Grafeas and in-toto

Completely Securing The Software Supply Chain

Wendy Dembowski
Google

Lukas Pühringer
NYU | TANDON SCHOOL OF ENGINEERING

Grafeas

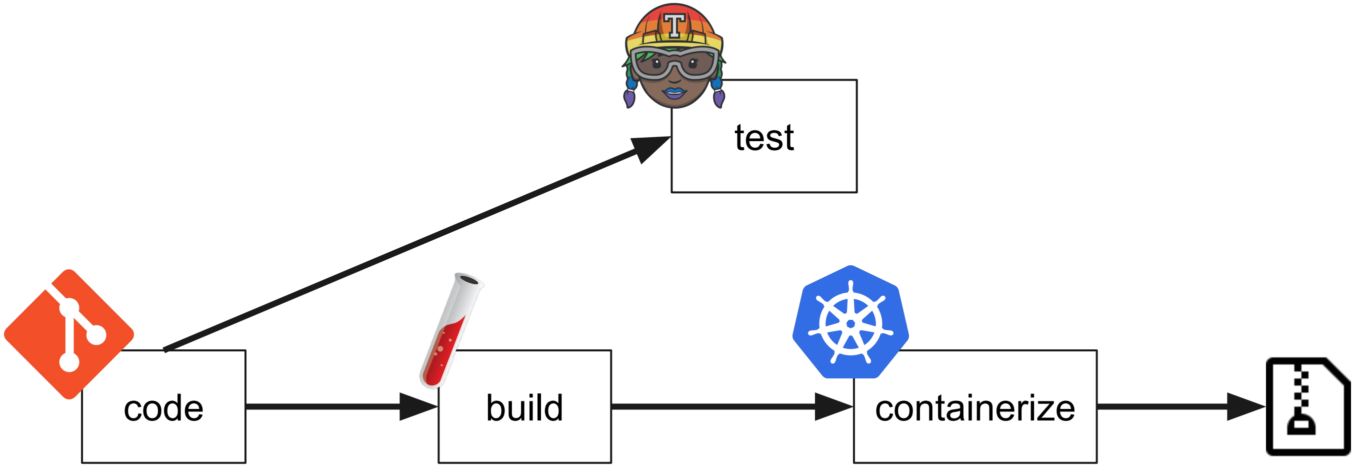
A CI/CD Artifact Metadata Storage And Signing For Cloud Applications

in-toto

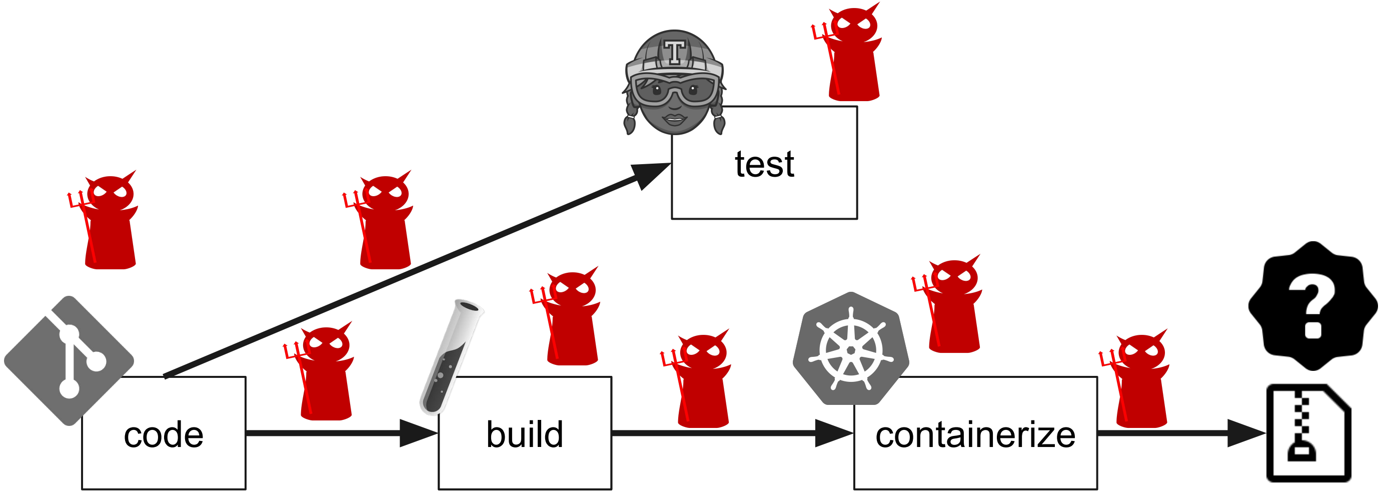
A Framework To Provide Integrity And Authenticity Of All The Steps Performed To Make Software

How Is Software Made?

A Stylized Software Supply Chain

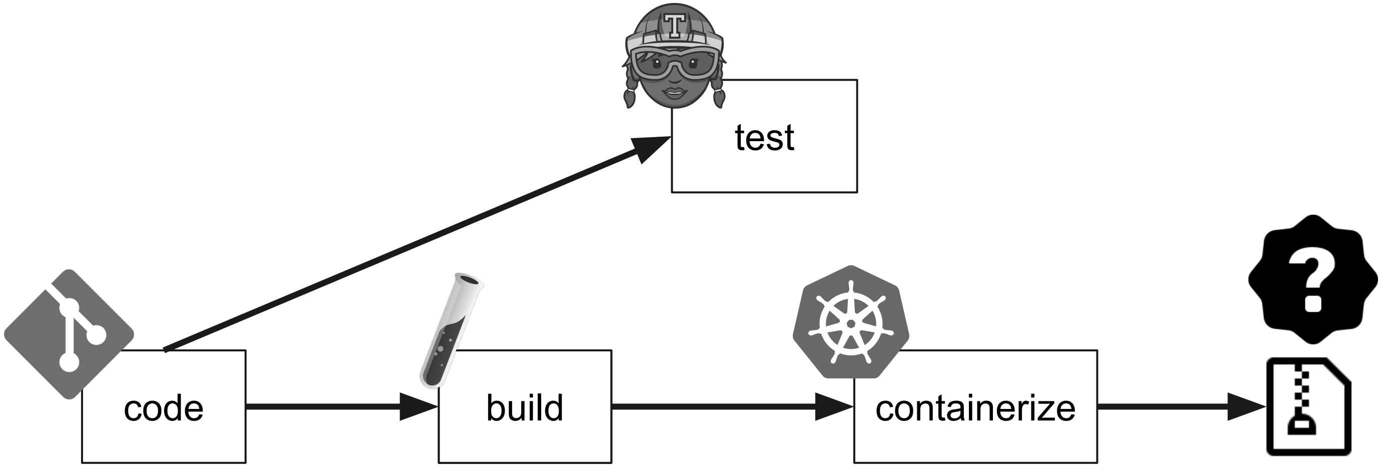


Attackers Can Hack The Software Supply Chain



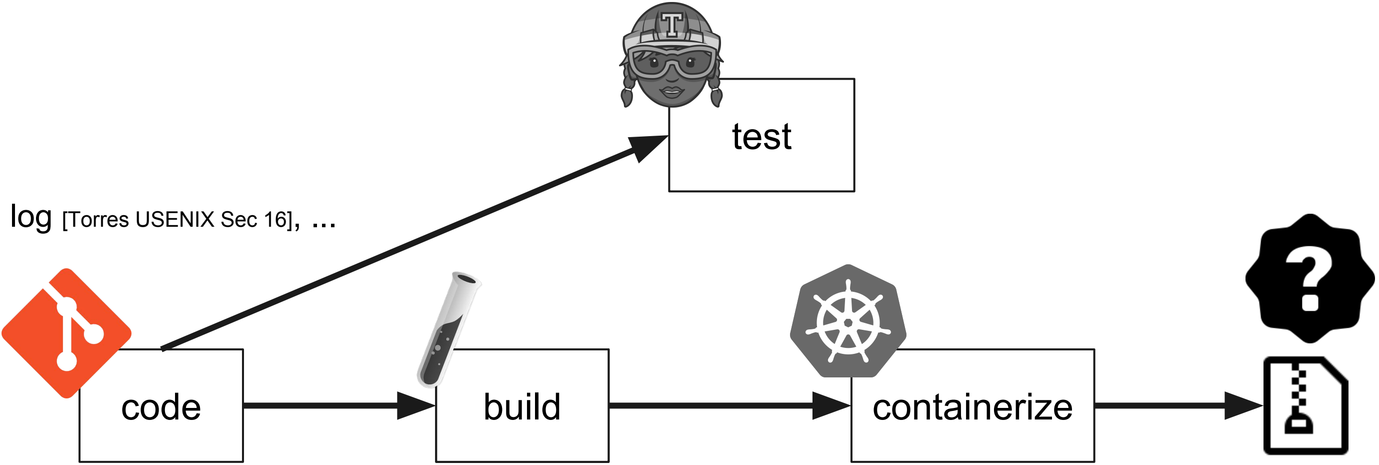
How Can We Fix This?

Many Good Point Solutions



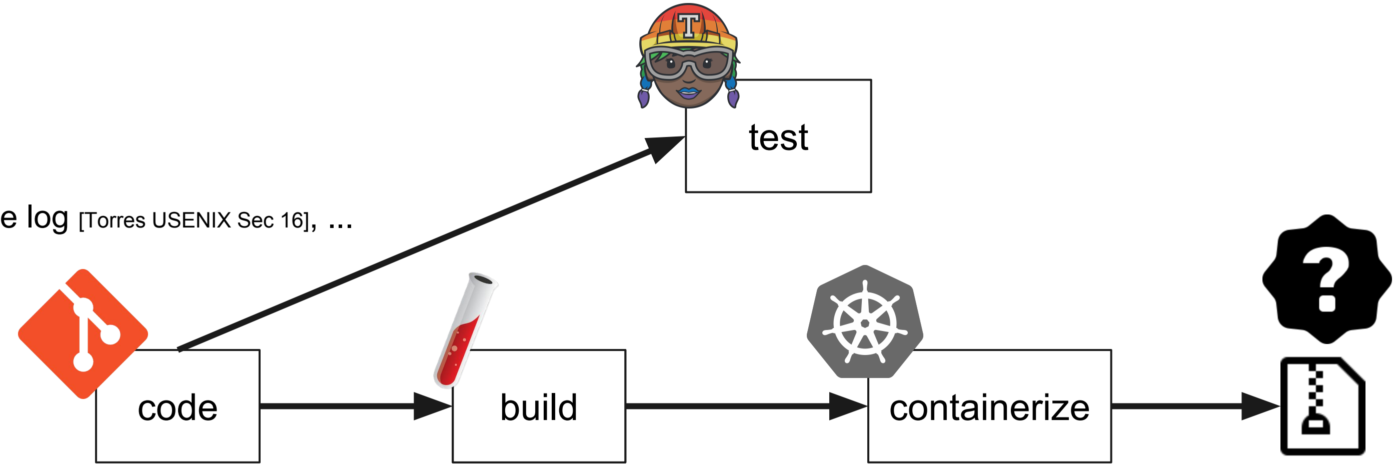
Many Good Point Solutions

→ git signing,
reference state log [Torres USENIX Sec 16], ...



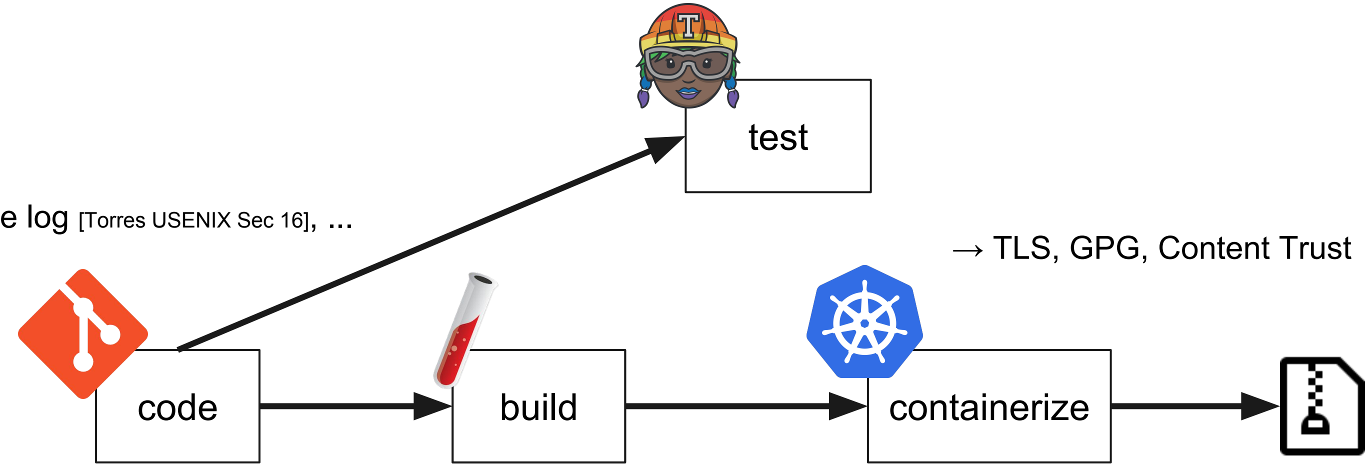
Many Good Point Solutions

→ git signing,
reference state log [Torres USENIX Sec 16], ...



→ TPMs, HSMs, reproducible builds, ...

Many Good Point Solutions



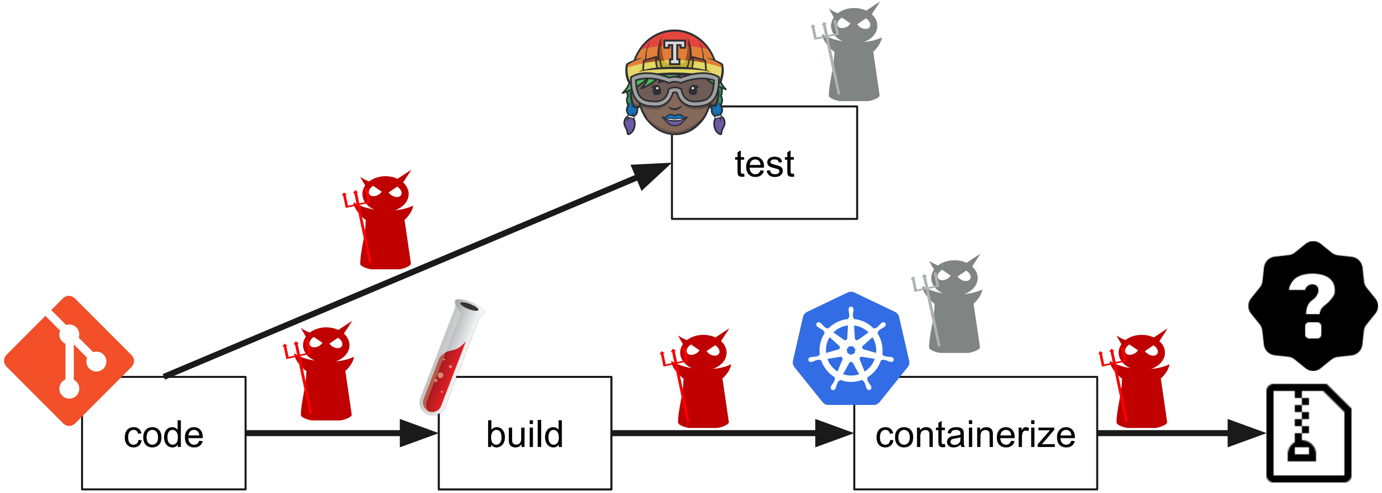
→ git signing,
reference state log [Torres USENIX Sec 16], ...

→ TLS, GPG, Content Trust

→ TPMs, HSMs, reproducible builds, ...

Fixed?

Gaps Between Steps? Compliance?



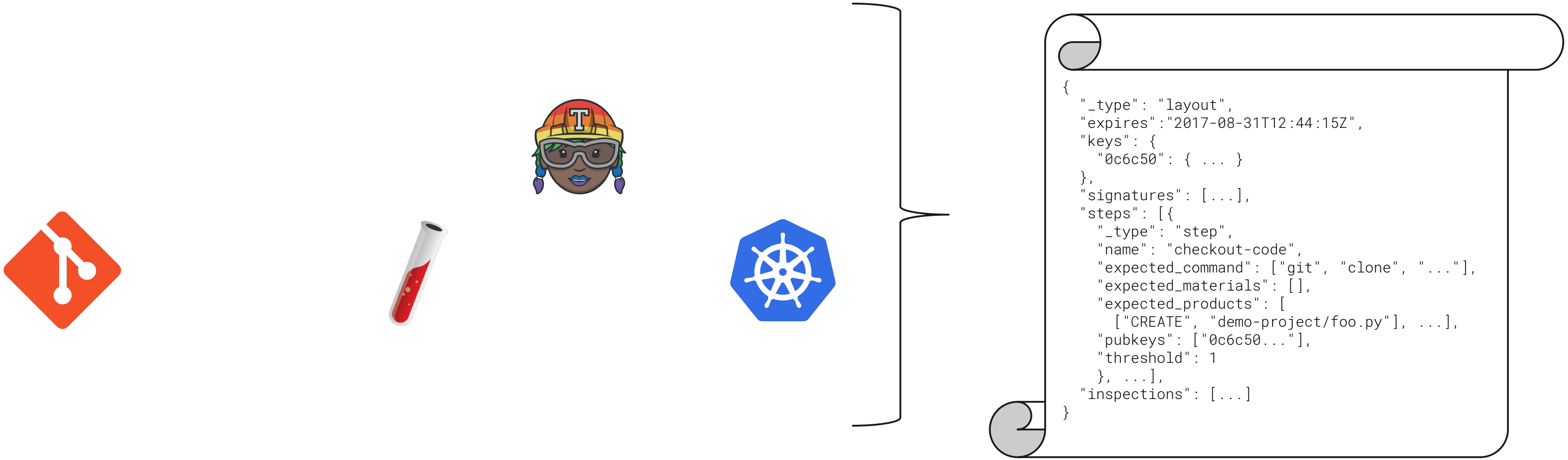
We Want To Secure The Complete Software Supply Chain!

→ Verifiably define the steps of the software supply chain

→ Verifiably define the authorized actors

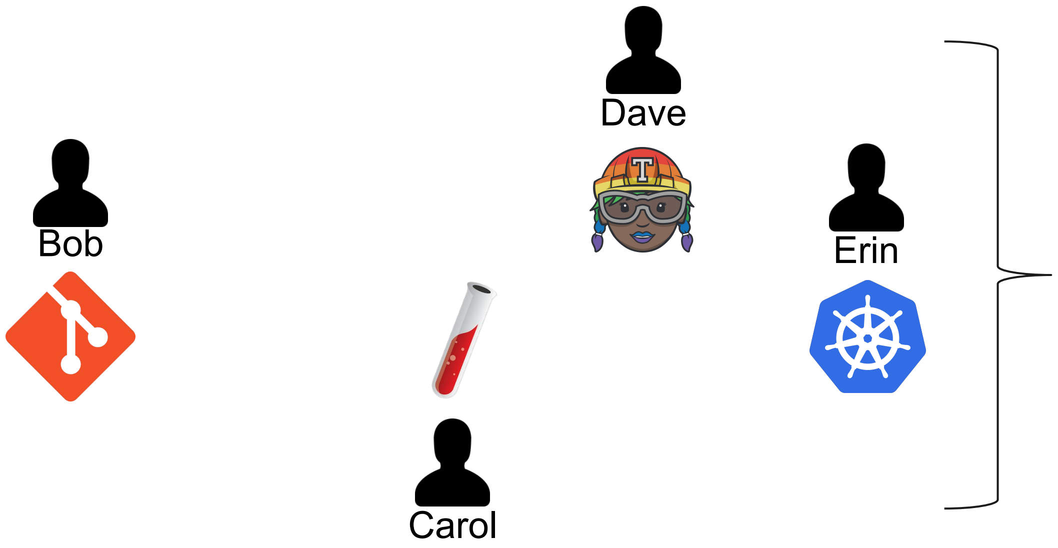
→ Guarantee that everything happens according to definition, and nothing else

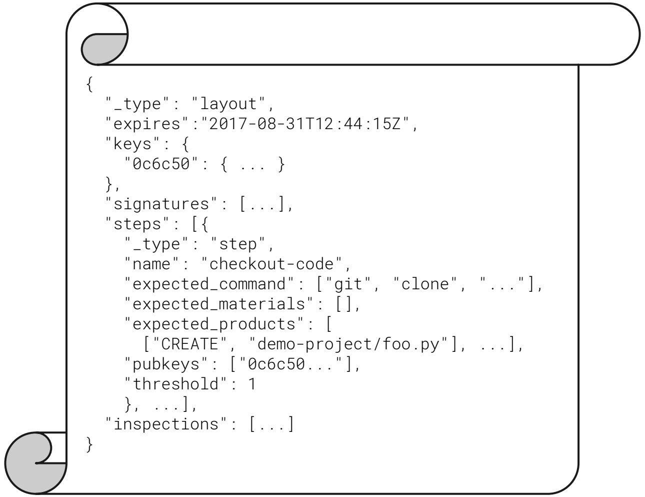
in-toto -- Project Definition -- Steps



```
{
  "_type": "layout",
  "expires":"2017-08-31T12:44:15Z",
  "keys": {
    "0c6c50": { ... }
  },
  "signatures": [...],
  "steps": [{
    "_type": "step",
    "name": "checkout-code",
    "expected_command": ["git", "clone", "..."],
    "expected_materials": [],
    "expected_products": [
      ["CREATE", "demo-project/foo.py"], ...],
    "pubkeys": ["0c6c50..."],
    "threshold": 1
    }, ...],
  "inspections": [...]
}
```

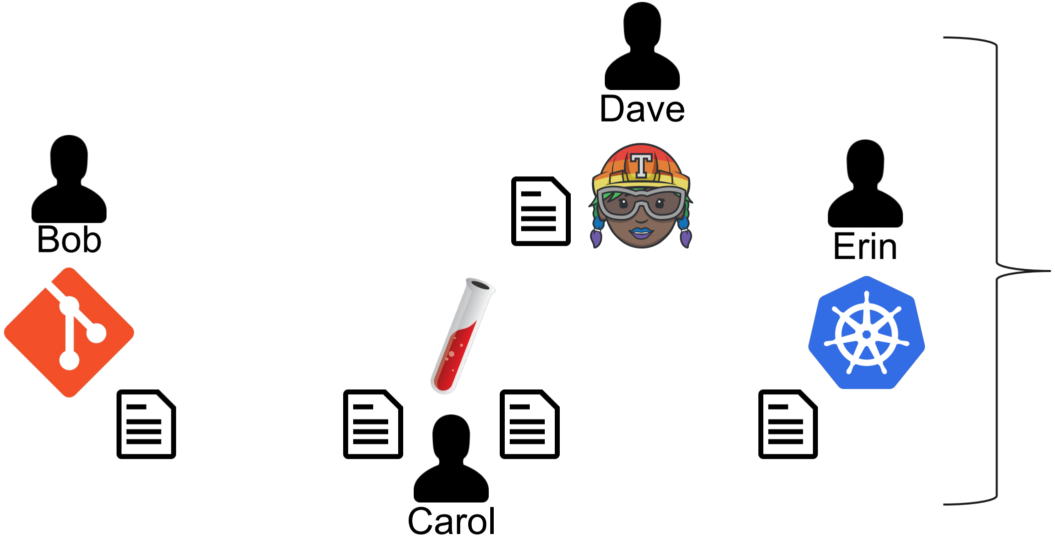
in-toto -- Project Definition -- Functionaries

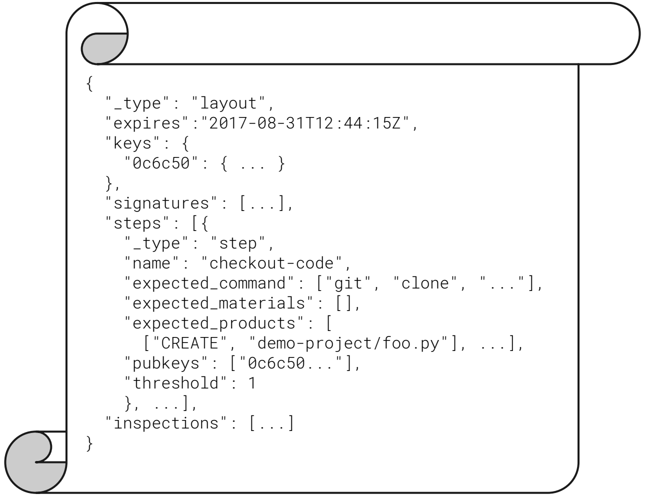




```
{
  "_type": "layout",
  "expires":"2017-08-31T12:44:15Z",
  "keys": {
    "0c6c50": { ... }
  },
  "signatures": [...],
  "steps": [{
    "_type": "step",
    "name": "checkout-code",
    "expected_command": ["git", "clone", "..."],
    "expected_materials": [],
    "expected_products": [
      ["CREATE", "demo-project/foo.py"], ...],
    "pubkeys": ["0c6c50..."],
    "threshold": 1
    }, ...],
  "inspections": [...]
}
```

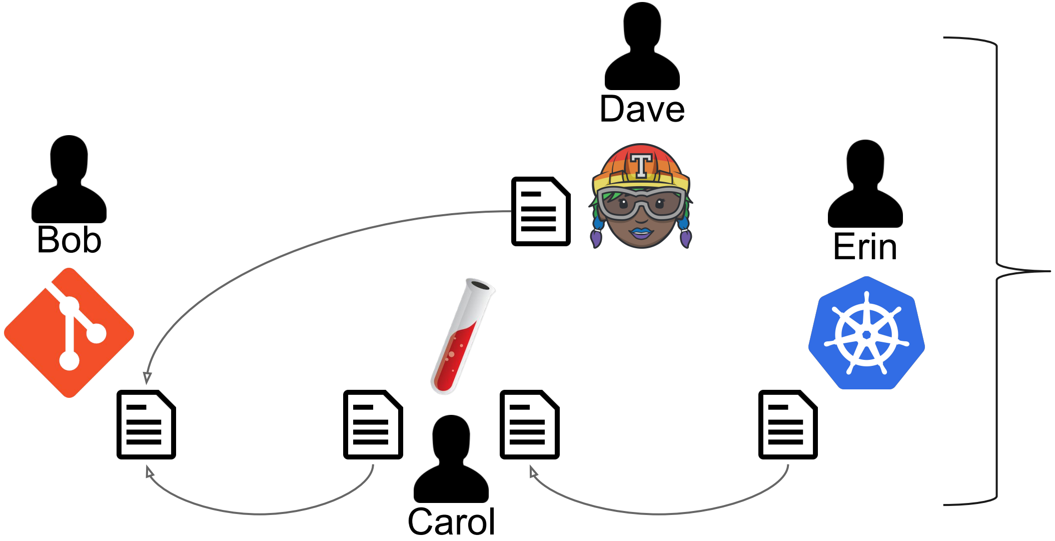
in-toto -- Project Definition -- Materials/Products

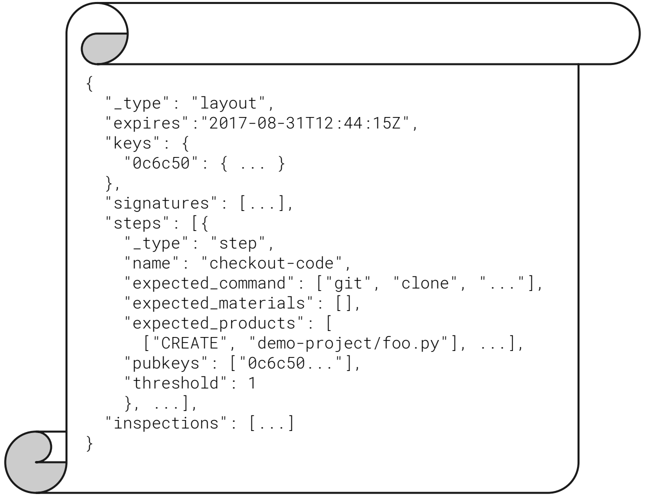




```
{
  "_type": "layout",
  "expires":"2017-08-31T12:44:15Z",
  "keys": {
    "0c6c50": { ... }
  },
  "signatures": [...],
  "steps": [{
    "_type": "step",
    "name": "checkout-code",
    "expected_command": ["git", "clone", "..."],
    "expected_materials": [],
    "expected_products": [
      ["CREATE", "demo-project/foo.py"], ...],
    "pubkeys": ["0c6c50..."],
    "threshold": 1
    }, ...],
  "inspections": [...]
}
```

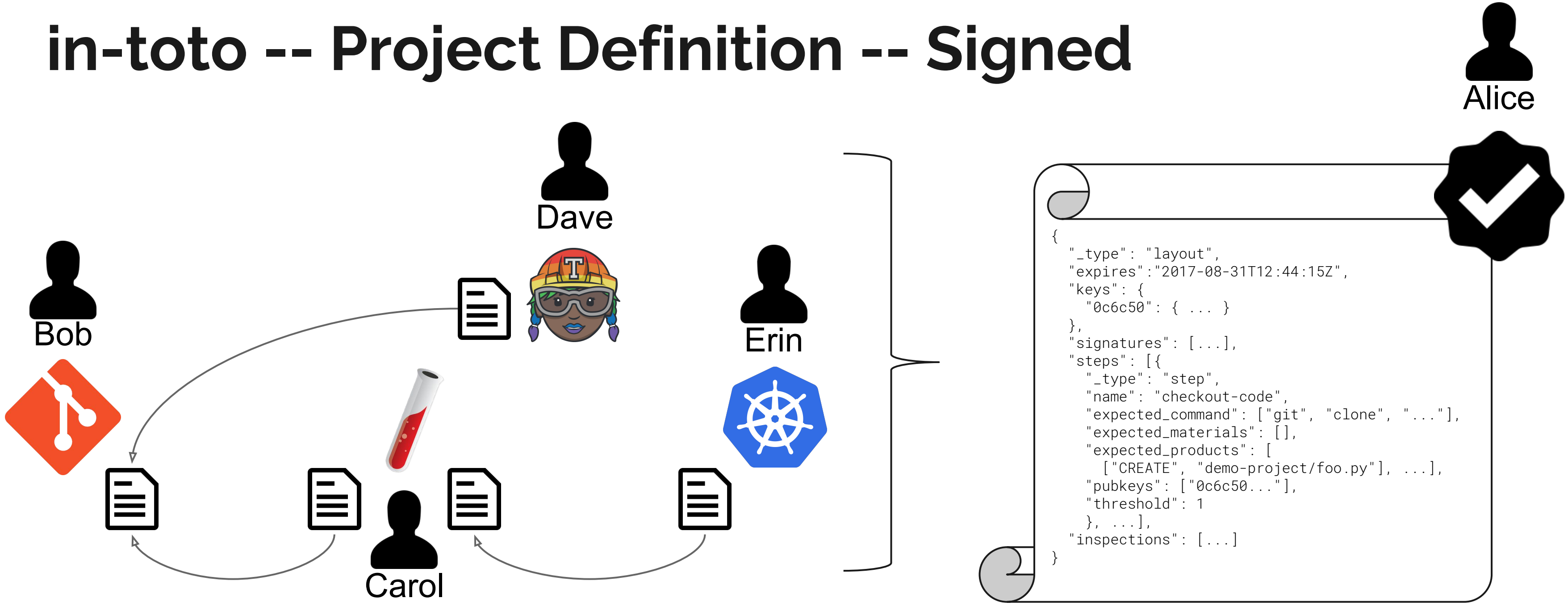
in-toto -- Project Definition -- Rules





```
{
  "_type": "layout",
  "expires":"2017-08-31T12:44:15Z",
  "keys": {
    "0c6c50": { ... }
  },
  "signatures": [...],
  "steps": [{
    "_type": "step",
    "name": "checkout-code",
    "expected_command": ["git", "clone", "..."],
    "expected_materials": [],
    "expected_products": [
      ["CREATE", "demo-project/foo.py"], ...],
    "pubkeys": ["0c6c50..."],
    "threshold": 1
    }, ...],
  "inspections": [...]
}
```

in-toto -- Project Definition -- Signed



```
{
  "_type": "layout",
  "expires":"2017-08-31T12:44:15Z",
  "keys": {
    "0c6c50": { ... }
  },
  "signatures": [...],
  "steps": [{
    "_type": "step",
    "name": "checkout-code",
    "expected_command": ["git", "clone", "..."],
    "expected_materials": [],
    "expected_products": [
      ["CREATE", "demo-project/foo.py"], ...],
    "pubkeys": ["0c6c50..."],
    "threshold": 1
    }, ...],
  "inspections": [...]
}
```

in-toto -- Signed Evidence For Each Step

```
$ in-toto-run [opts] -- ./do-the-supply-chain-step
```

```
{
  "_type": "Link",
  "name": "code",
  "byproducts":
{"stderr": "", "stdout":
"",
"return_value": 0
},
  "command": [...],
  "materials": {},
  "products": {
    "foo": {"sha256":
"..."}},
  "signatures": [...]
}
```

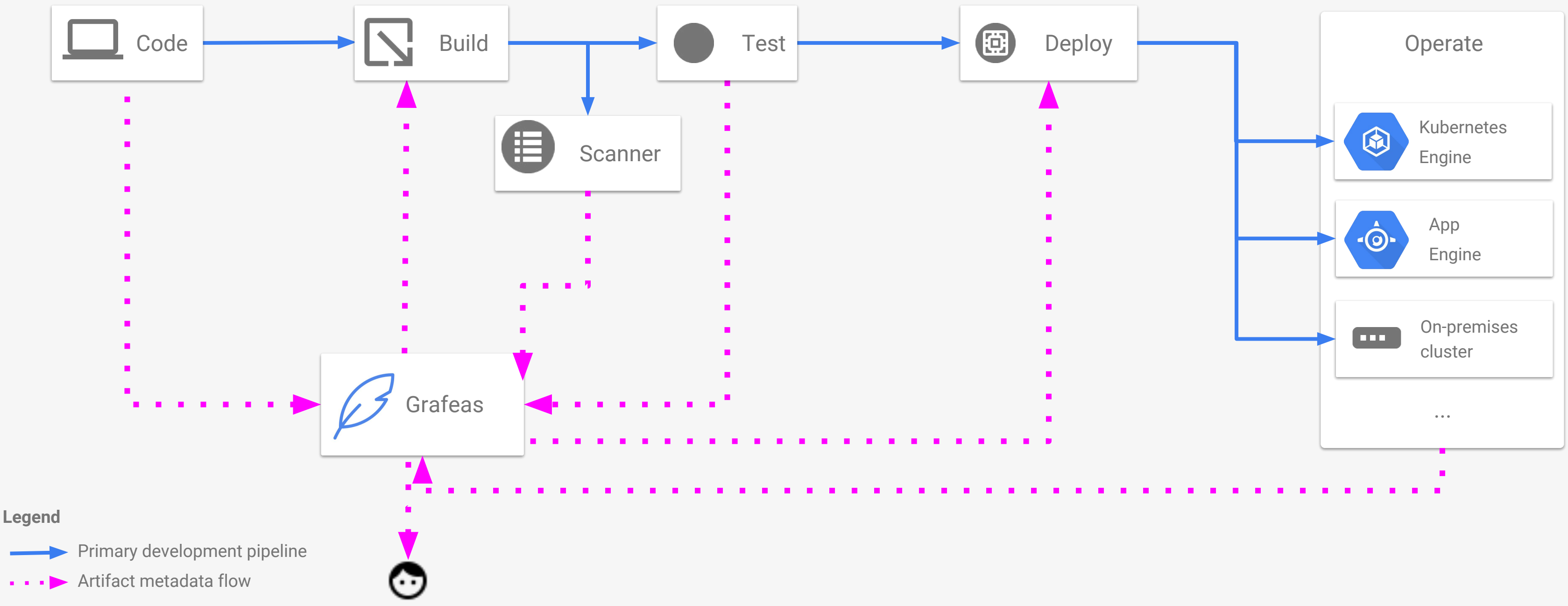
```
{
  "_type": "Link",
  "name": "test",
  "byproducts":
{"stderr": "", "stdout":
"",
"return_value": 0
},
  "command": [...],
  "materials": {...},
  "products": {
    "foo": {"sha256":
"..."}},
  "signatures": [...]
}
```

```
{
  "_type": "Link",
  "name": "build",
  "byproducts":
{"stderr": "", "stdout":
"",
"return_value": 0
},
  "command": [...],
  "materials": {},
  "products": {
    "foo": {"sha256":
"..."}},
  "signatures": [...]
}
```

```
{
  "_type": "Link",
  "name": "container",
  "byproducts":
{"stderr": "", "stdout":
"",
"return_value": 0
},
  "command": [...],
  "materials": {},
  "products": {
    "in-toto/.git/HEAD":
{"sha256": "..."}},
  "signatures": [...]
}
```

So much metadata, what do we do?

Grafeas Motivation



tl;dr A structured metadata API
for annotating cloud components

Grafeas API

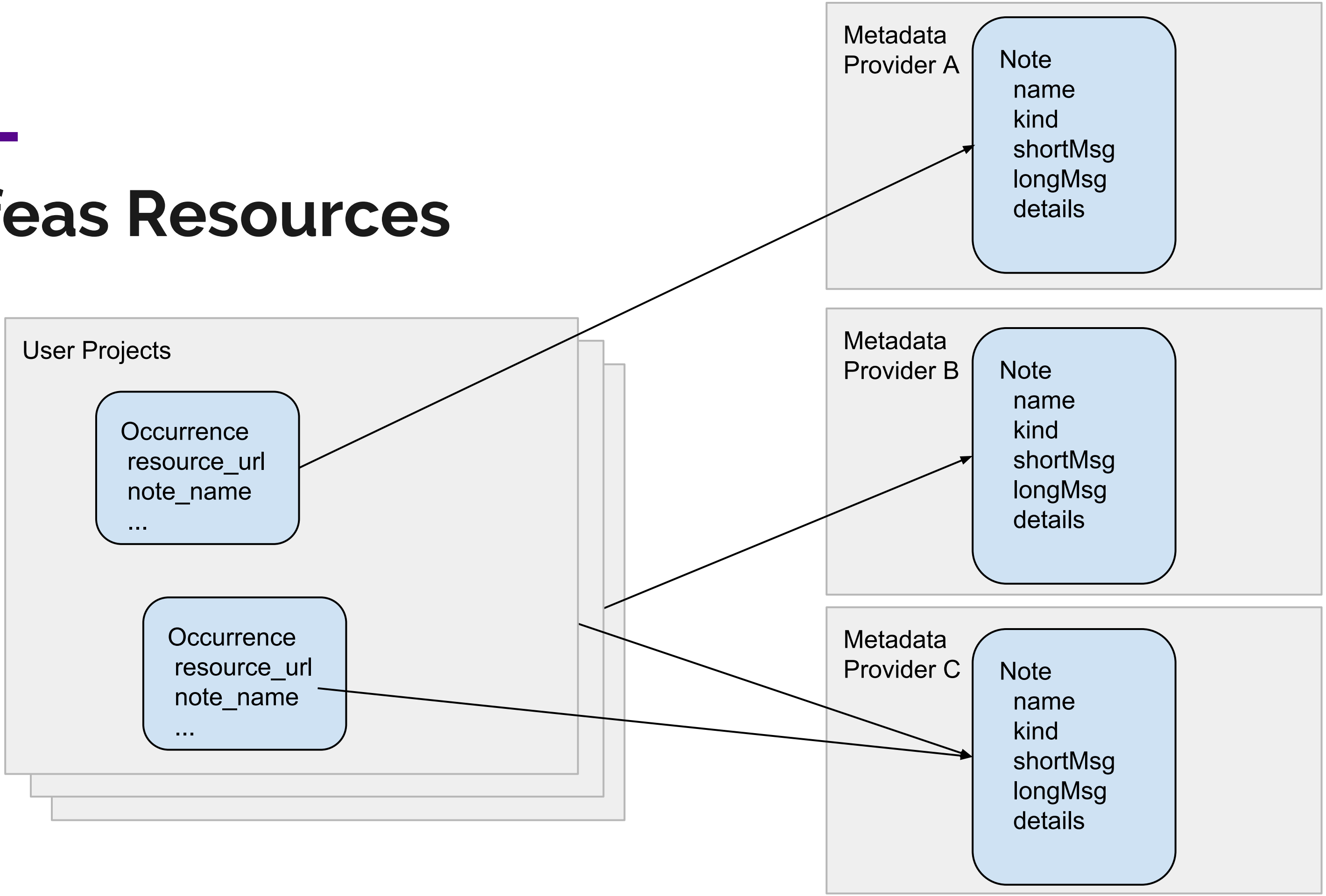
Notes

- Context-insensitive metadata in a provider’s project

Occurrences

- Links to a provider’s note
- Binds a note to a resource in a user’s project

Grafeas Resources



Grafeas API: Package

- Which packages are installed?

Grafeas API: Vulnerabilities

- Which packages have known vulnerabilities?

Grafeas API: Discovery

- What type of analysis is ongoing or has happened for this resource?

Grafeas API: Builds

- What source was this built from?
- Who built it?
- What builder was used?

Grafeas API: Image

- Which base image was used for this container?

Grafeas API: Attestation

- Have policy requirements been met?
  - Has QA team signed off?
  - Do I approve of the way this image was built?
  - Is this resource free of exploitable Vulnerabilities?
  - Endless possibilities...

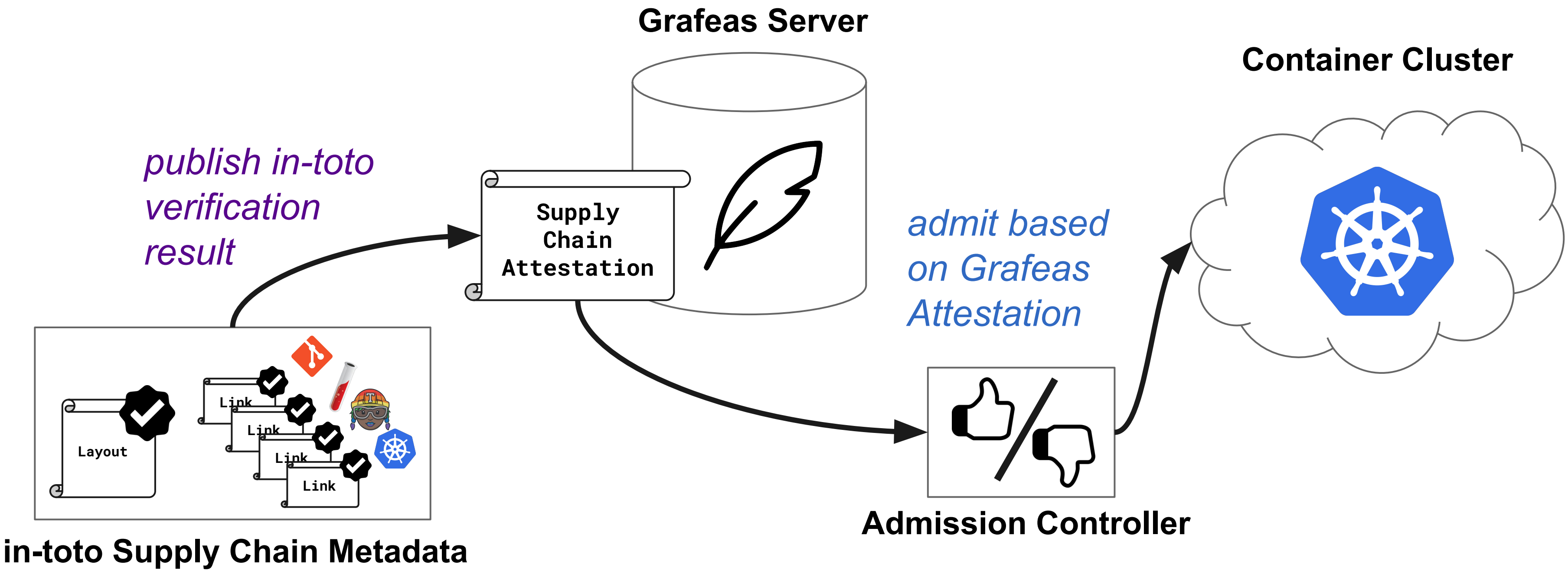
Grafeas API: Deployment History

- When was this deployed?
- By whom?
- Where?
- Cross check production against new vulnerability information

Query Data From Grafeas To Control Your Deployment

Publish in-toto Verification Results To Grafeas Server

in-toto Verification Result As Grafeas Attestation



Grafeas Server

Container Cluster

publish in-toto verification result

admit based on Grafeas Attestation

Admission Controller

in-toto Supply Chain Metadata

in-toto.io
github.com/in-toto
jcappos@nyu.edu

Thank You!

Grafeas.io
github.com/Grafeas
grafeas-users@googlegroups.com
grafeas-dev@googlegroups.com
github.com/kelseyhightower/grafeas-tutorial

Questions?