Open Component Model

Secure Delivery for Sovereign Clouds

First class air-gap enabled, immutable releases

Open source by default. Donated to the NeoNephos Foundation.





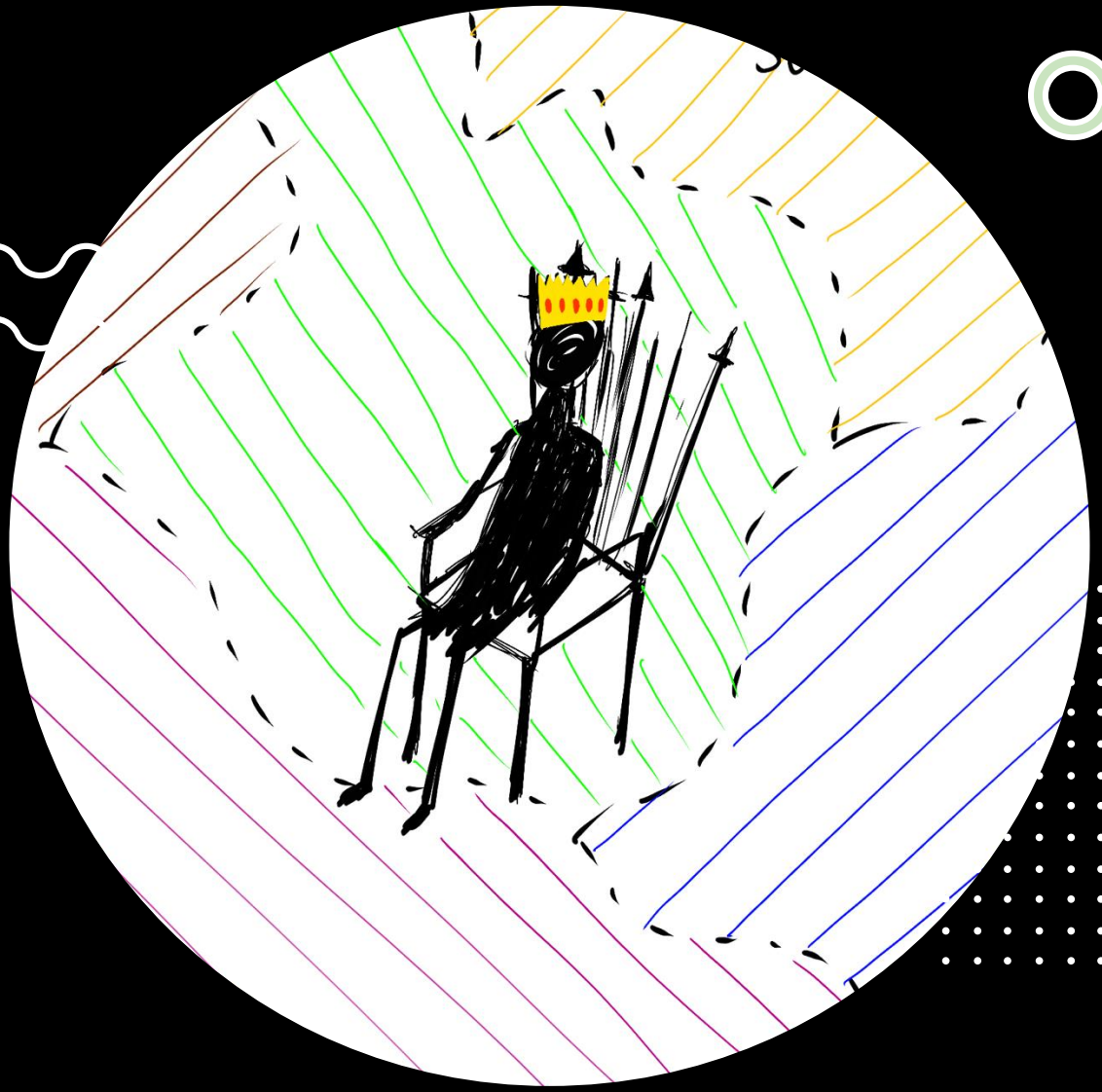
Who am I?



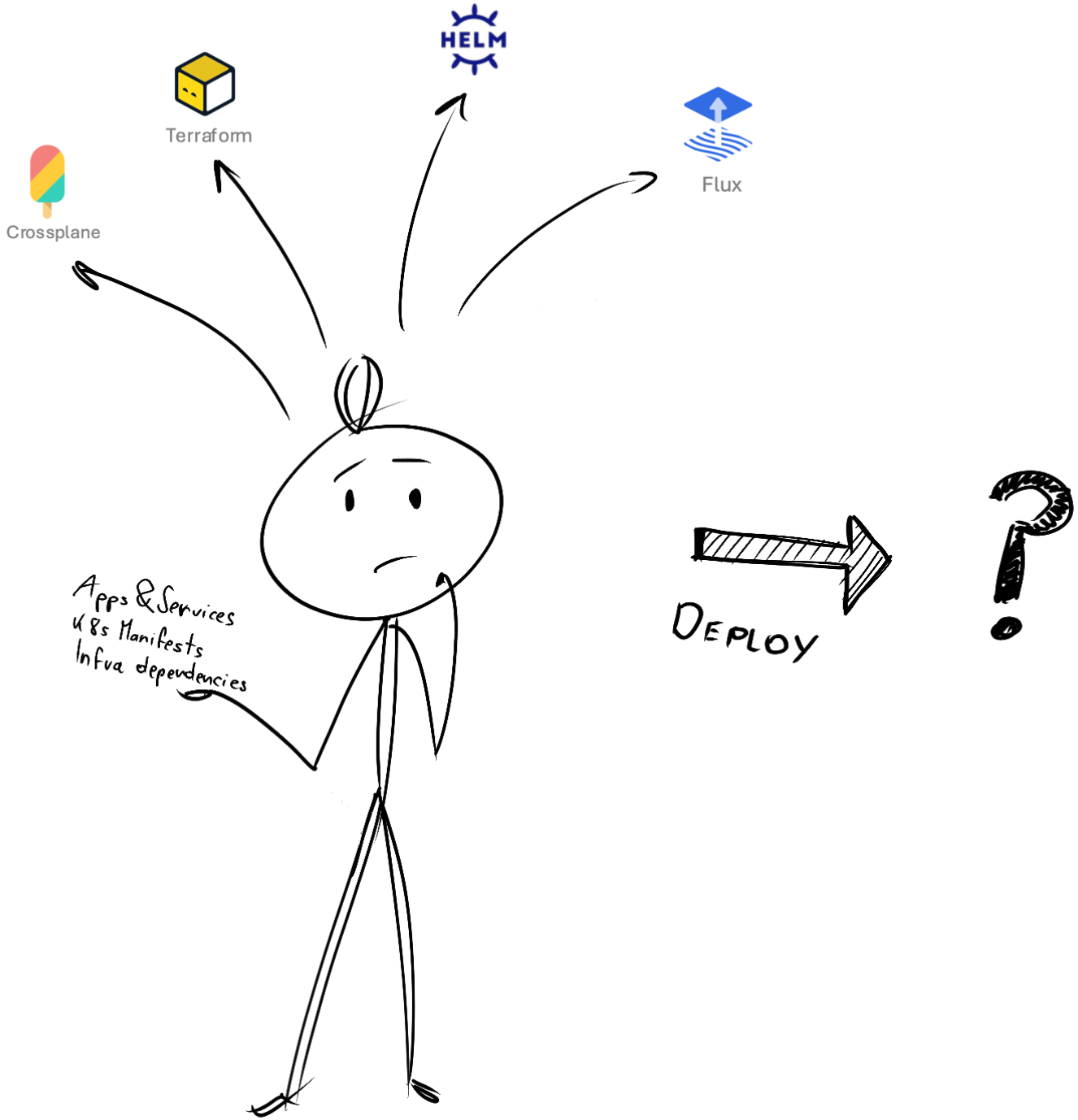
Name: Gergely Bräutigam

GitHub: Skarlso

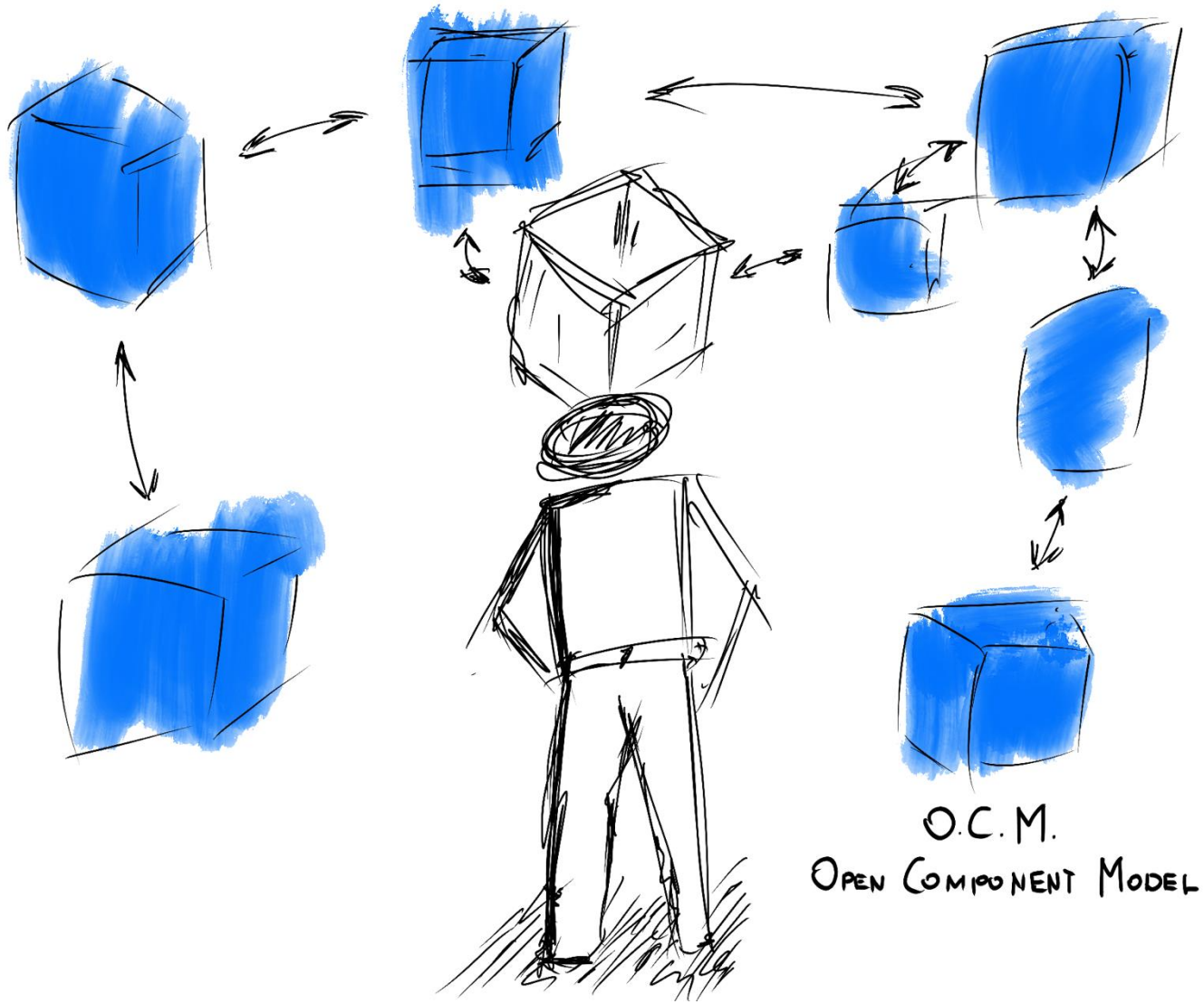
Sovereign Cloud



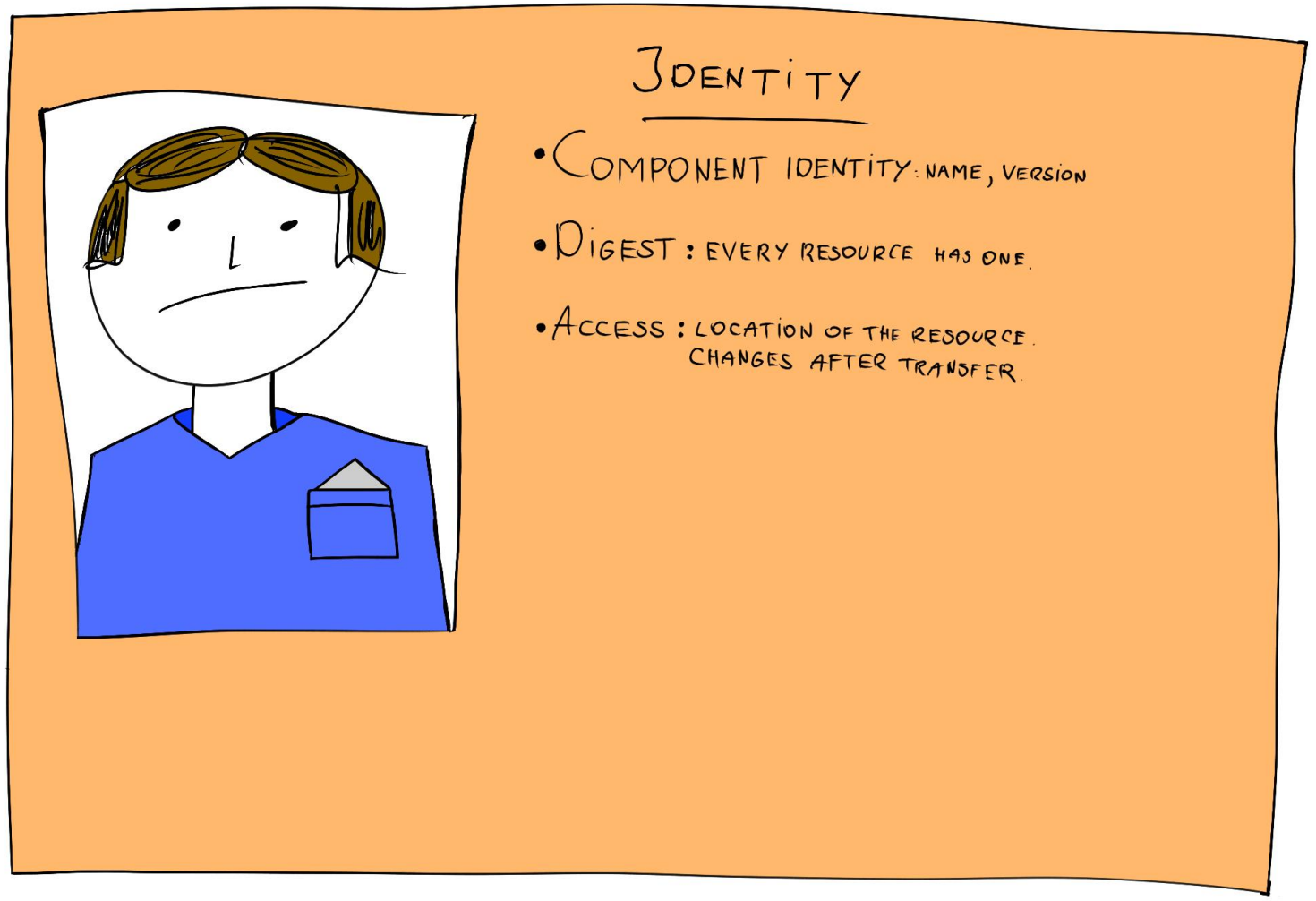
The Problem


HELM
Terraform
Flux
Crossplane
Apps & Services
k8s Manifests
Infra dependencies
DEPLOY
?

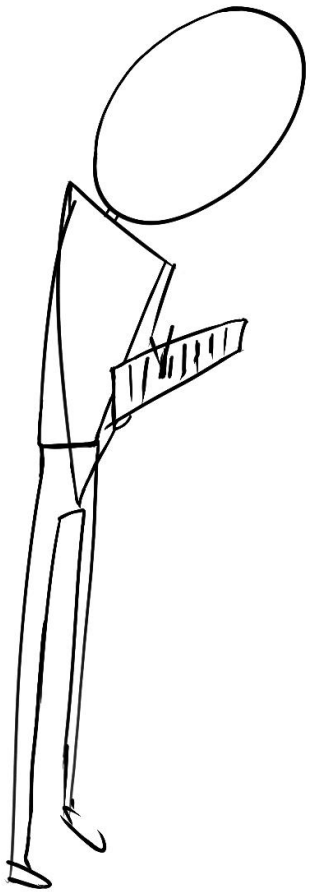
Meet OCM



One Identity – Signed and Verified



What you write



Software-Bill-of-Delivery (SBoD)

https://github.com/open-component-model/ocm-spec

```yaml
components:
- name: github.com/acme.org/helloworld
  version: 1.0.0
  provider:
    name: acme.org
  resources:
    - name: mylocalfile
      type: blob
      input:                    # Embed by value
        type: File/v1
        path: ./my-local-resource.txt

    - name: image
      type: ociImage
      version: 1.0.0
      access:                   # Reference external artifact
        type: OCIImage/v1
        imageReference: ghcr.io/stefanprodan/podinfo:6.9.1
```

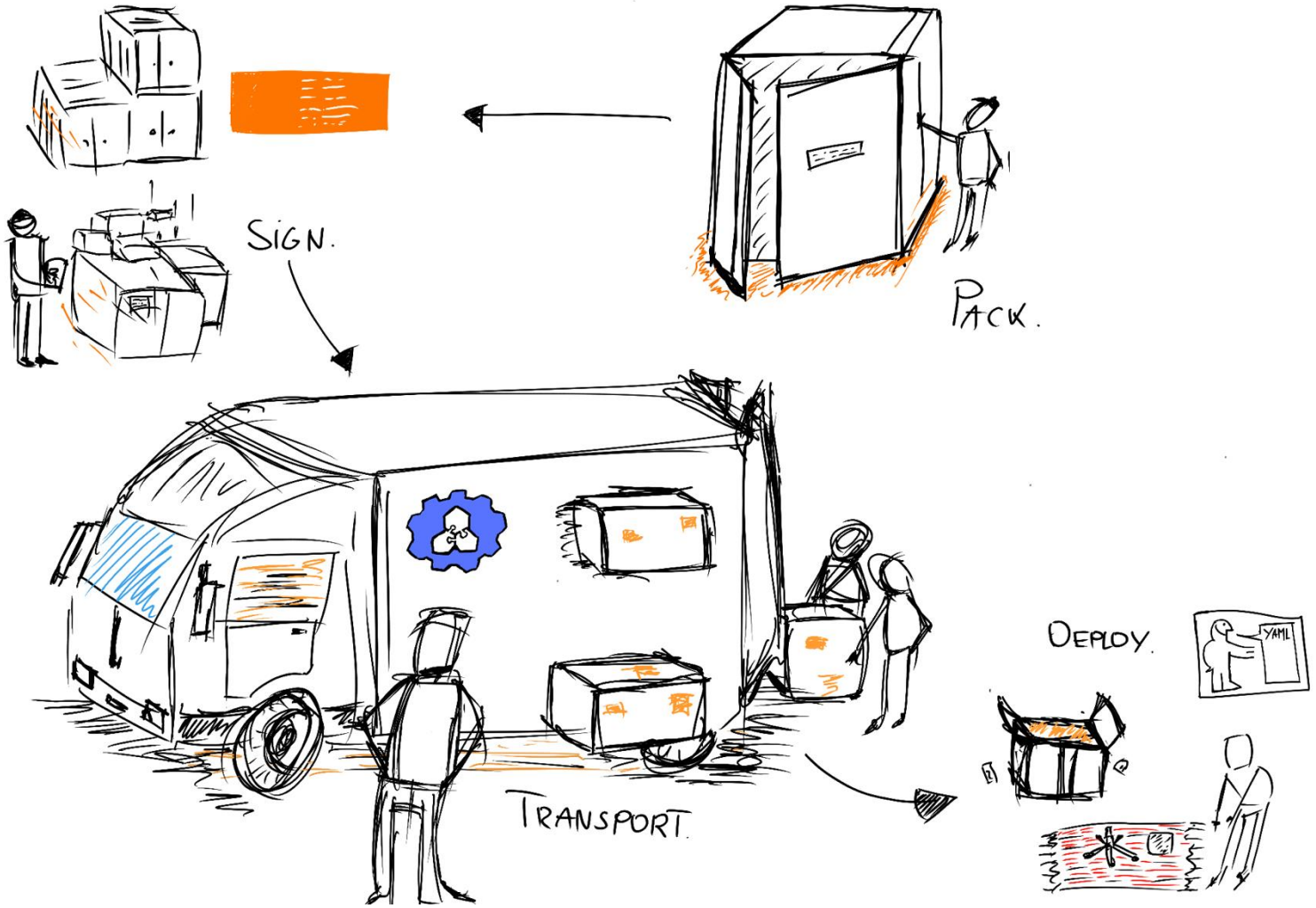
The result

```yaml
component:                                  # (fields trimmed)
  name: github.com/acme.org/helloworld
  version: 1.0.0
  resources:
    - name: image
      type: ociImage
      access:                               # excluded - rewritten on transfer
        type: OCIImage/v1
        imageReference: ghcr.io/stefanprodan/podinfo@sha256:8fa5691d768ef456...

      digest:                               # content identity - input to descriptor hash
        hashAlgorithm: SHA-256
        value: 262578cde928d5c9eba3bce0...

signatures:                                 # signature: one hash over the canonicalized descriptor
  - name: acme-release-key
    digest:                                 # of the descriptor
      hashAlgorithm: SHA-256
      value: a4b1c2d3e4f5...
    signature:
      algorithm: RSASSA-PSS
      value: <hex-encoded signature>
```

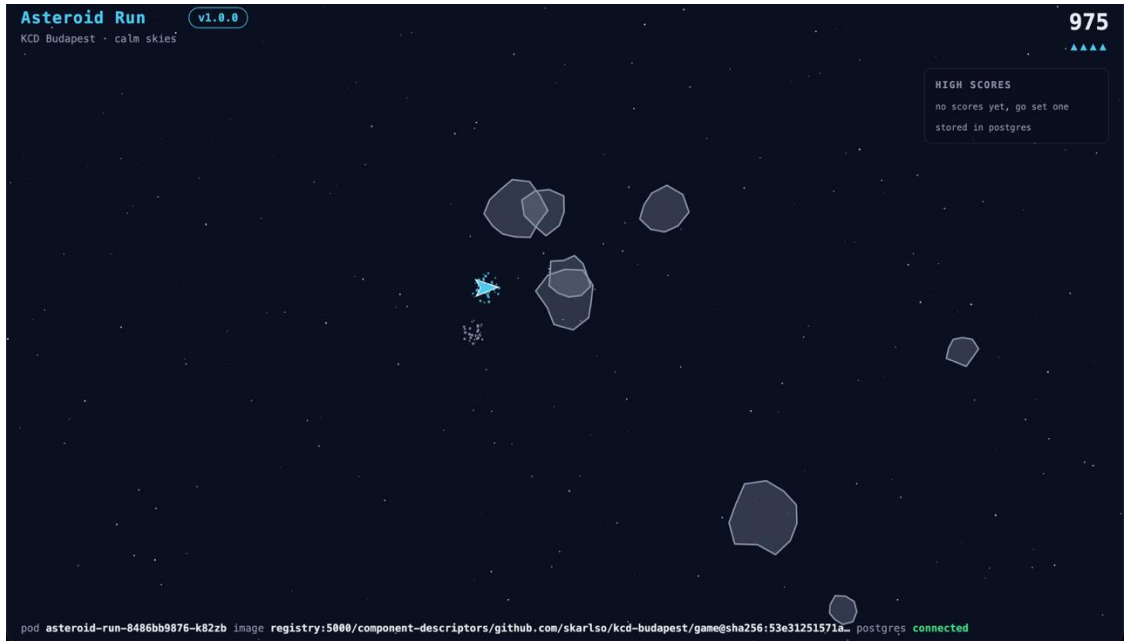
Pack. Sign. Transport. Deploy.



Demo Time

In Case the demo gods were not with me

Before Upgrade running v1.0.0



After Upgrade running v1.0.1



OCM TECHNOLOGY LANDSCAPE

Supported technologies today.

ARTIFACTS & PACKAGES

- OCI artifacts
- Container images
- Helm charts
- YAML · JSON
- Files · dirs
- Local blobs

Inputs: File · Dir · UTF8 · Helm
Access: OCIImage · OCIImageLayer · LocalBlob

SOURCE CODE

- Any Git server
- GitHub
- GitLab
- Bitbucket
- Gitea
- Azure DevOps

Git/v1 via HTTPS, SSH, git:// or local path
GitHub/v1 kept for published components

HTTP & OBJECT STORAGE

- HTTP · HTTPS
- Amazon S3
- MinIO
- Ceph RGW
- Cloudflare R2

Wget/v1 and S3/v2 as input or access
Digest verified on every fetch

TRANSFER TARGETS

- OCI registries
- CTF archives
- Artifactory
- Nexus
- Maven
- npm

OCI, Artifactory and Nexus uploaders
CTF archives carry releases into air gaps

DEPLOY & EXTEND

- Kubernetes
- OCM controllers
- Flux
- Argo CD
- kro
- Plugins

Repository · Component · Resource · Deployer
Replication · Discovery · plugin access types

SIGNING & TRUST

- Sigstore
- cosign
- Fulcio
- Rekor
- OIDC identity
- RSA-PSS keys

Keyless via OIDC or key-based signing
One signature covers every digest



Explore OCM yourself

https://ocm.software

