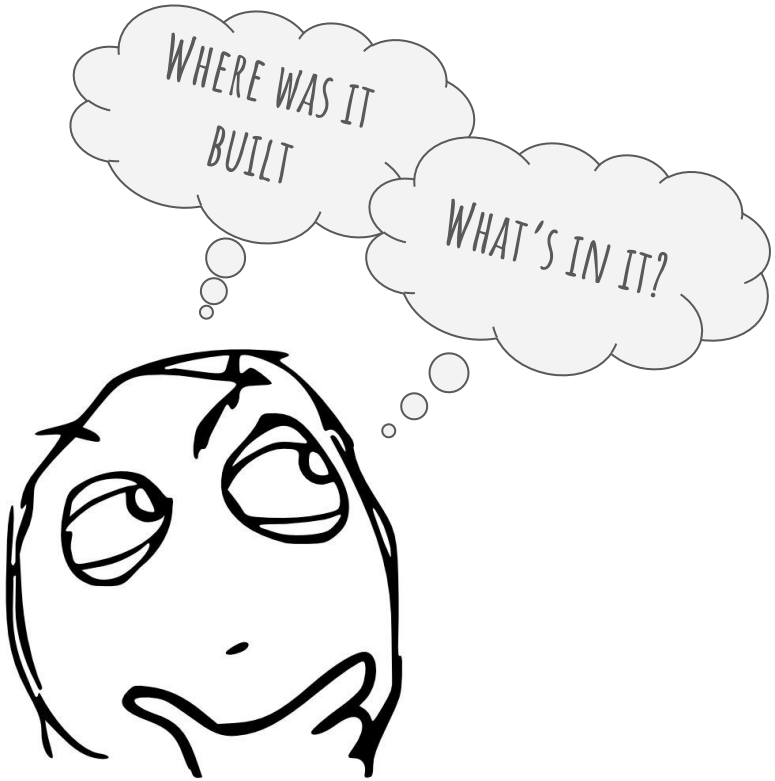


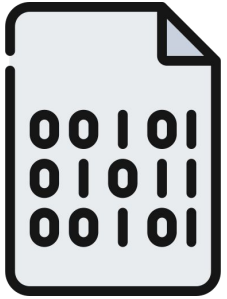
carabiner





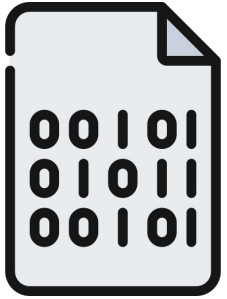
carabiner



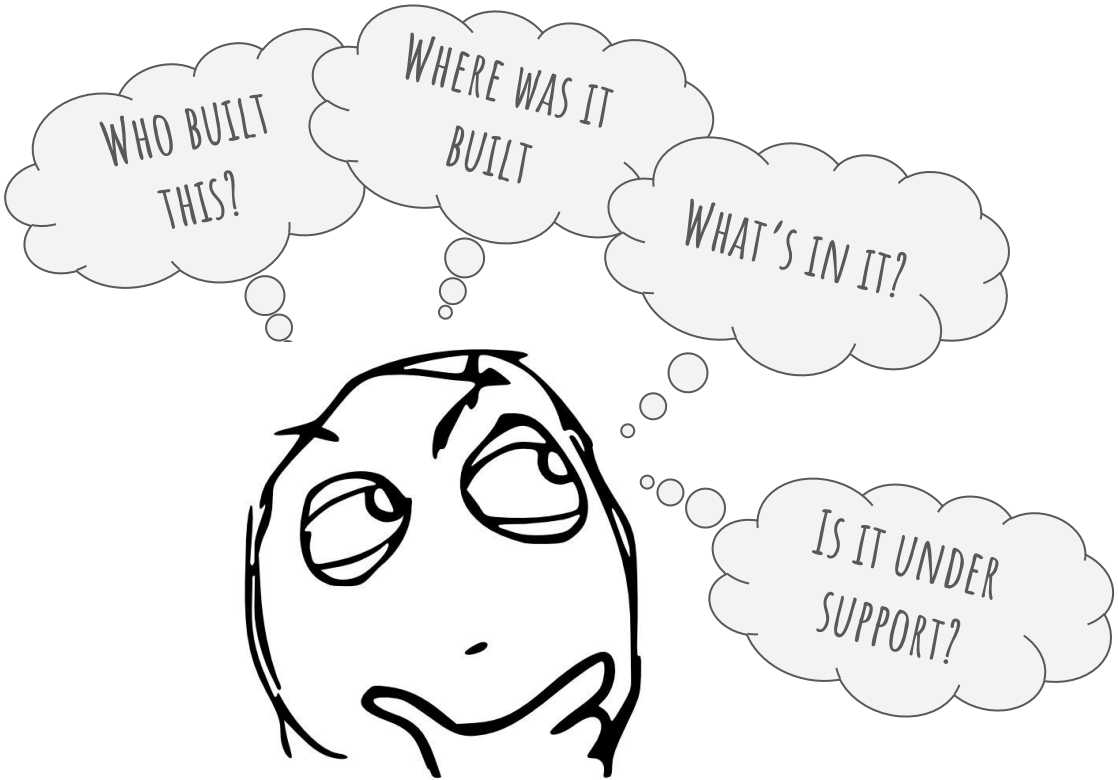


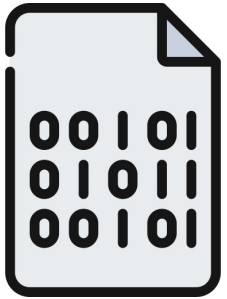
carabiner


WHO BUILT THIS?
WHERE WAS IT BUILT
WHAT'S IN IT?

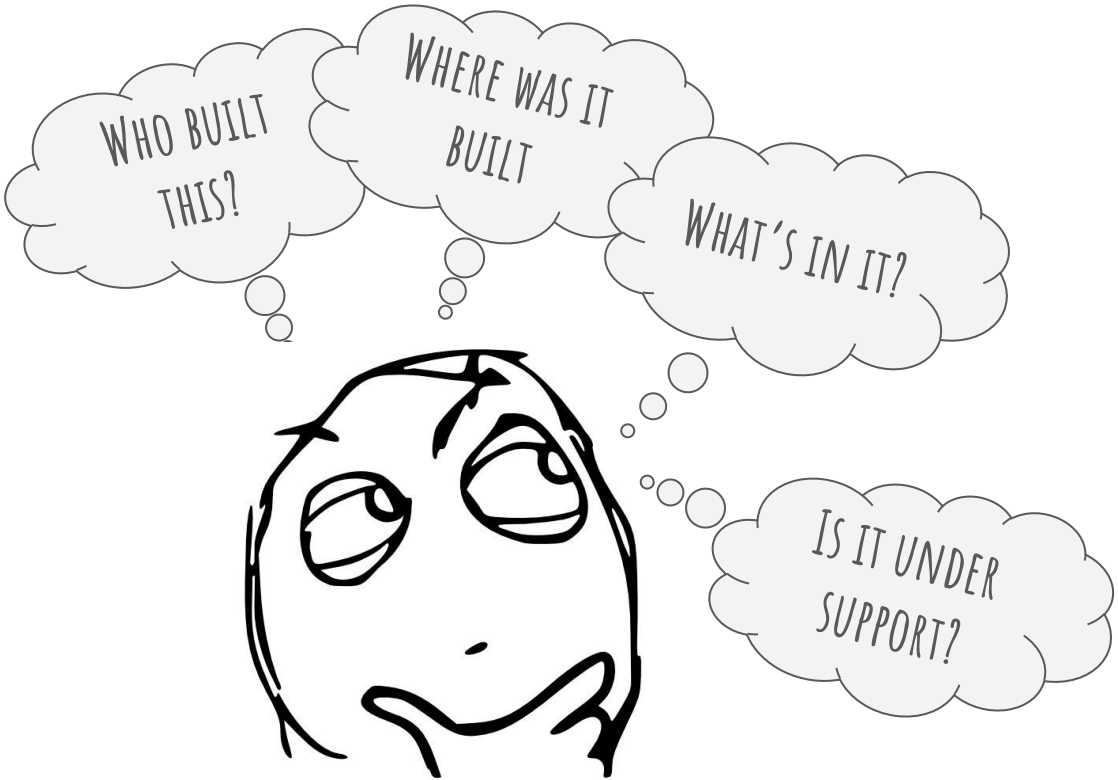

00101
01011
00101

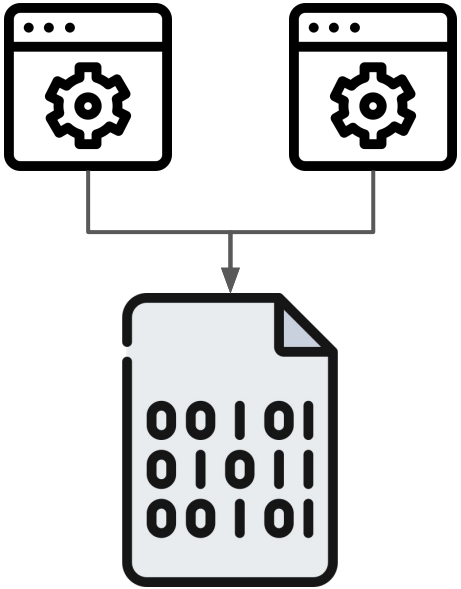
carabiner


Who built this?
Where was it built
What's in it?
Is it under support?

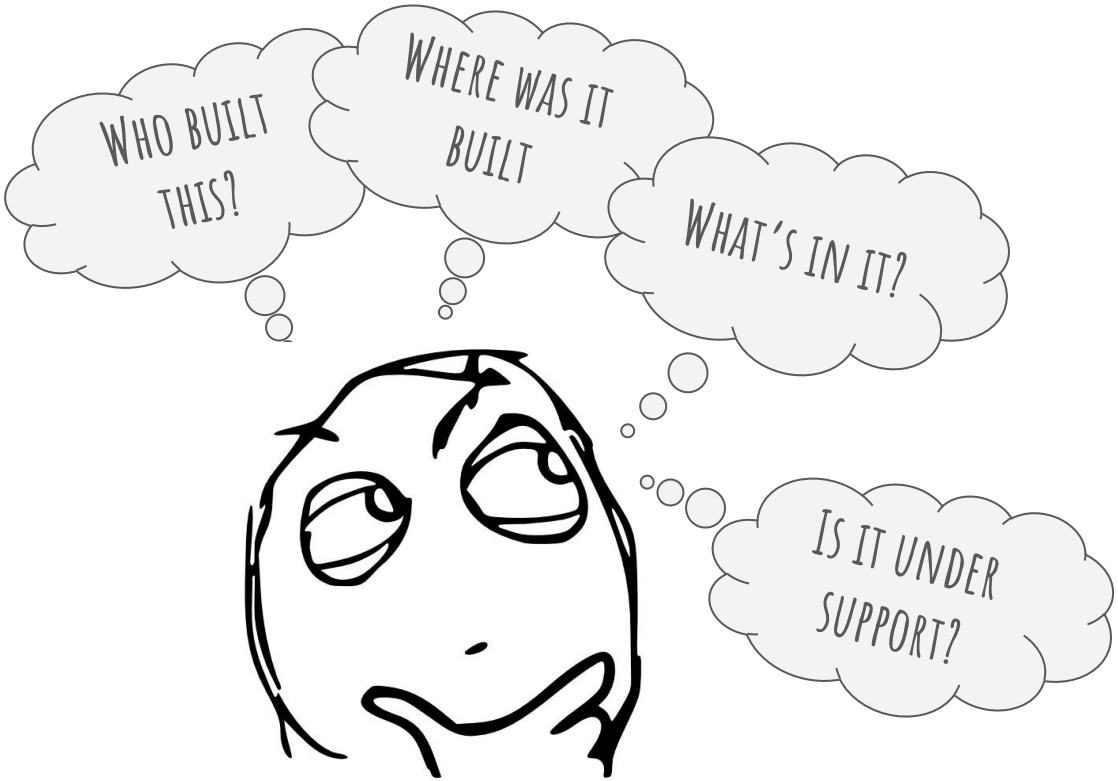

00101
01011
00101

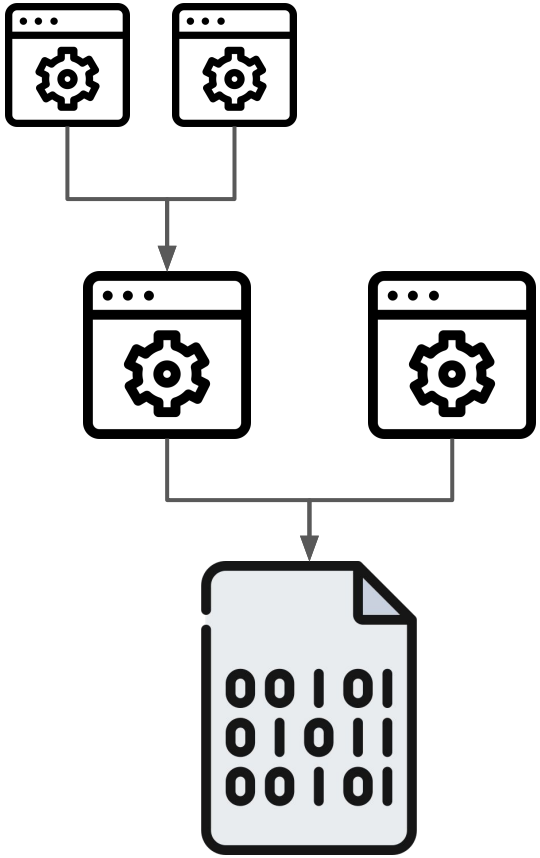
carabiner


WHO BUILT THIS?
WHERE WAS IT BUILT
WHAT'S IN IT?
IS IT UNDER SUPPORT?

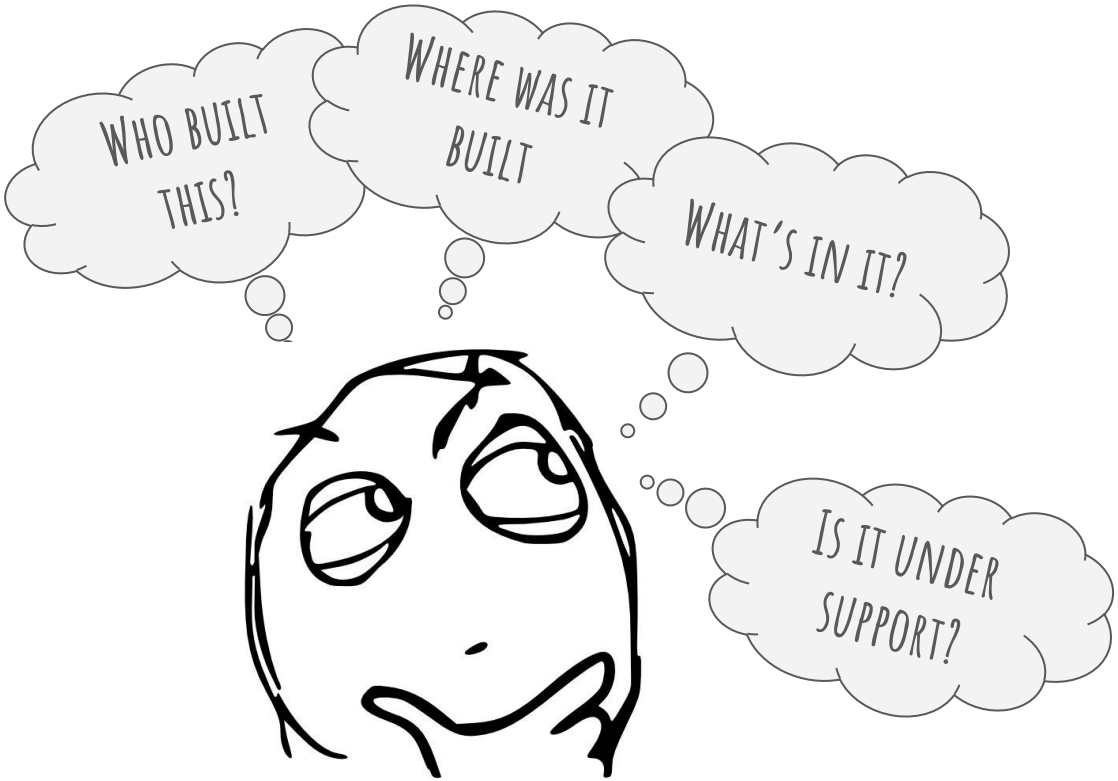

00101
01011
00101

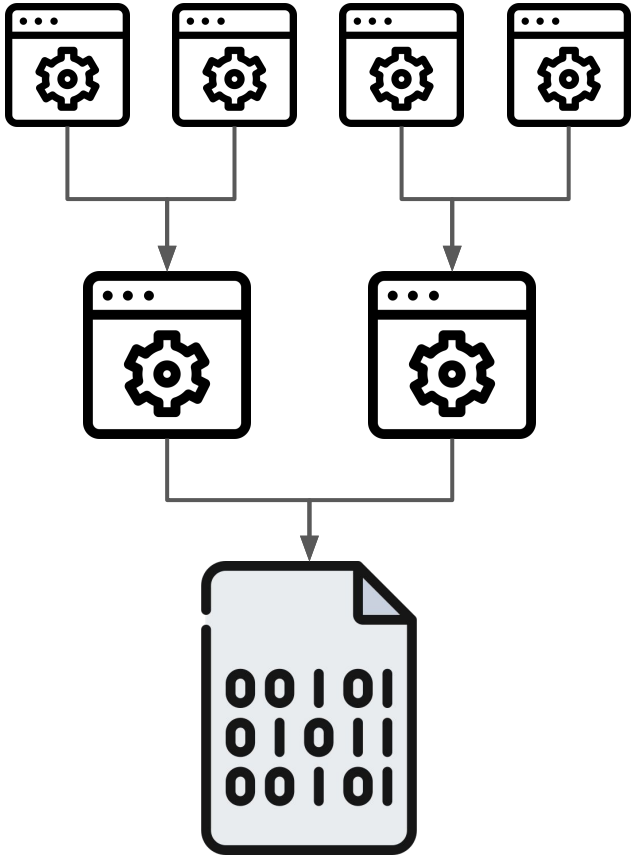
carabiner


WHO BUILT THIS?
WHERE WAS IT BUILT
WHAT'S IN IT?
IS IT UNDER SUPPORT?

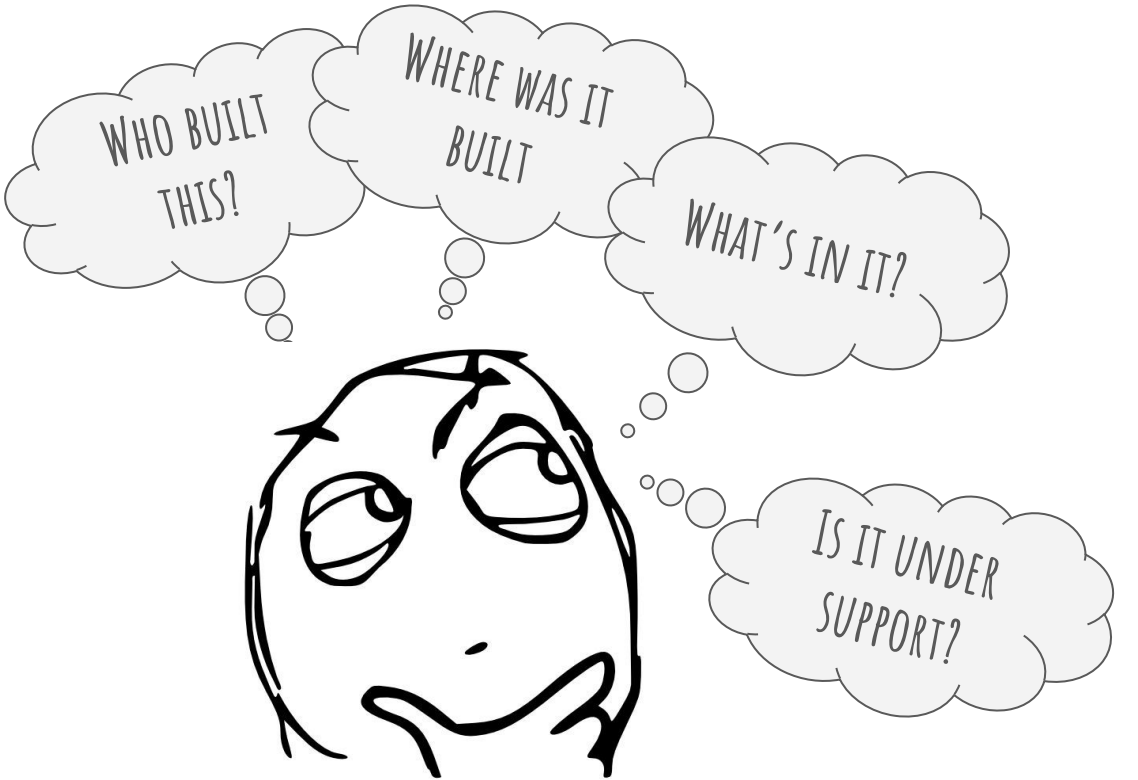

00101
01011
00101

carabiner


Who built this?
Where was it built
What's in it?
Is it under support?

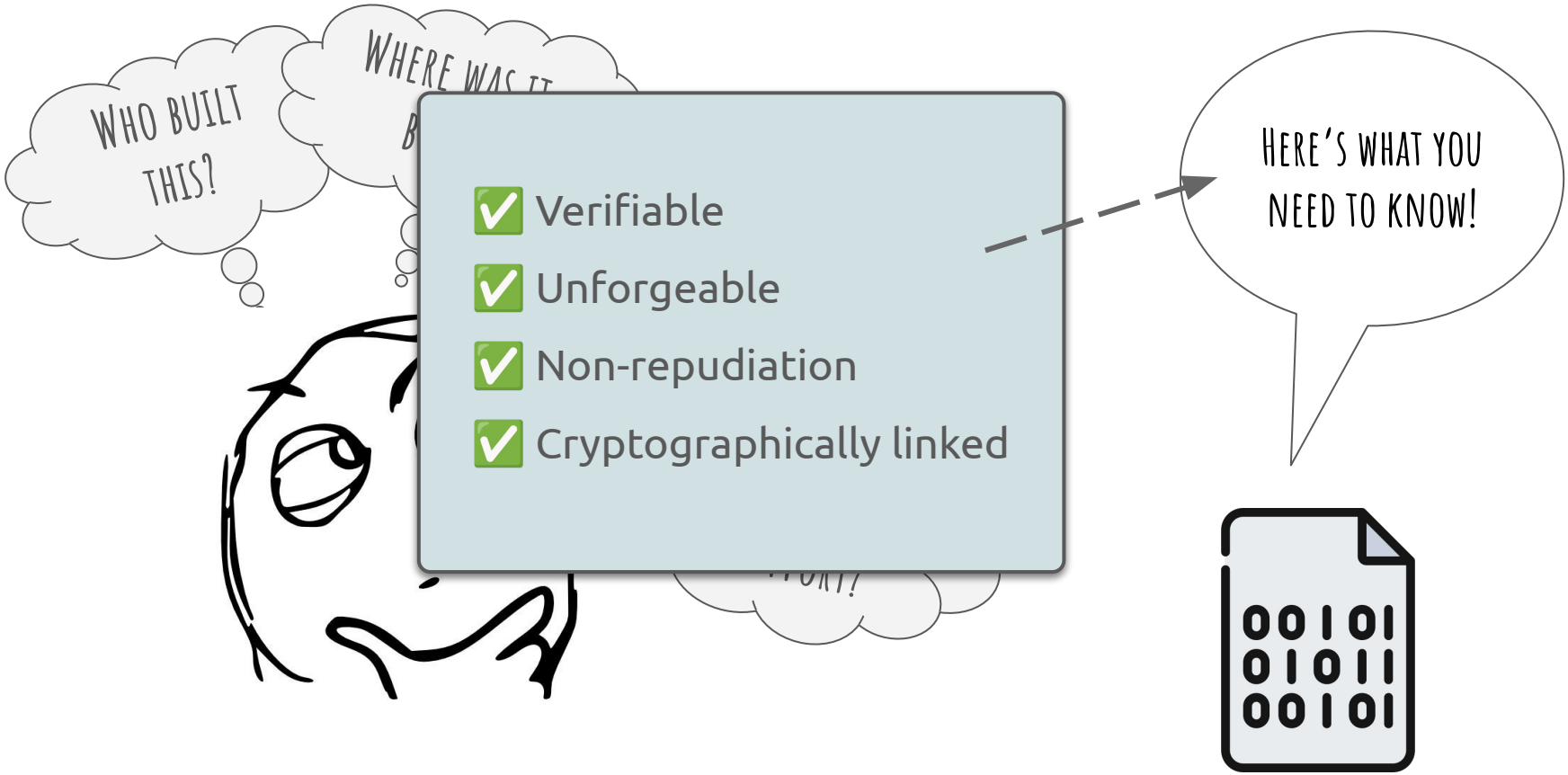

00101
01011
00101

carabiner


Who built this?
Where was it built
What's in it?
Is it under support?


Here's what you need to know!
00101
01011
00101

carabiner


WHO BUILT THIS?
WHERE WAS IT
✅ Verifiable
✅ Unforgeable
✅ Non-repudiation
✅ Cryptographically linked
HERE'S WHAT YOU NEED TO KNOW!
00101
01011
00101

carabiner

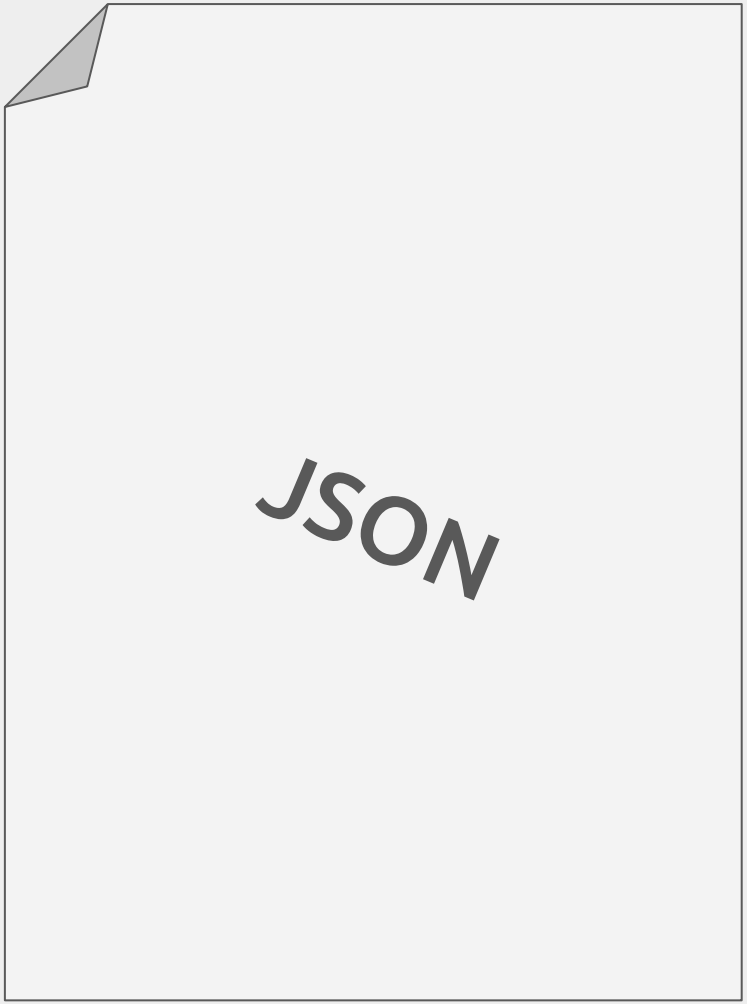
What is an Attestation?

Understanding signed claims

carabiner

What is an Attestation?

“A signed set of claims about a subject”



carabiner

What is an Attestation?

> *Little atoms of a Secure Software Supply Chain*
>
> Dr Santiago Torres-Arias

JSON

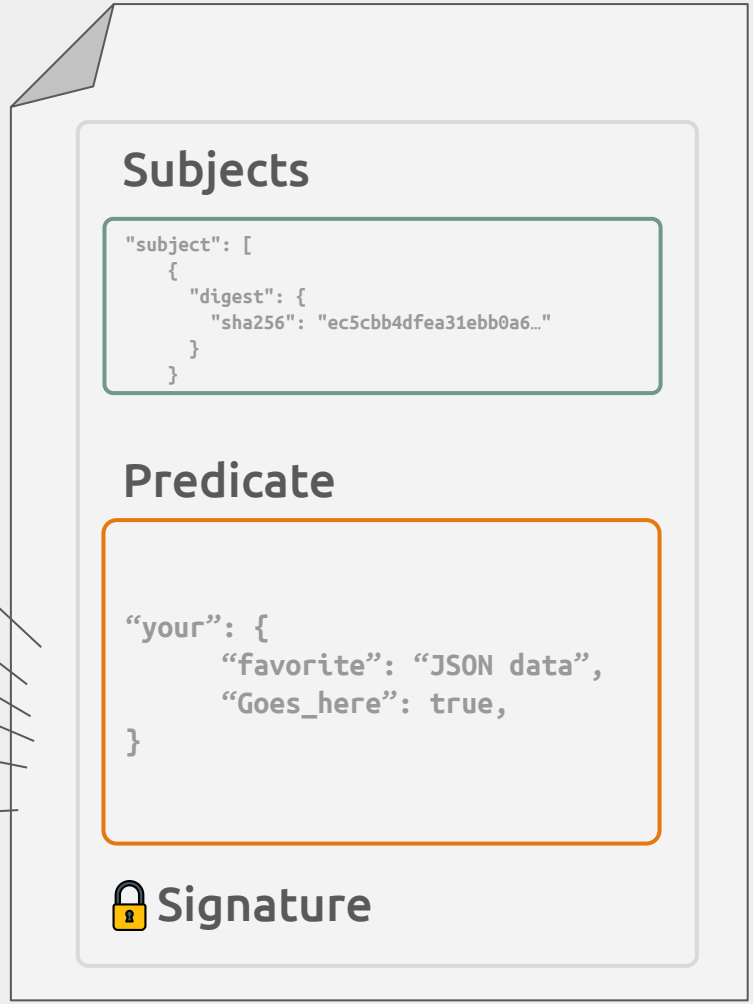
carabiner

What is an Attestation?

“A signed set of claims about a subject”

carabiner

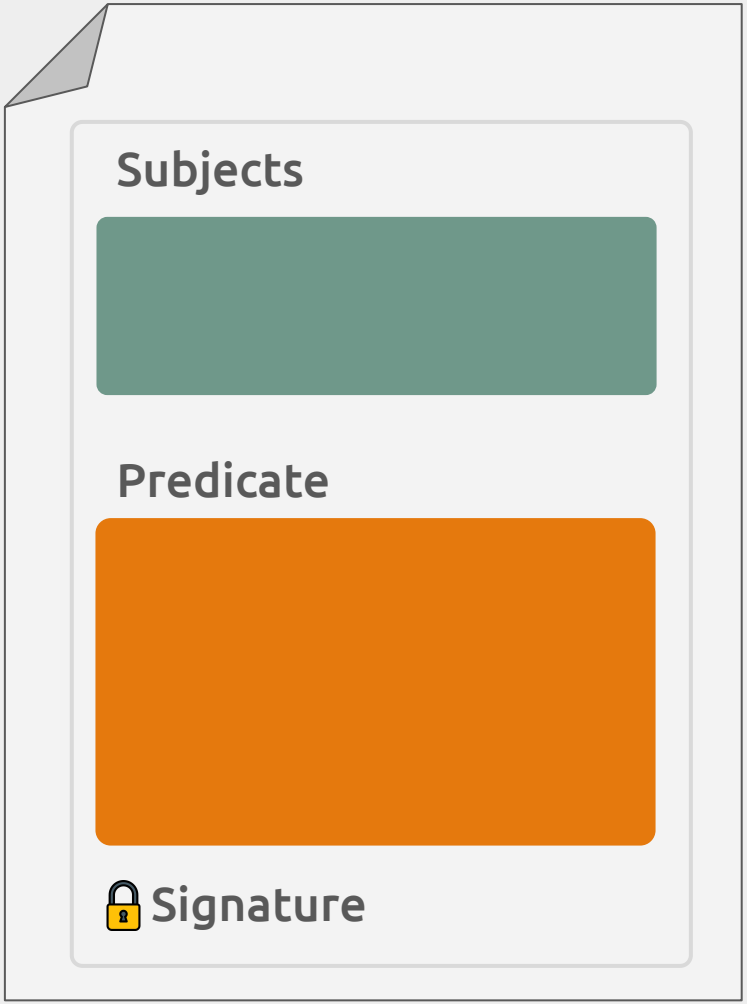
What is an Attestation?



carabiner

What is an Attestation?

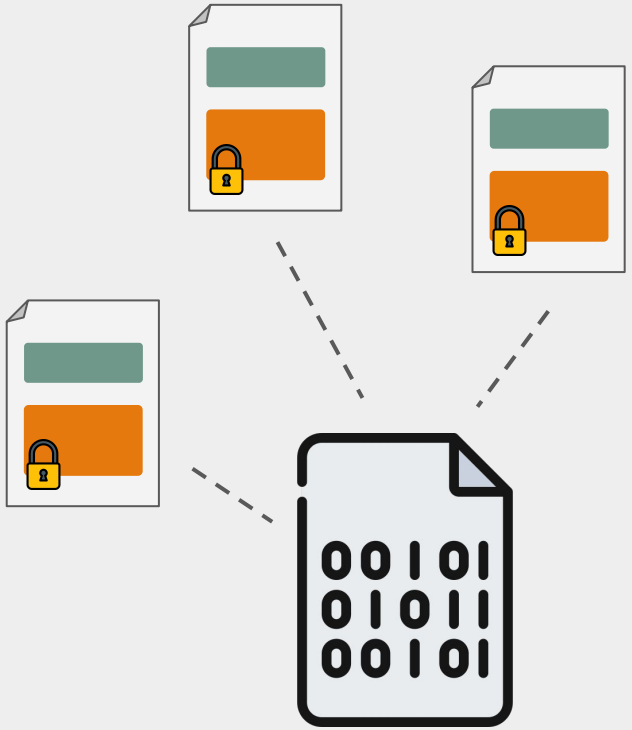
“A signed set of claims about a subject”



carabiner

What is an Attestation?

“A signed set of claims about a subject”



carabiner

What is an Attestation?

carabiner

“ There’s no security without verification „

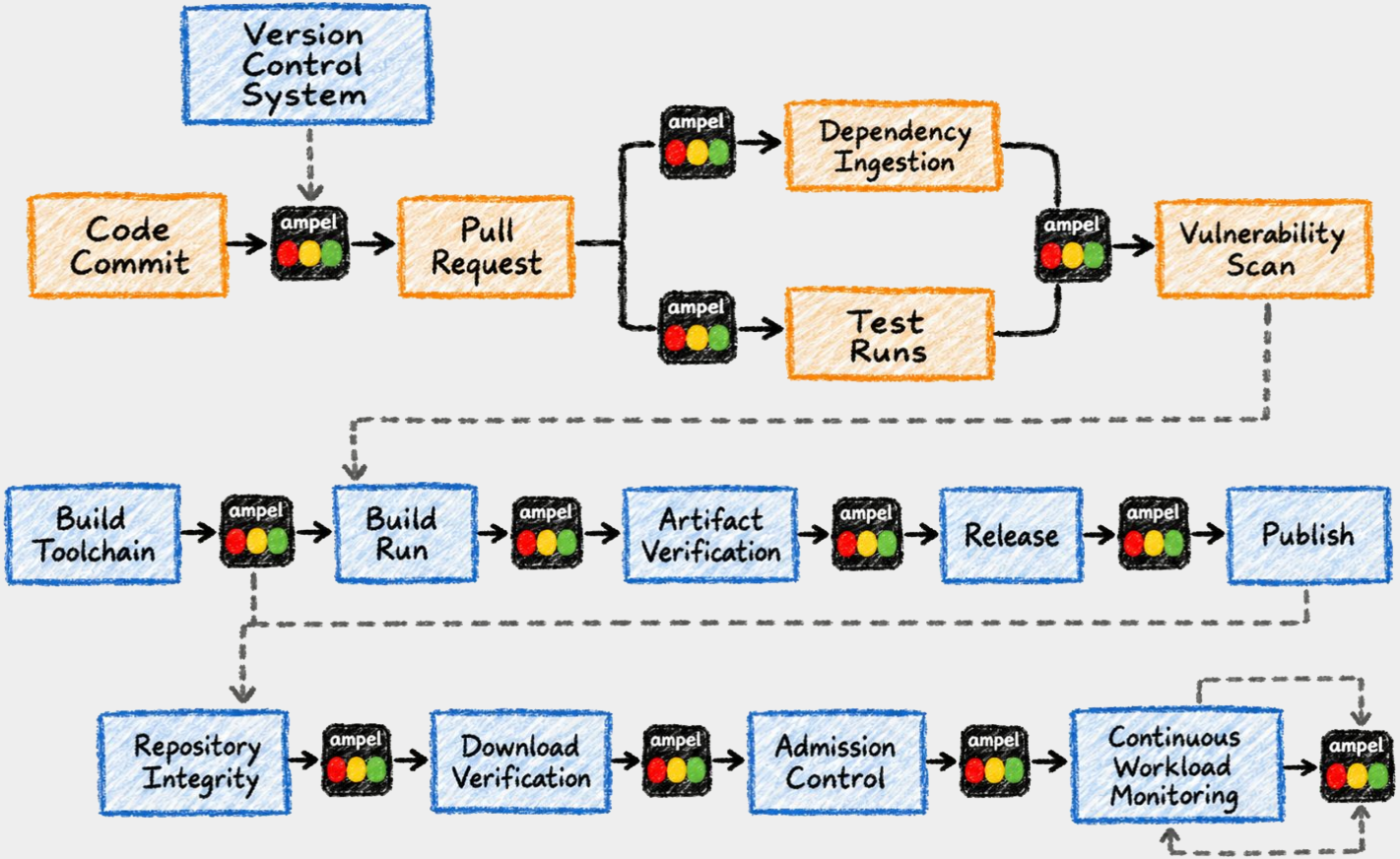
- Trevor Rosen
GitHub

carabiner


ampel

Amazing Multipurpose Policy Engine

Amazing Multipurpose Policy Engine (and L)


Version Control System
Code Commit
ampel
Pull Request
ampel
Dependency Ingestion
ampel
Test Runs
ampel
Vulnerability Scan
Build Toolchain
ampel
Build Run
ampel
Artifact Verification
ampel
Release
ampel
Publish
Repository Integrity
ampel
Download Verification
ampel
Admission Control
ampel
Continuous Workload Monitoring
ampel

carabiner

With a modular architecture, AMPEL solves some of the problems preventing the operationalization of software supply chain security technologies.

Key Blockers Solved by AMPEL

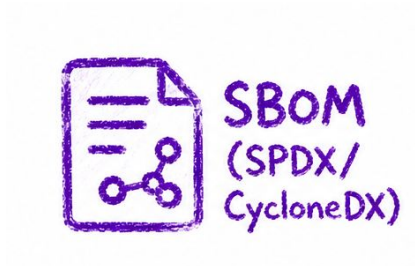
- Embeddable
- Policy Reuse
- Policy Composition
- Community ecosystem
- Domain-based extensions
- Tool Compatibility

carabiner

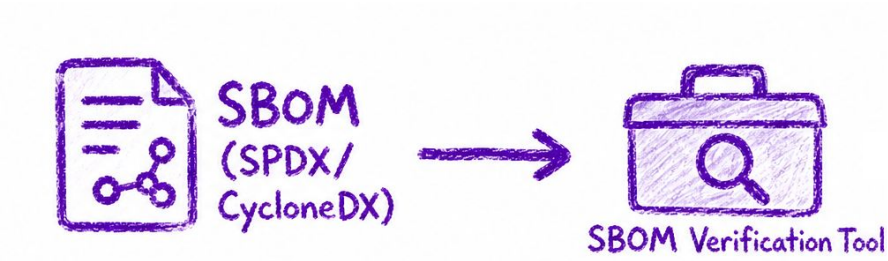
Evidence Diversity

Gimme all the formats!

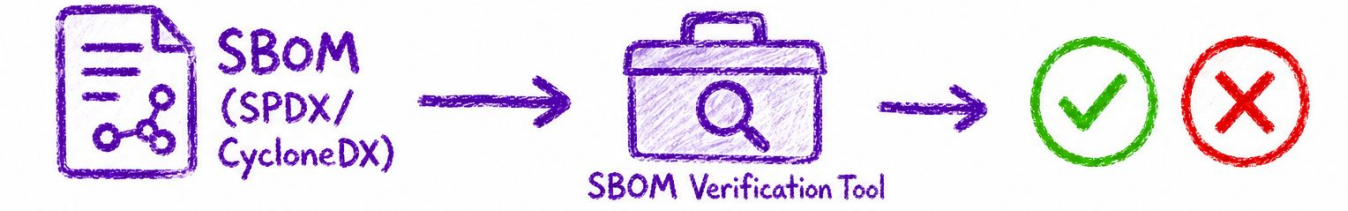
carabiner



carabiner



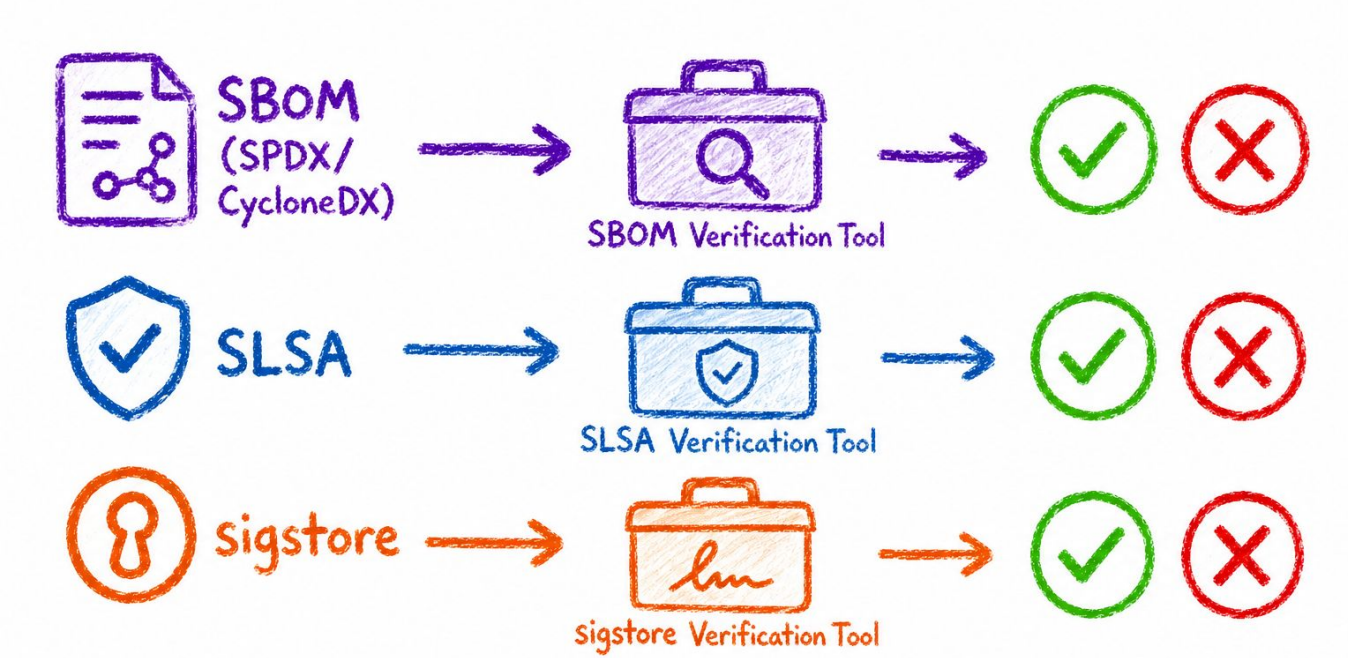
carabiner



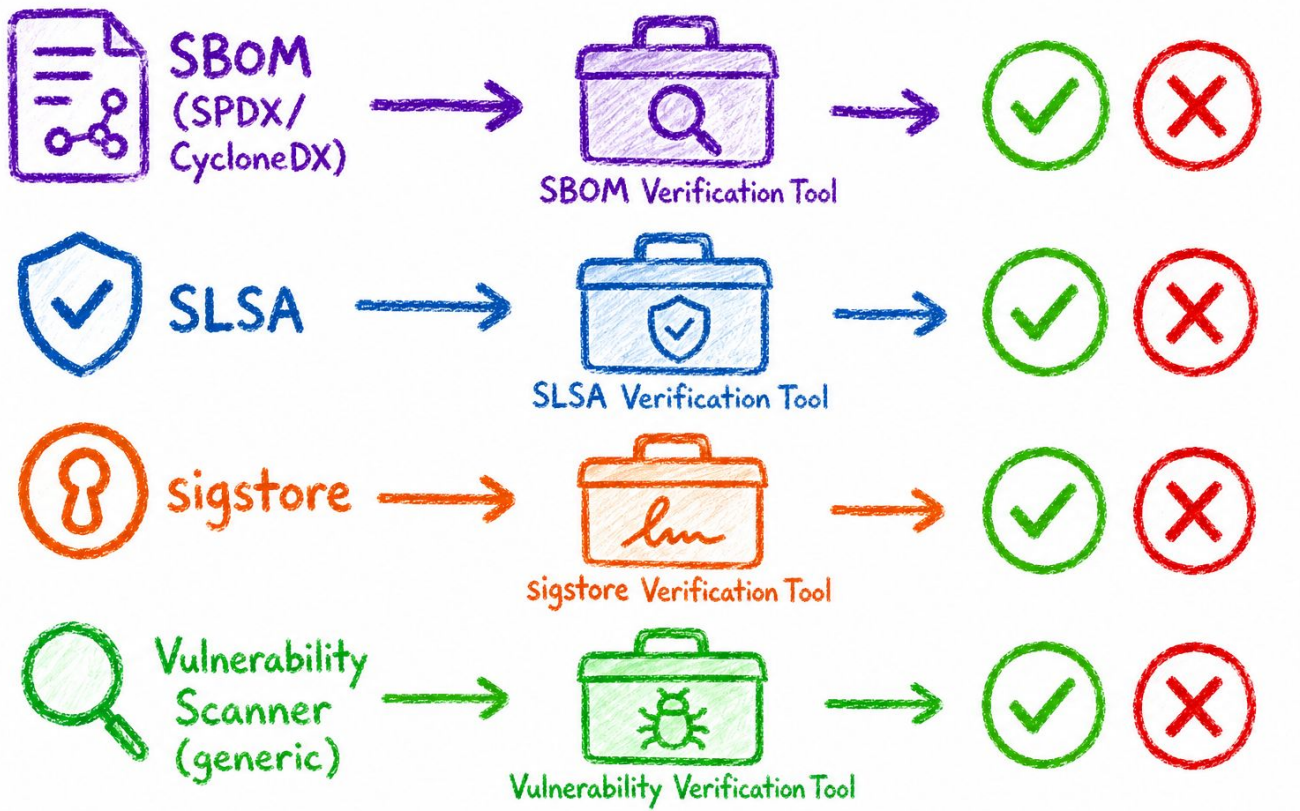
carabiner


SBOM
(SPDX/
CycloneDX)
SBOM Verification Tool
SLSA
SLSA Verification Tool

carabiner


SBOM
(SPDX/
CycloneDX)
SBOM Verification Tool
SLSA
SLSA Verification Tool
sigstore
sigstore Verification Tool

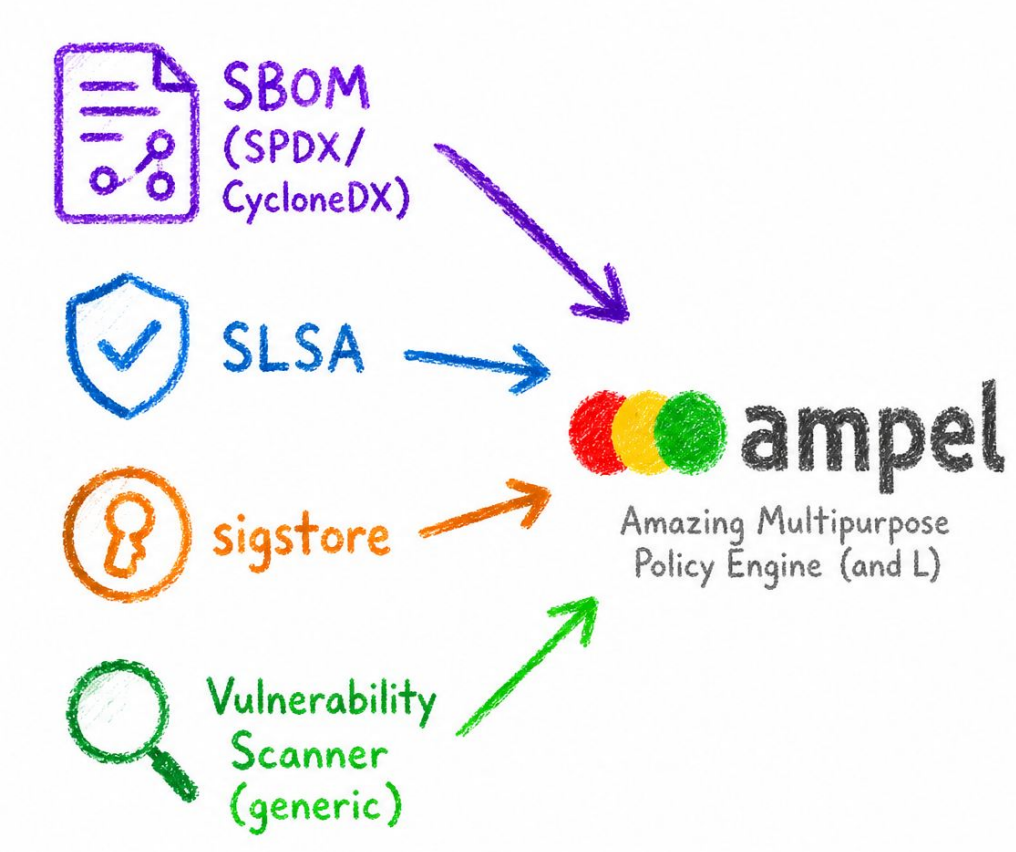
carabiner


SBOM
(SPDX/
CycloneDX)
SBOM Verification Tool
SLSA
SLSA Verification Tool
sigstore
sigstore Verification Tool
Vulnerability
Scanner
(generic)
Vulnerability Verification Tool

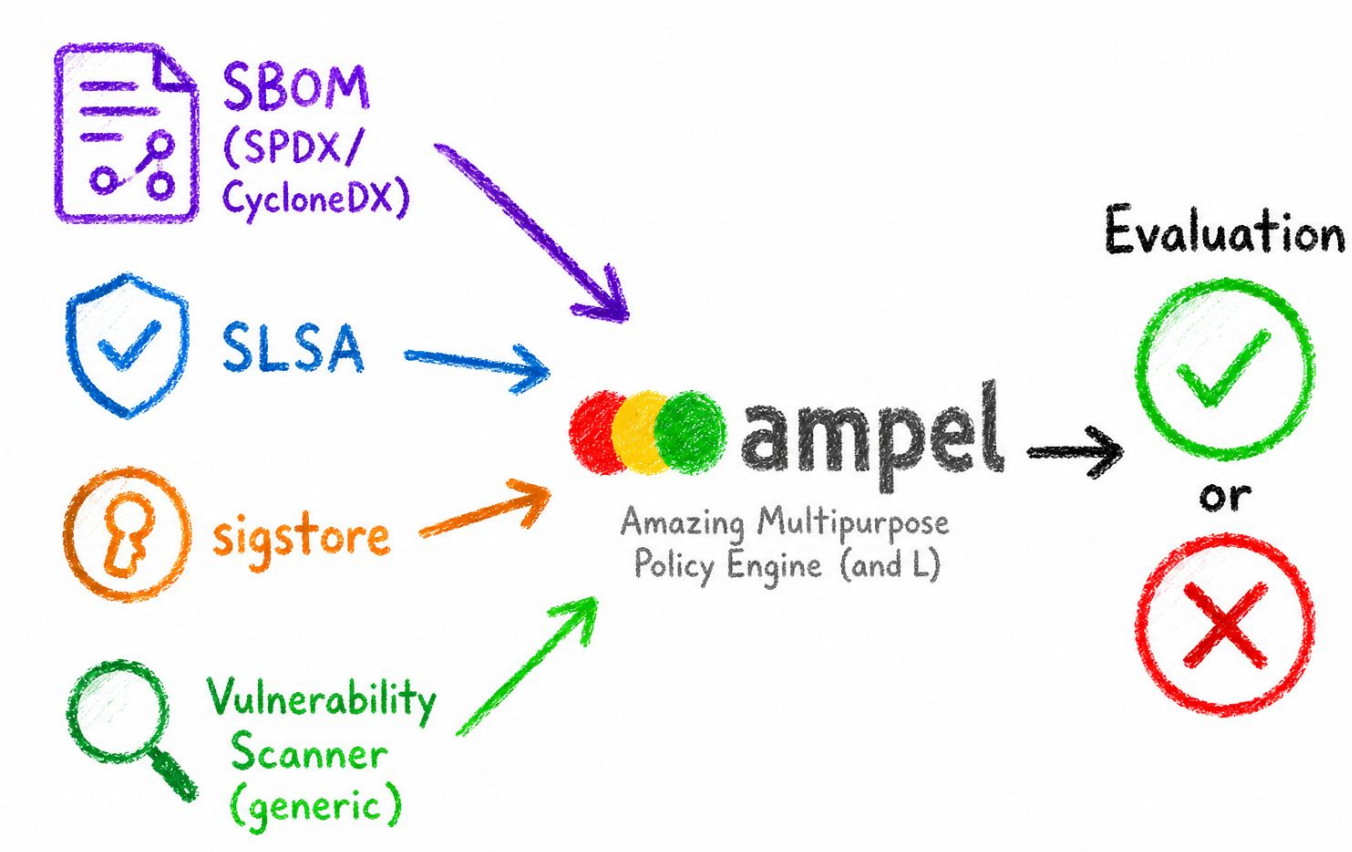
carabiner


SBOM
(SPDX/
CycloneDX)
SLSA
sigstore
Vulnerability
Scanner
(generic)

carabiner


SBOM
(SPDX/
CycloneDX)
SLSA
sigstore
Vulnerability
Scanner
(generic)
ampel
Amazing Multipurpose
Policy Engine (and L)

carabiner


SBOM
(SPDX/
CycloneDX)
SLSA
sigstore
Vulnerability
Scanner
(generic)
ampel
Amazing Multipurpose
Policy Engine (and L)
Evaluation
or

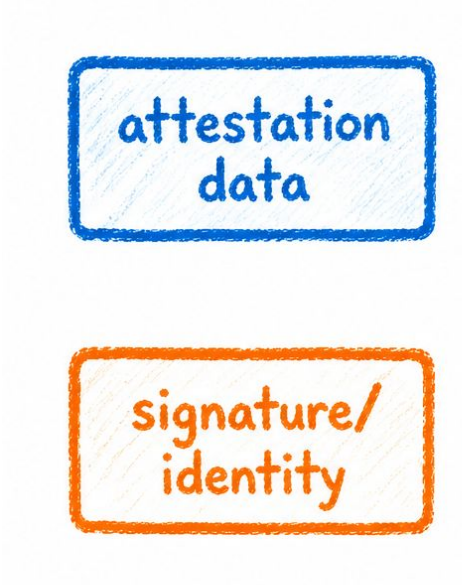
carabiner

Full Stack Verification

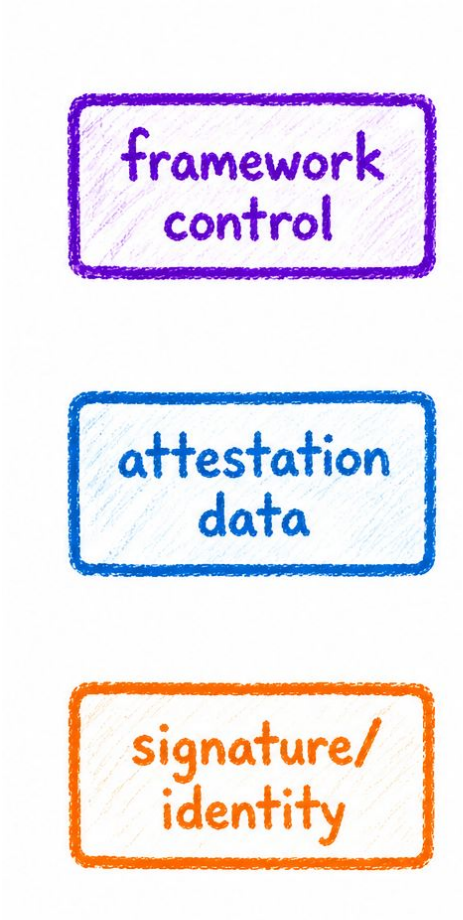
All them cakes belong to you!

carabiner

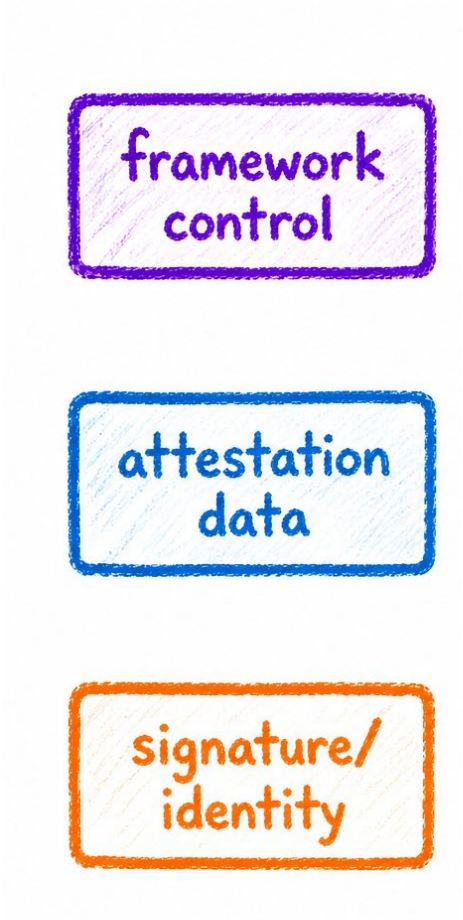
carabiner



carabiner

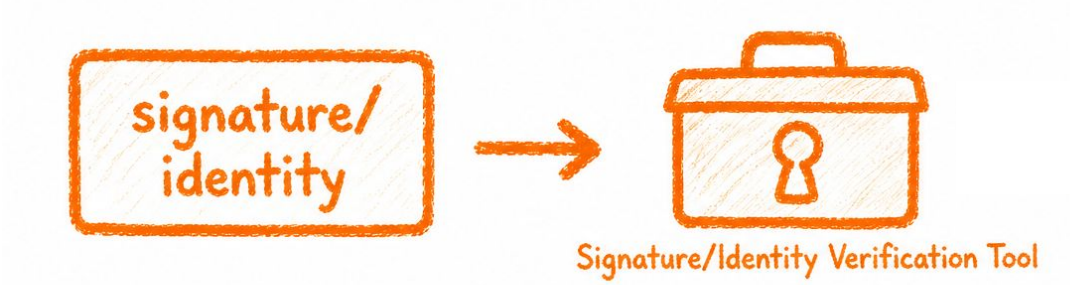


carabiner


framework control
attestation data
signature/ identity
Why?
What?
Who?

carabiner

carabiner


signature/
identity
Signature/Identity Verification Tool

carabiner


signature/
identity
Signature/Identity Verification Tool

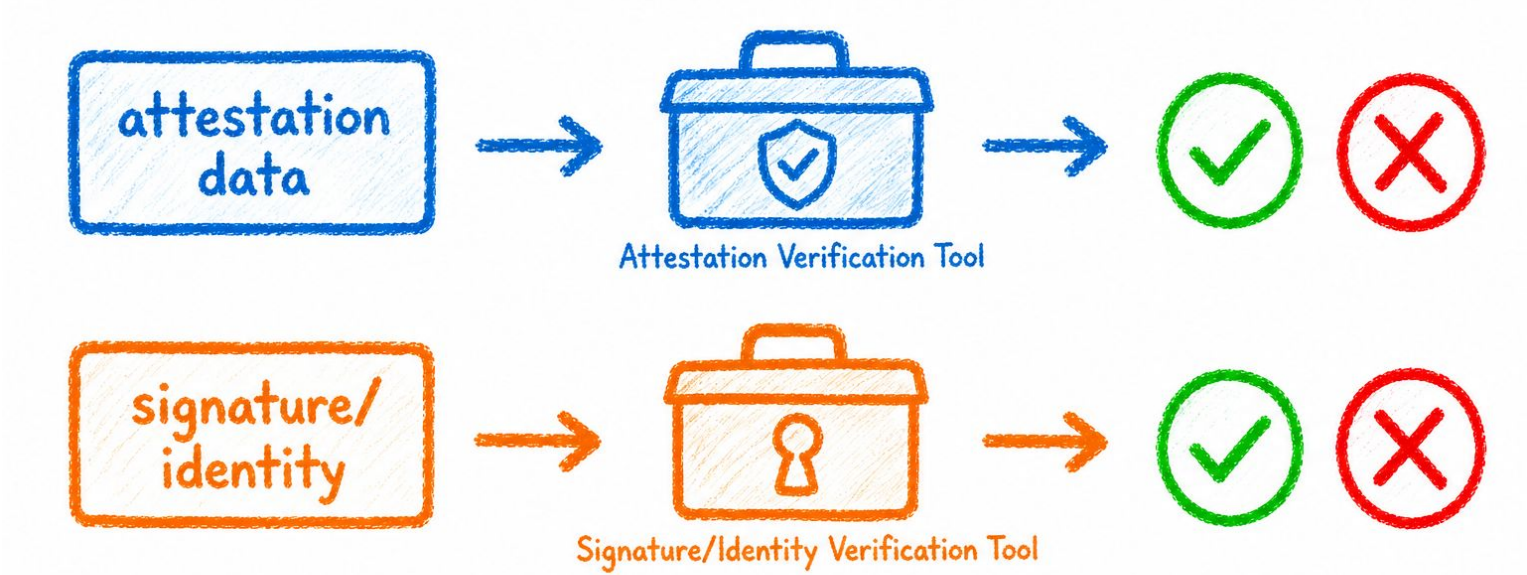
carabiner


attestation data
signature/ identity
Signature/Identity Verification Tool

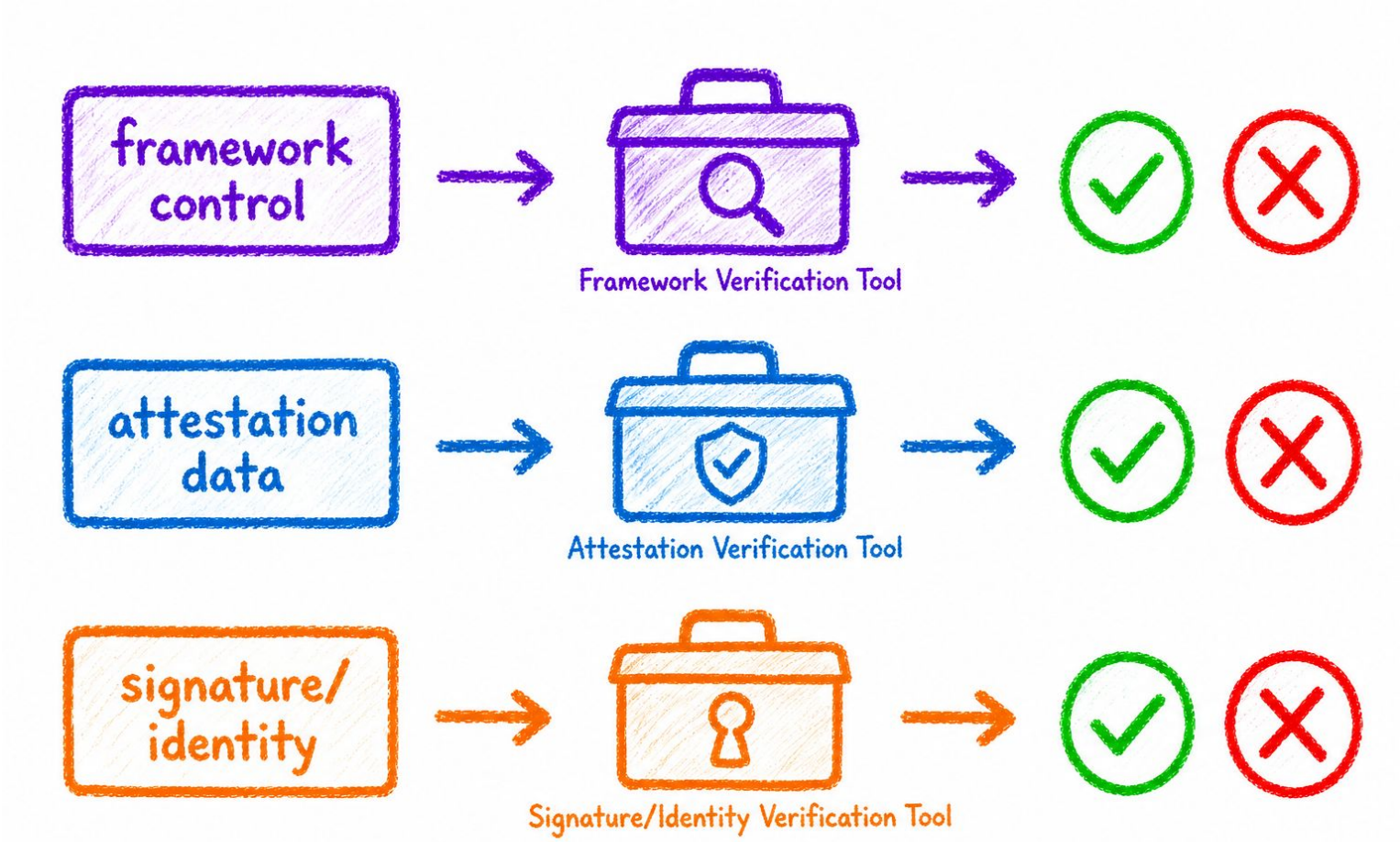
carabiner


attestation data
Attestation Verification Tool
signature/ identity
Signature/Identity Verification Tool

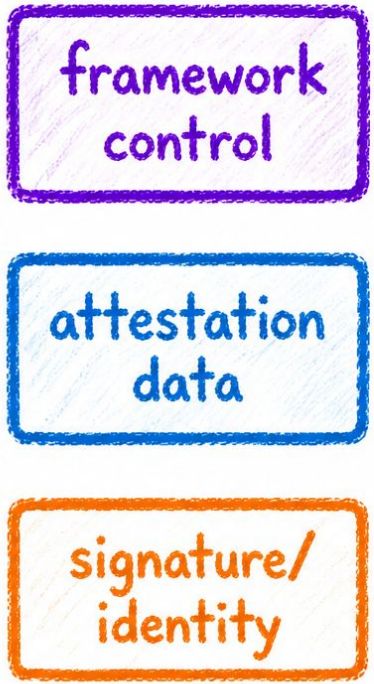
carabiner


attestation data
Attestation Verification Tool
signature/ identity
Signature/Identity Verification Tool

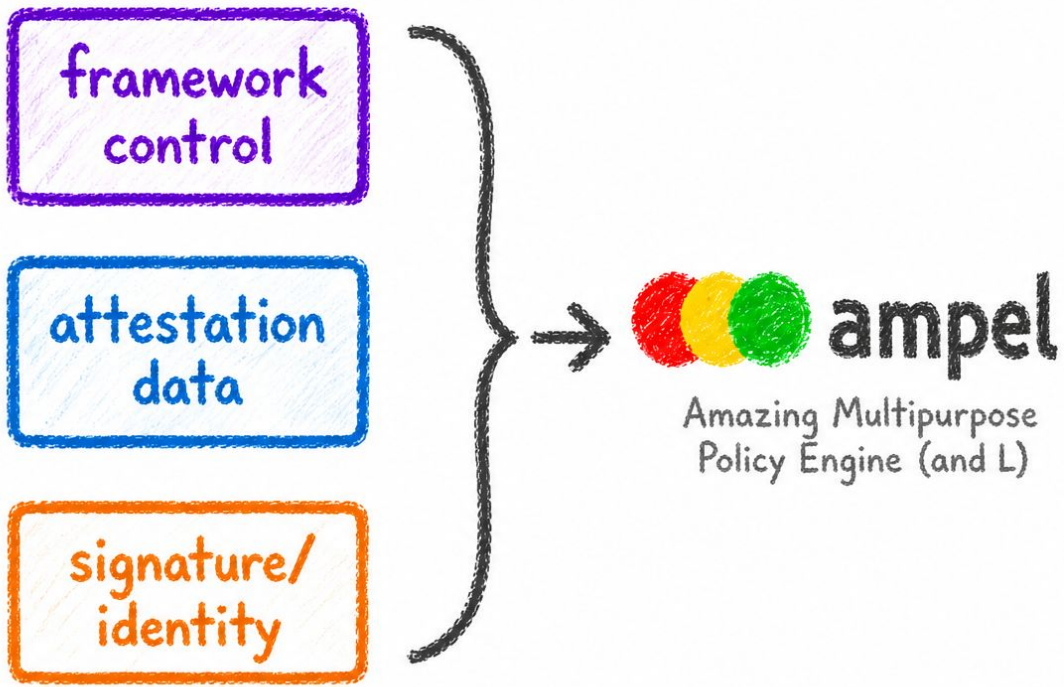
carabiner


framework control
Framework Verification Tool
attestation data
Attestation Verification Tool
signature/ identity
Signature/Identity Verification Tool

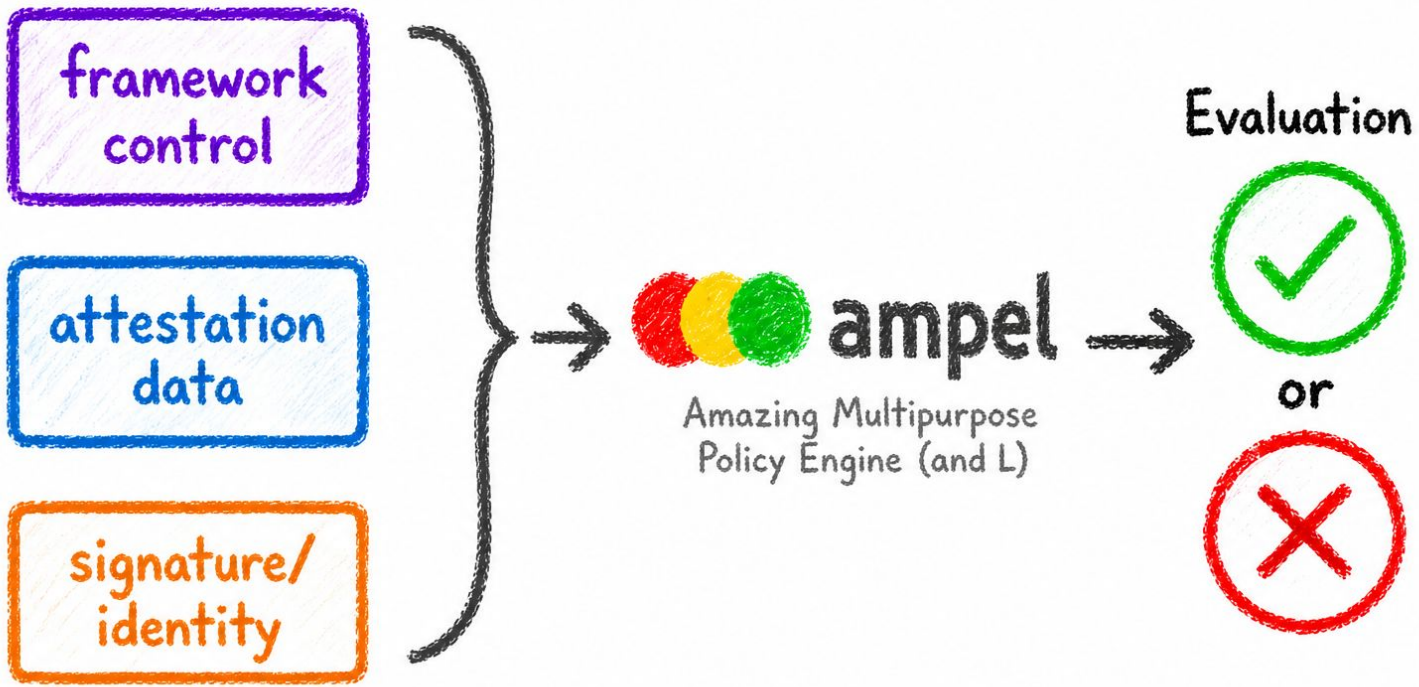
carabiner



carabiner


framework control
attestation data
signature/ identity
ampel
Amazing Multipurpose Policy Engine (and L)

carabiner

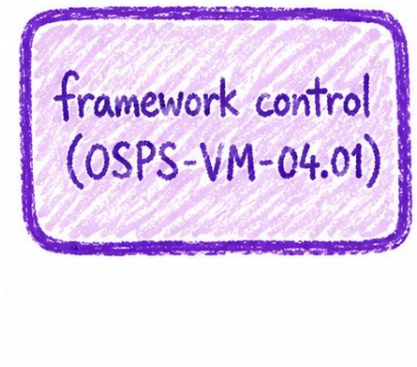

framework control
attestation data
signature/ identity
ampel
Amazing Multipurpose Policy Engine (and L)
Evaluation
or

carabiner

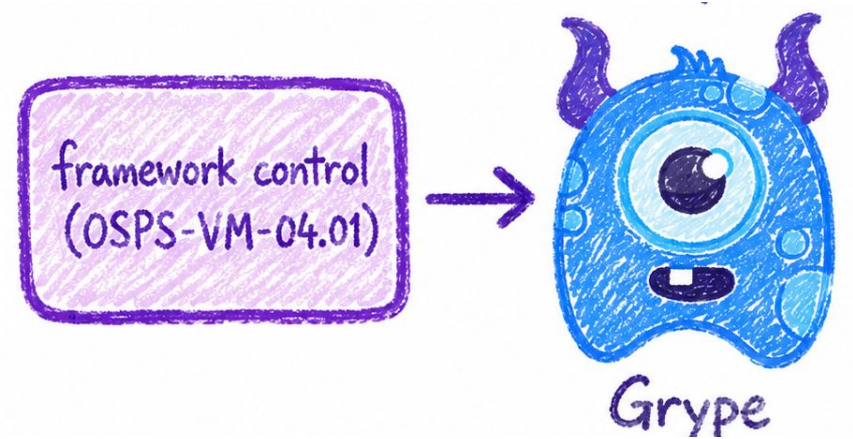
Implementation Diversity

Do what you want, not what they say

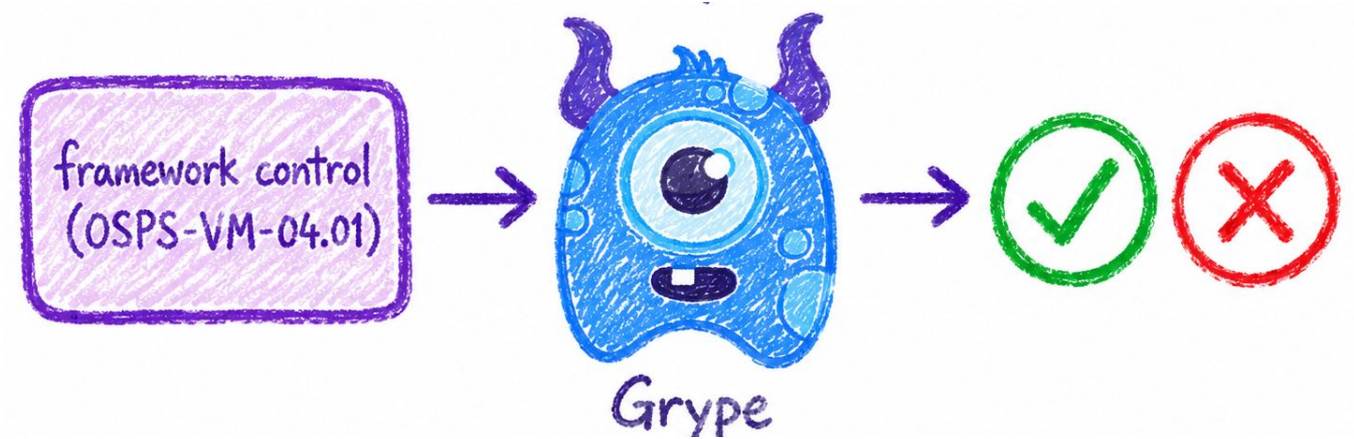
carabiner



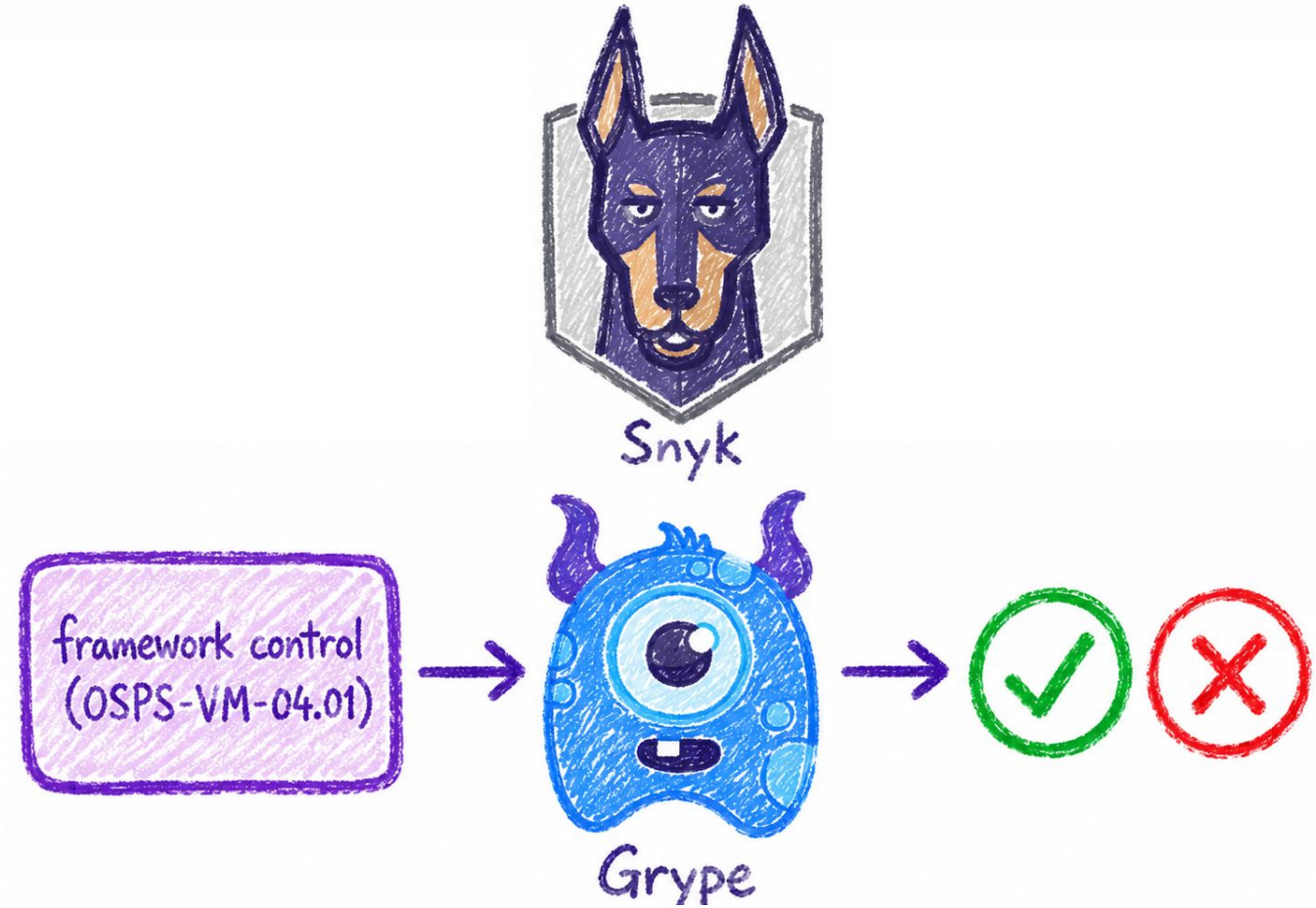
carabiner



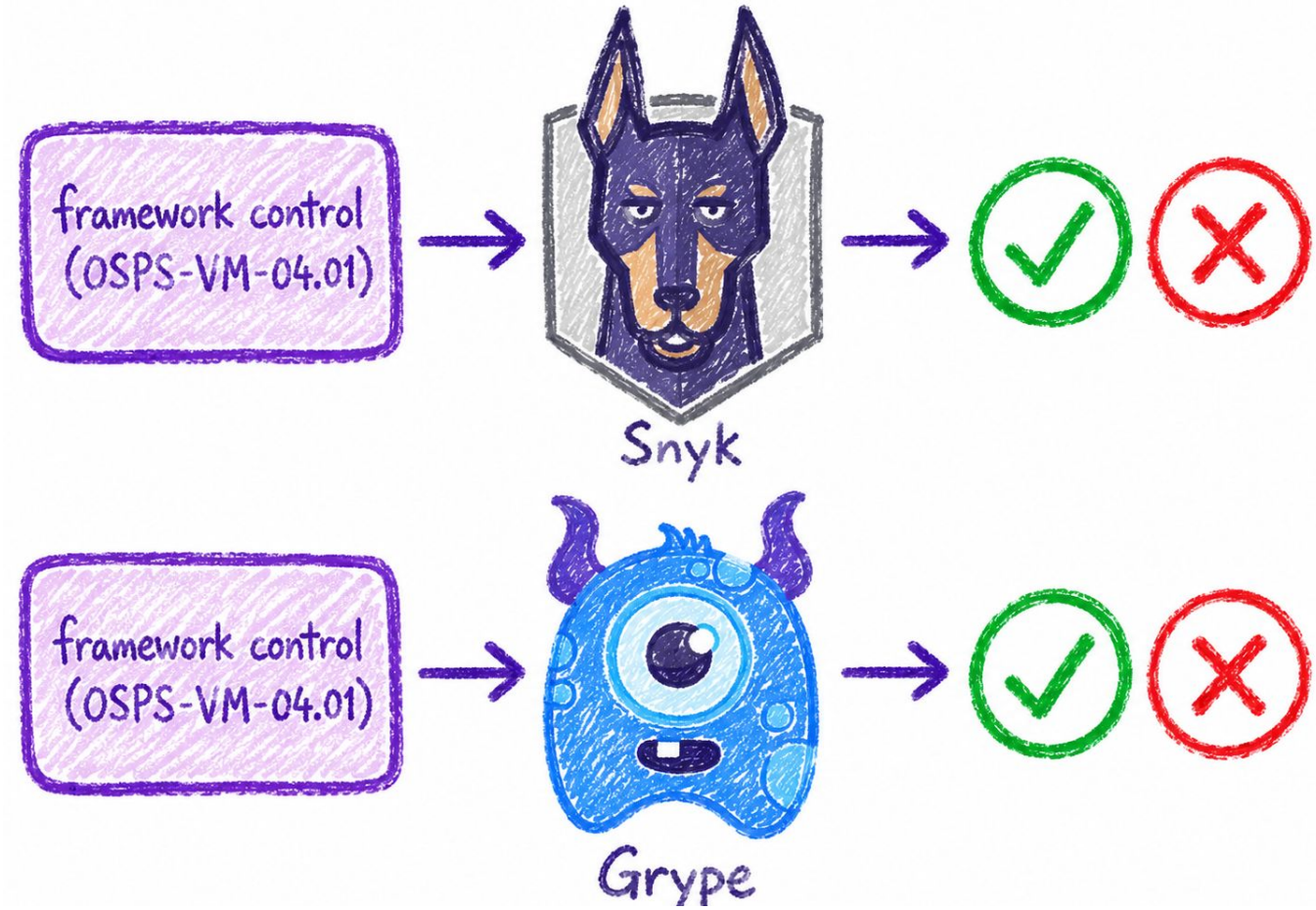
carabiner



carabiner



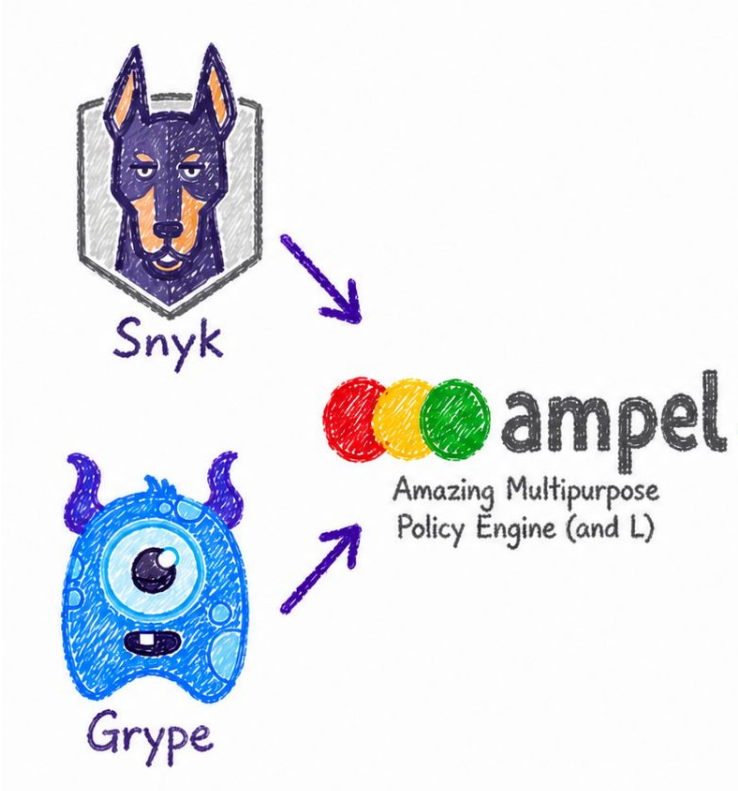
carabiner


framework control
(OSPS-VM-04.01)
Snyk
framework control
(OSPS-VM-04.01)
Grype

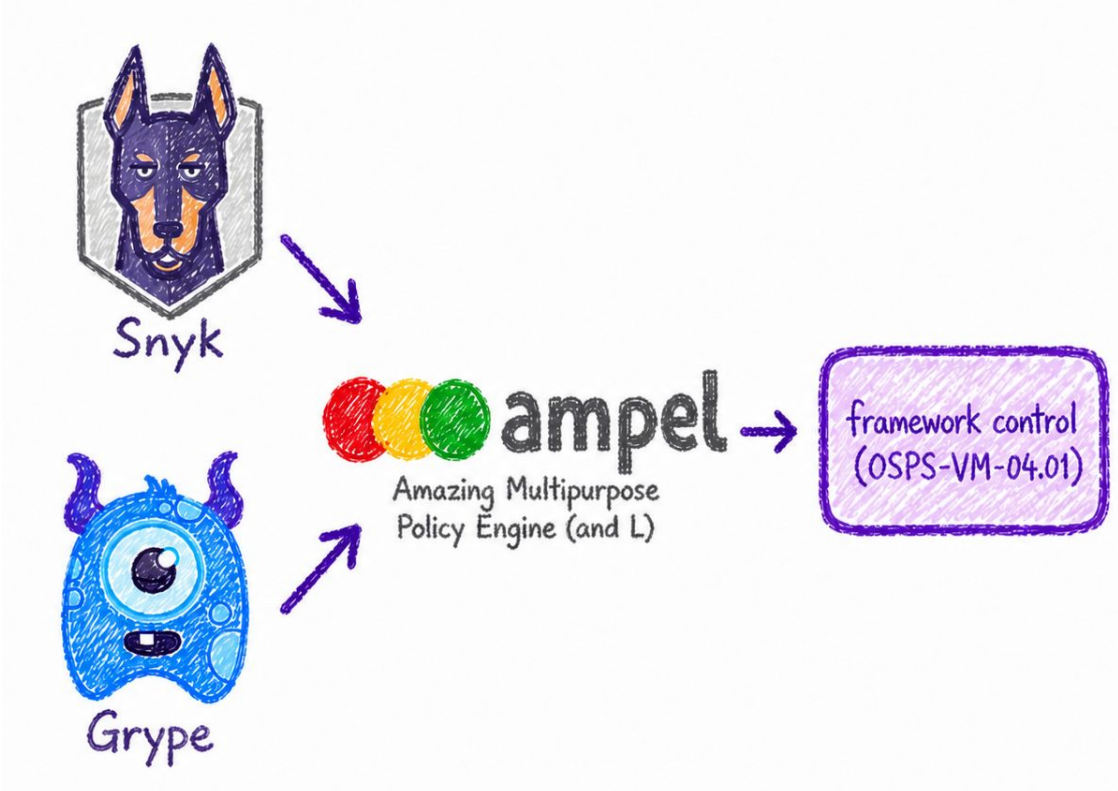
carabiner

carabiner

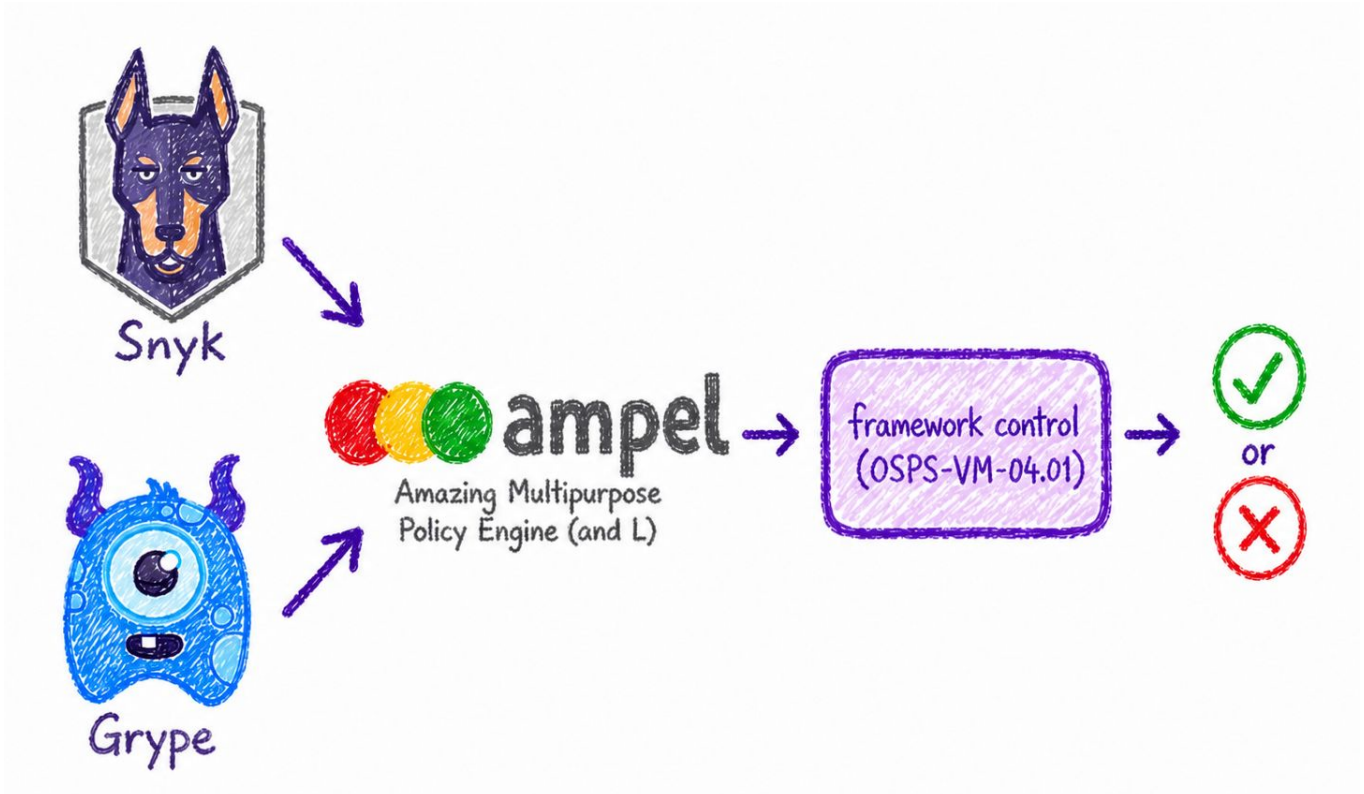
carabiner



carabiner


Snyk
Grype
ampel
Amazing Multipurpose
Policy Engine (and L)
framework control
(OSPS-VM-04.01)

carabiner

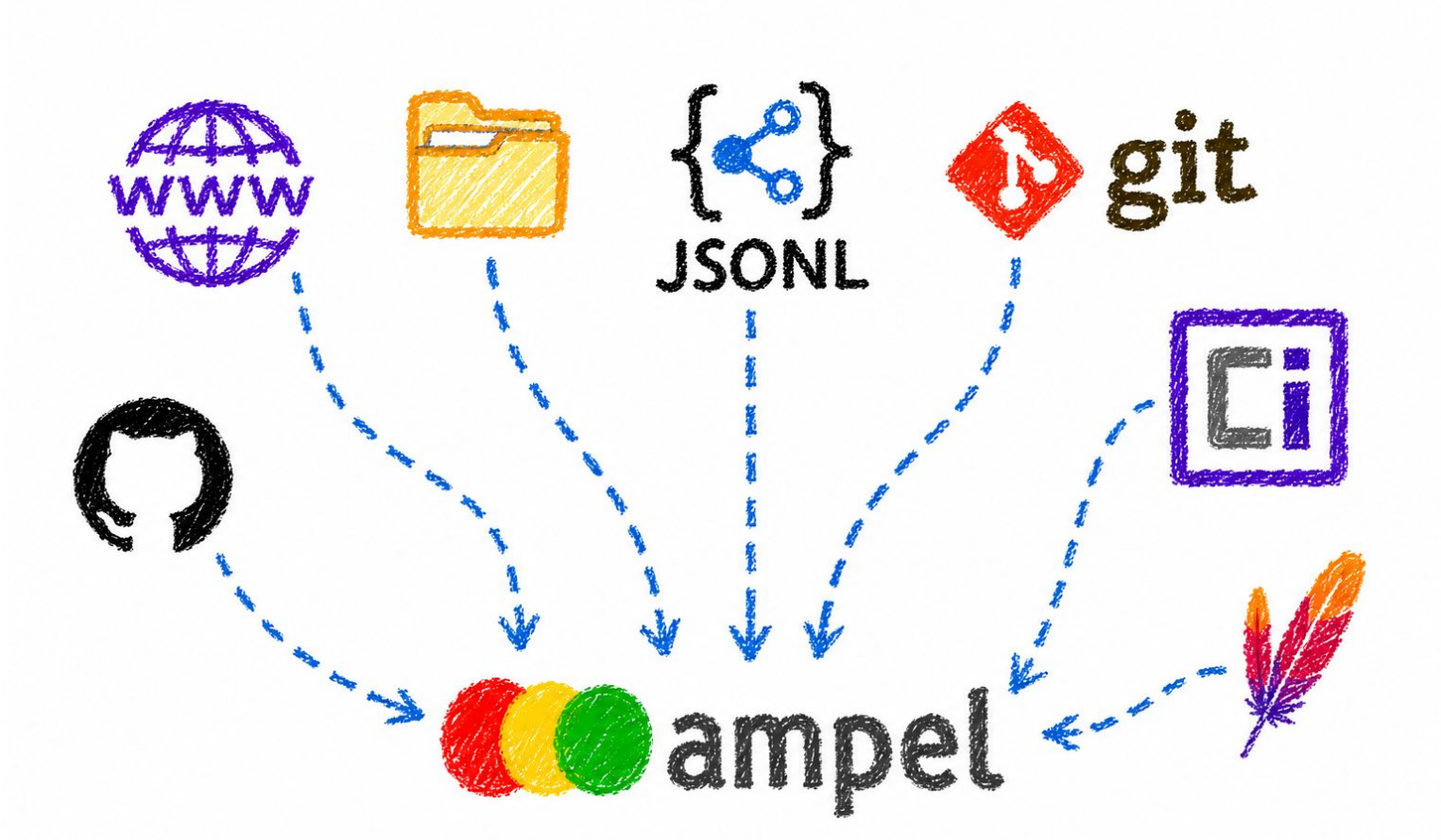

Snyk
Grype
ampel
Amazing Multipurpose
Policy Engine (and L)
framework control
(OSPS-VM-04.01)
or

carabiner

Evidence Discovery

There is no one source to rule them all :(

carabiner

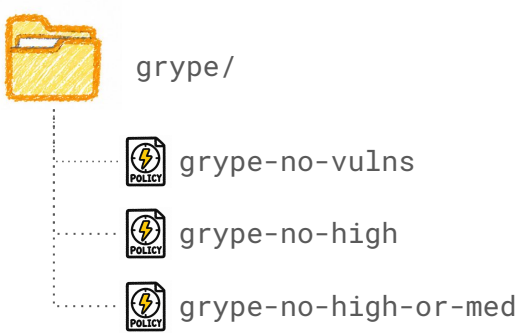


carabiner

Community Policies

Do it once. For everybody.

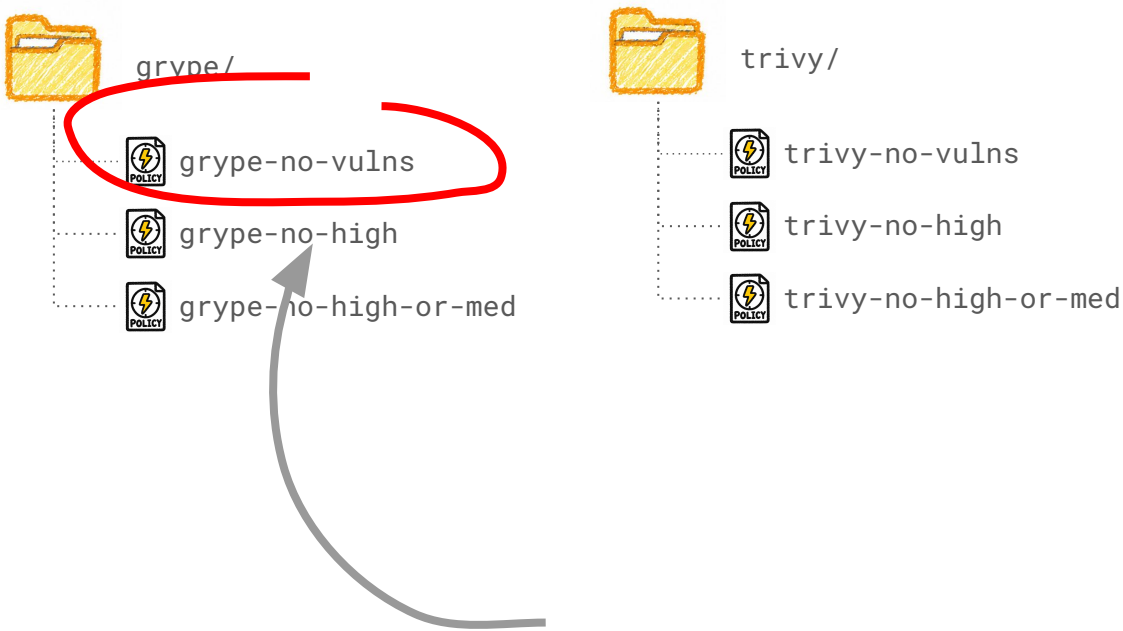
carabiner


grype/
grype-no-vulns
grype-no-high
grype-no-high-or-med


trivy/
trivy-no-vulns
trivy-no-high
trivy-no-high-or-med

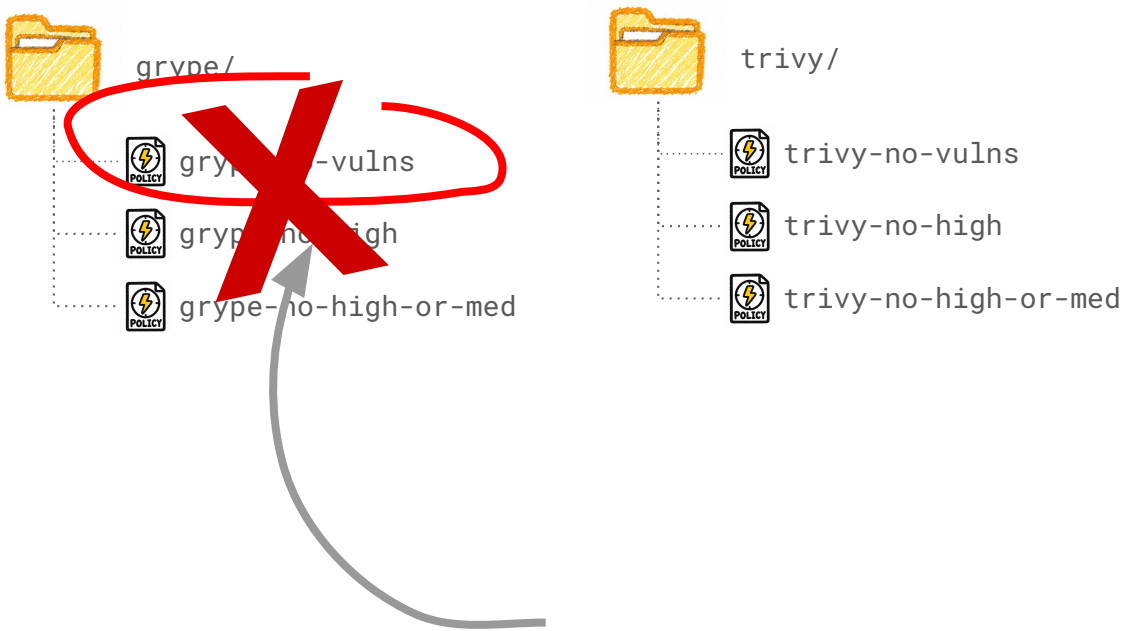

ampel

carabiner



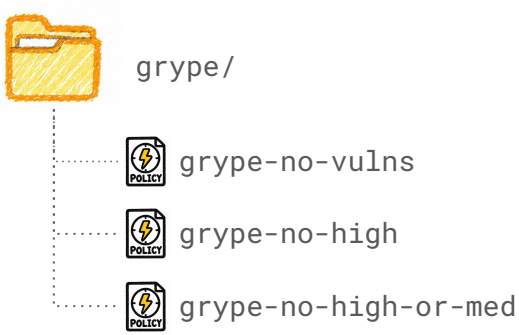
ampel

carabiner

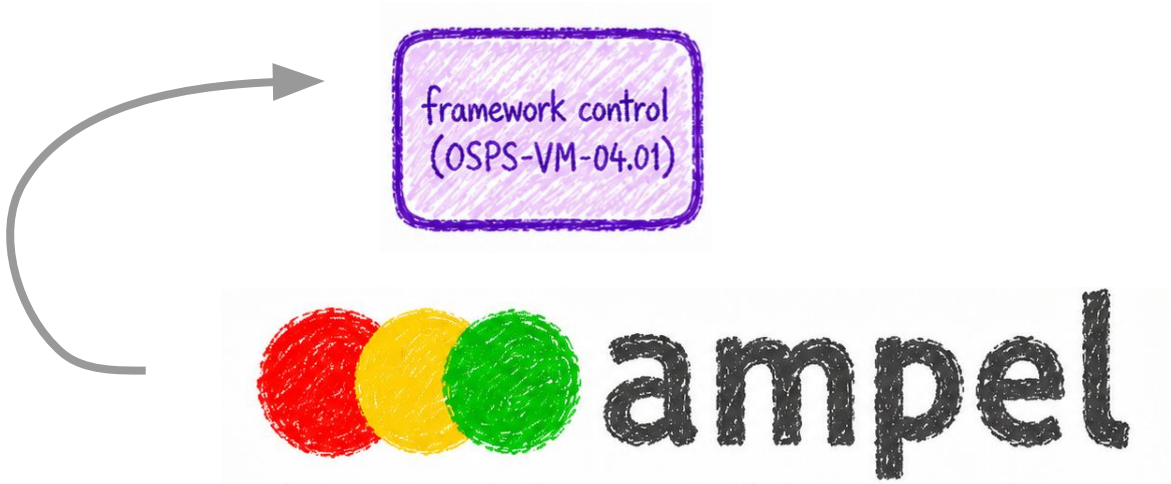


ampel

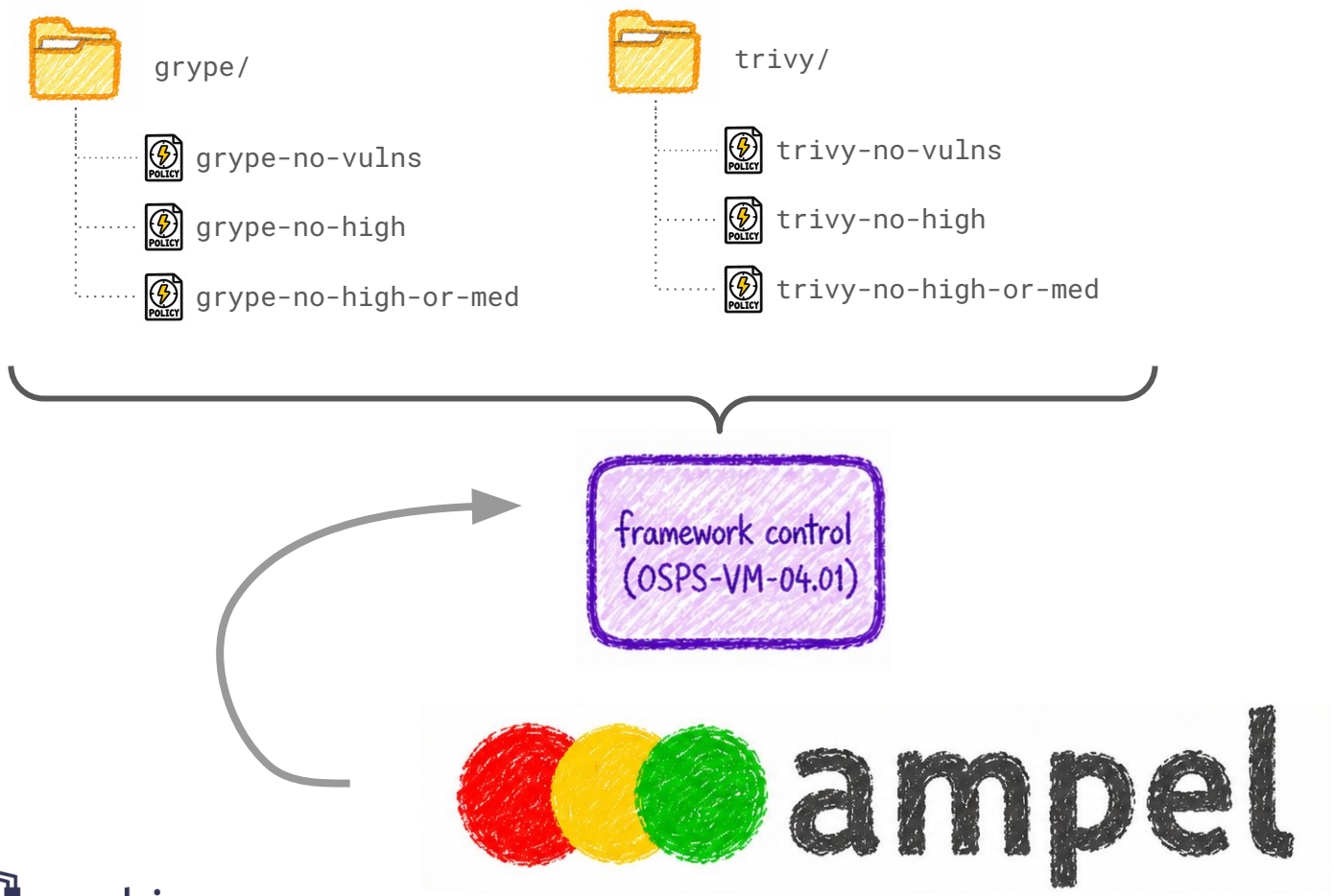
carabiner


grype/
grype-no-vulns
grype-no-high
grype-no-high-or-med

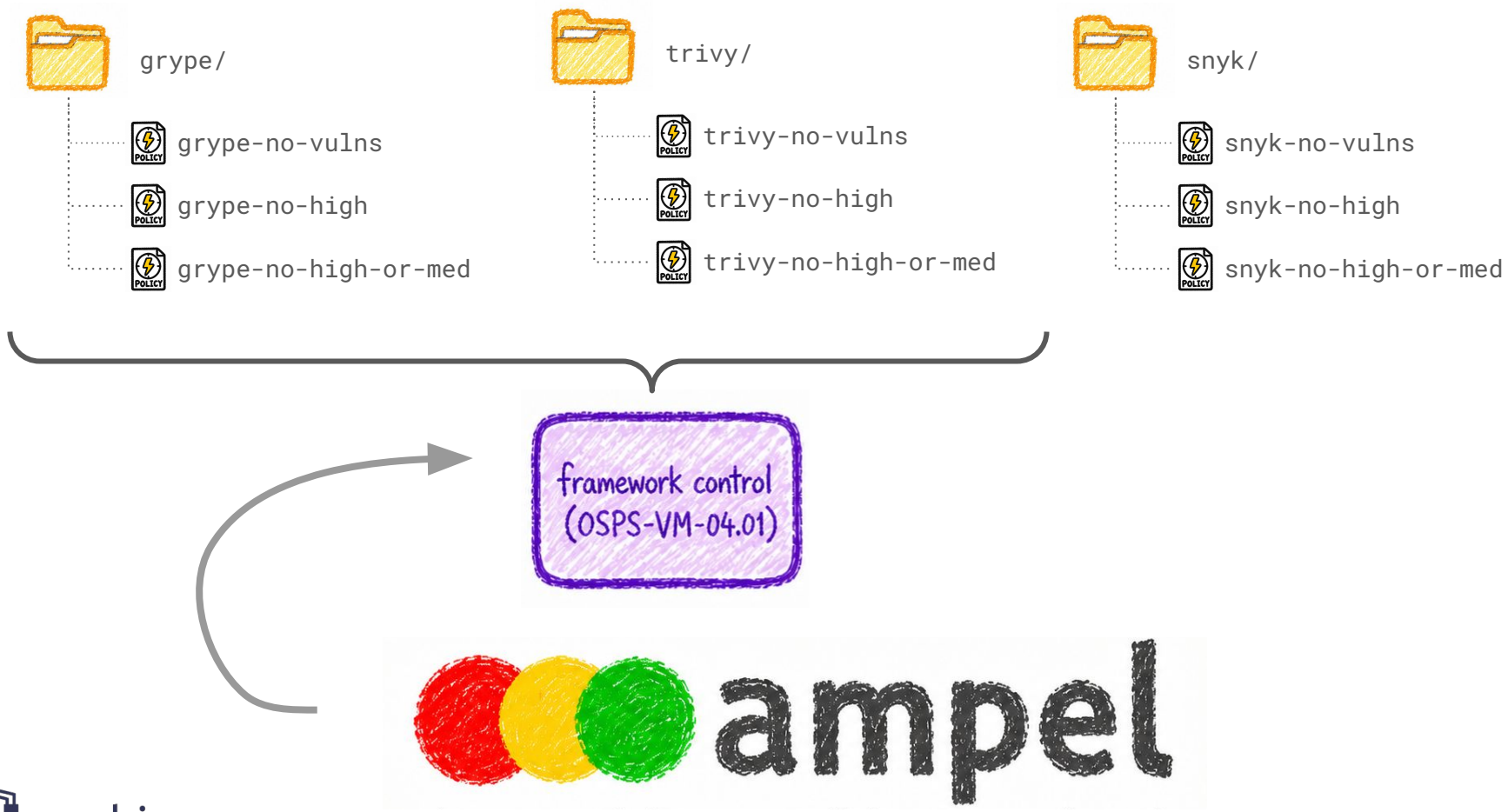

trivy/
trivy-no-vulns
trivy-no-high
trivy-no-high-or-med

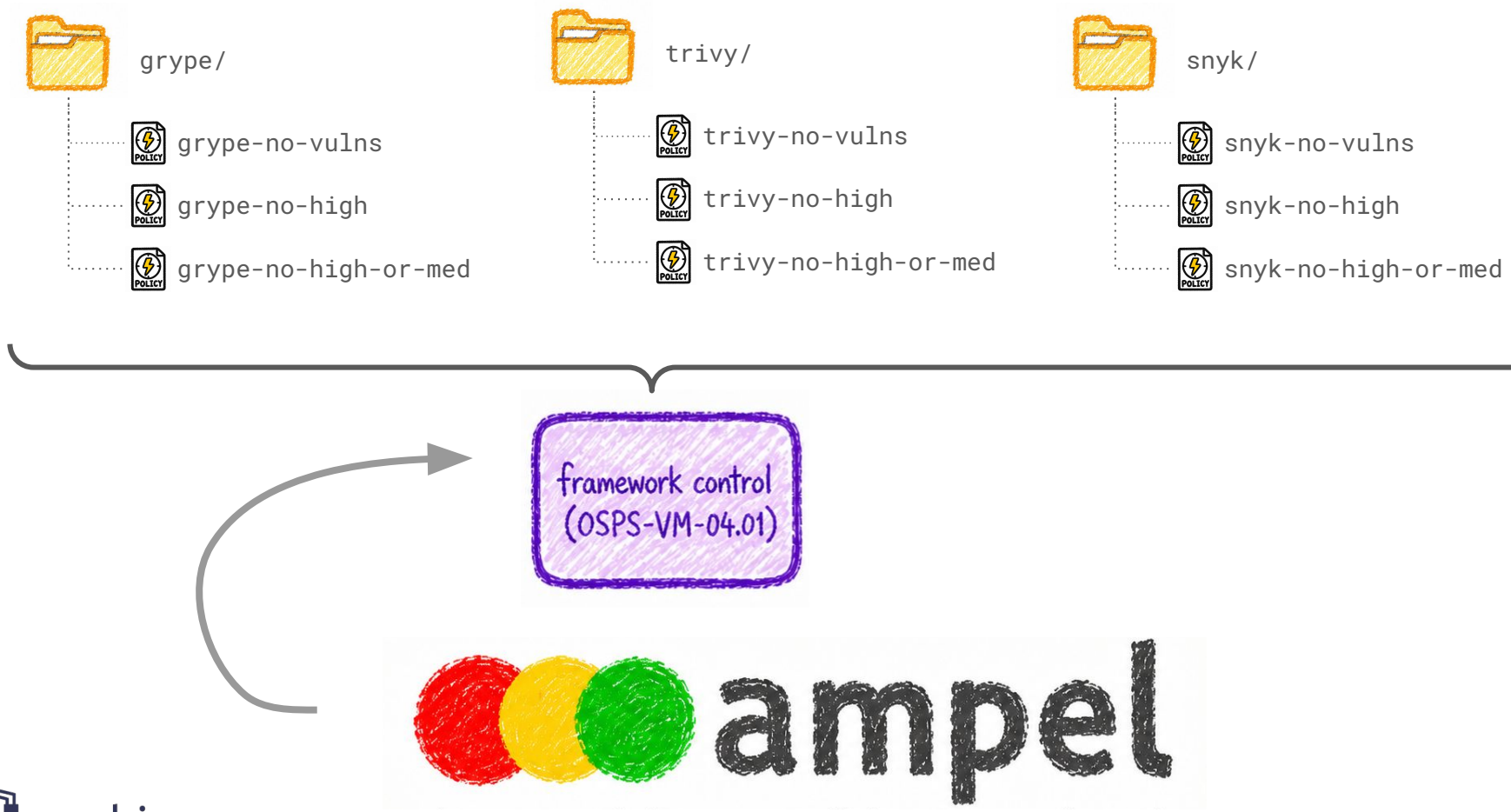

framework control
(OSPS-VM-04.01)
ampel

carabiner


grype/
grype-no-vulns
grype-no-high
grype-no-high-or-med
trivy/
trivy-no-vulns
trivy-no-high
trivy-no-high-or-med
framework control
(OSPS-VM-04.01)
ampel

carabiner


grype/
grype-no-vulns
grype-no-high
grype-no-high-or-med
trivy/
trivy-no-vulns
trivy-no-high
trivy-no-high-or-med
snyk/
snyk-no-vulns
snyk-no-high
snyk-no-high-or-med
framework control
(OSPS-VM-04.01)
ampel
carabiner


grype/
grype-no-vulns
grype-no-high
grype-no-high-or-med
trivy/
trivy-no-vulns
trivy-no-high
trivy-no-high-or-med
snyk/
snyk-no-vulns
snyk-no-high
snyk-no-high-or-med
framework control
(OSPS-VM-04.01)
ampel
carabiner

Let me show you >>>

carabiner

OK, but why?

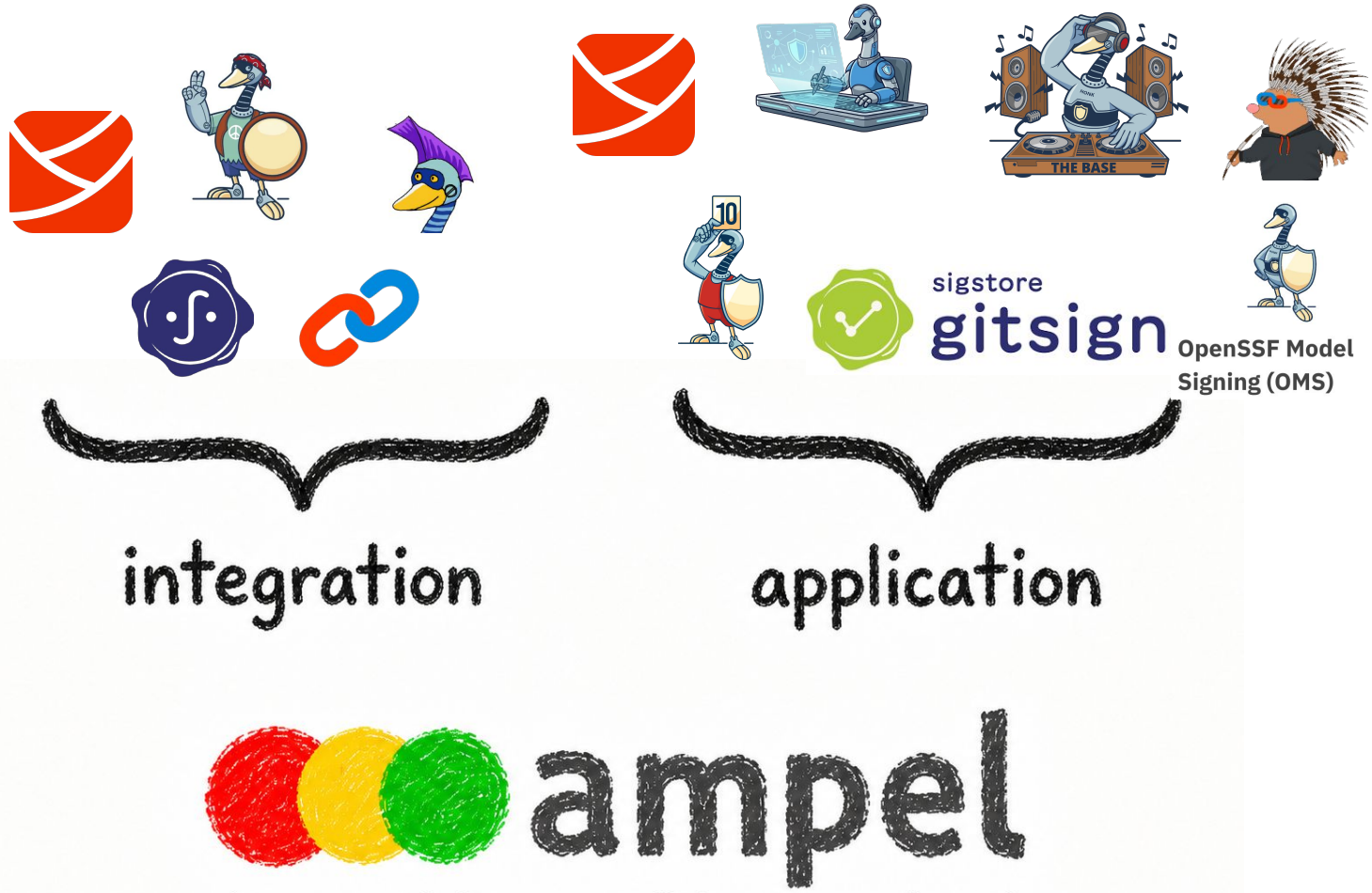
Here's why.

carabiner

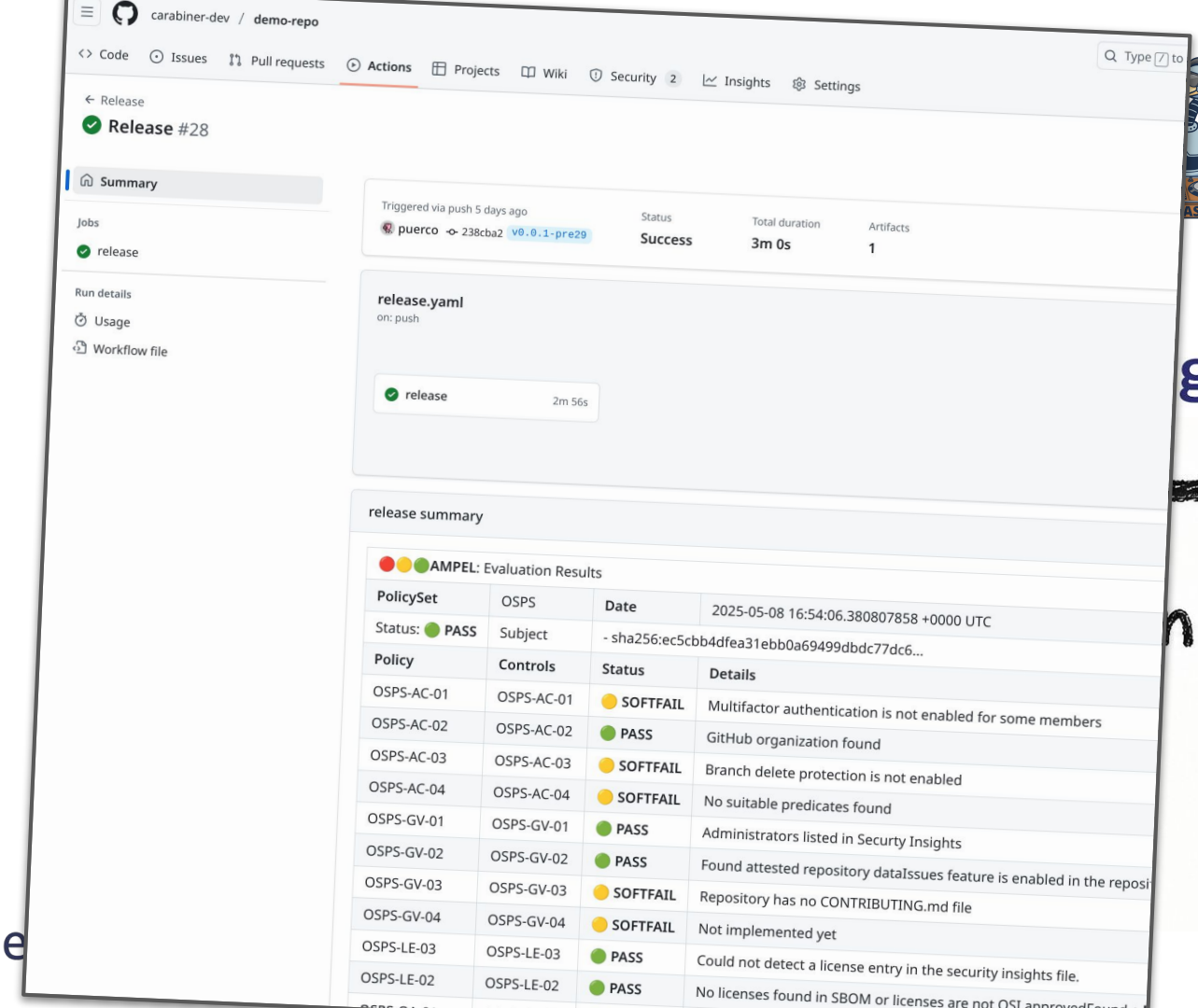
integration

ampel

carabiner


THE BASE
10
sigstore
gitsign
OpenSSF Model Signing (OMS)
integration
application
ampel

carabiner



gn OpenSSF Model Signing (OMS)

carabiner

But oh, look 👀

It’s a whole mini-ecosystem!

carabiner

ampel

Amazing Multipurpose Policy Engine (and L)

libraries utilities

carabiner

Thank you!

carabiner

Thank you!

https://github.com/carabiner-dev/ampel

Adolfo García Veytia
@puerco

carabiner