

De Toekomst van Federatieve Toegang

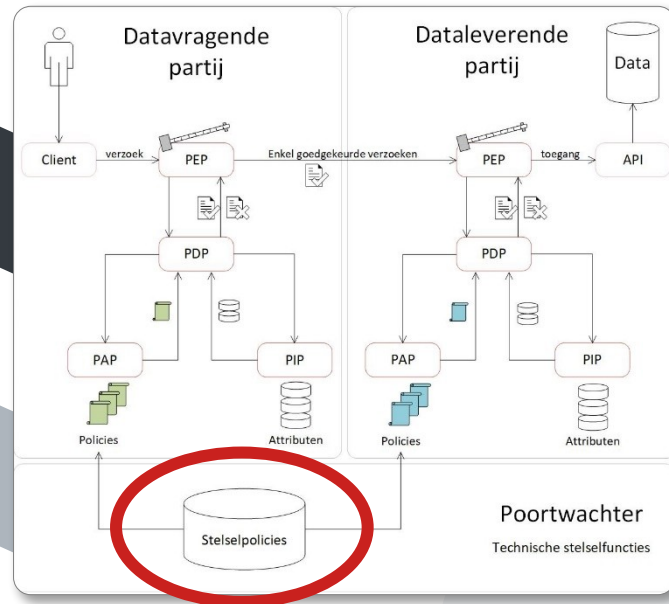
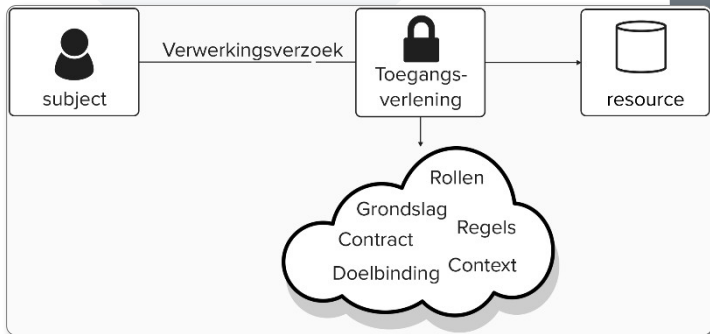
22 okt 2024



Technisch spoor:
Policies!



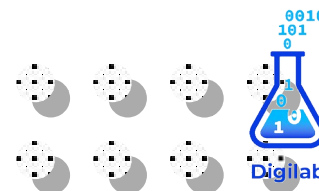
Technisch spoor: **Policies!**



De beste oplossing voor federatieve toegangsverlening

Policies → Policy talen

- XACML
- ODRL
- Lock/Unlock
- OPA/Rego-lang
- Cedar Policy
- Cerbos/CEL
- ...?



XACML

- OASIS standaard - 2003
- XML
- Gestructureerd
- Weinig open-source implementaties
- Java, .NET, REST



XACML

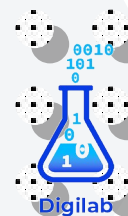
Policy -

```
<Target>
  <Subjects>
    <Subject>
      <SubjectMatch
        MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match">
          <AttributeValue
            DataType="http://www.w3.org/2001/XMLSchema#string">
            med.example.com
          </AttributeValue>
          <SubjectAttributeDesignator
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
            DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name"/>
          </SubjectAttributeDesignator>
        </SubjectMatch>
      </Subject>
    </Subjects>
  </Target>
```

Parameter 1

Function to apply

Parameter 2 – But need to
dereference from the request.



XACML

Voordelen

Door de wel geverfde standaard

Policies modulair te bouwen

Nadelen

Weinig open-source

Vooral (kostbare) gesloten software

Policies zijn niet heel leesbaar

ODRL

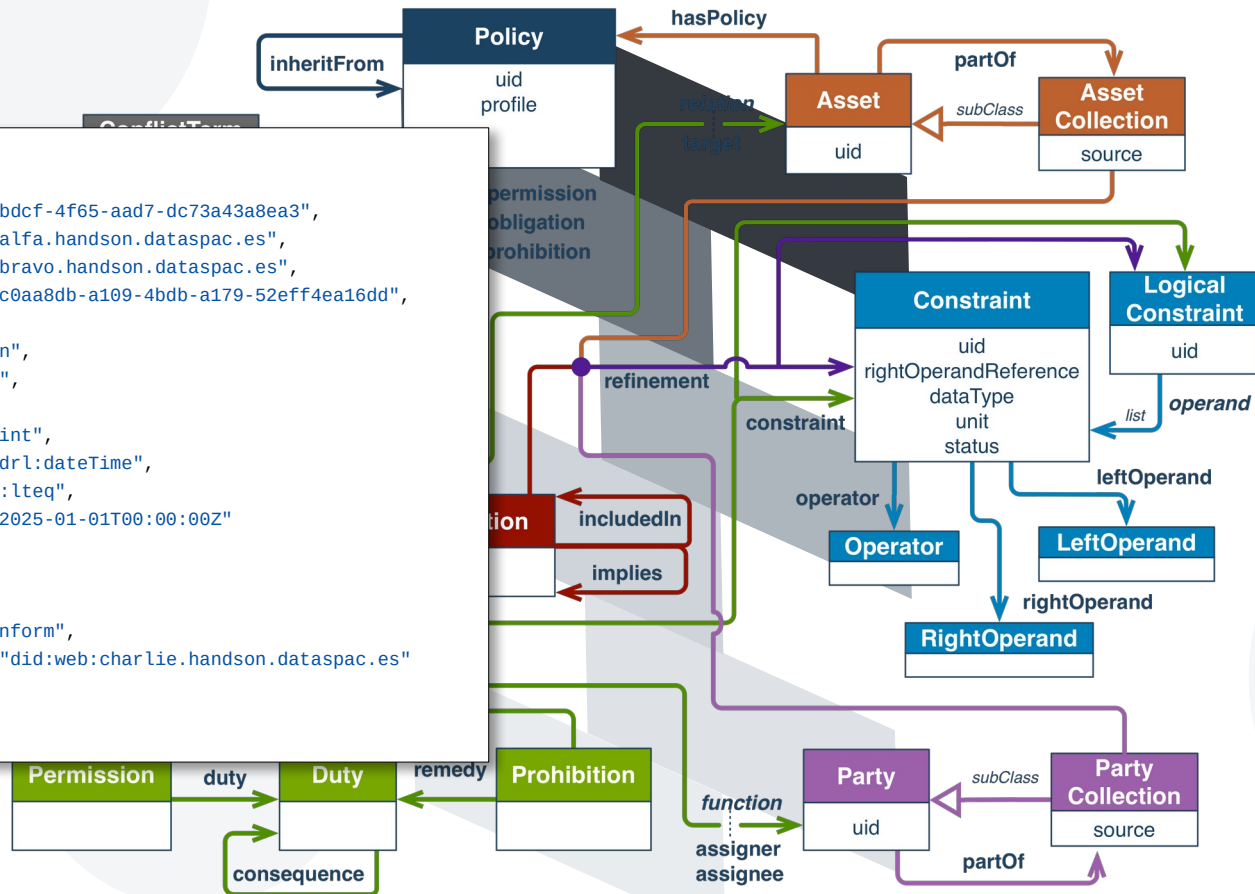
- W3C standaard - 2002
- RDF – turtle, json, xml
- Gestructureerd
- Weinig open-source implementaties (wel actuele initiatieven)
- Javascript, Java

ODRL

```

{
  "@type": "odrl:Agreement",
  "@id": "urn:uuid:4b4afc34-bdcf-4f65-aad7-dc73a43a8ea3",
  "odrl:assigner": "did:web:alfa.handson.dataspac.es",
  "odrl:assignee": "did:web:bravo.handson.dataspac.es",
  "odrl:target": "urn:uuid:dc0aa8db-a109-4bdb-a179-52eff4ea16dd",
  "odrl:permission": [{
    "@type": "odrl:Permission",
    "odrl:action": "odrl:use",
    "odrl:constraint": [{
      "@type": "odrl:Constraint",
      "odrl:leftOperand": "odrl:dateTime",
      "odrl:operator": "odrl:lteq",
      "odrl:rightOperand": "2025-01-01T00:00:00Z"
    }],
    "odrl:duty": [{
      "@type": "odrl:Duty",
      "odrl:action": "odrl:inform",
      "odrl:informedParty": "did:web:charlie.handson.dataspac.es"
    }]
  }],
}

```



ODRL

Voordelen

Door de wol geverfde standaard

Meest gebruikt

Policies modulair te bouwen

Link met DCAT

Nadelen

Weinig open-source

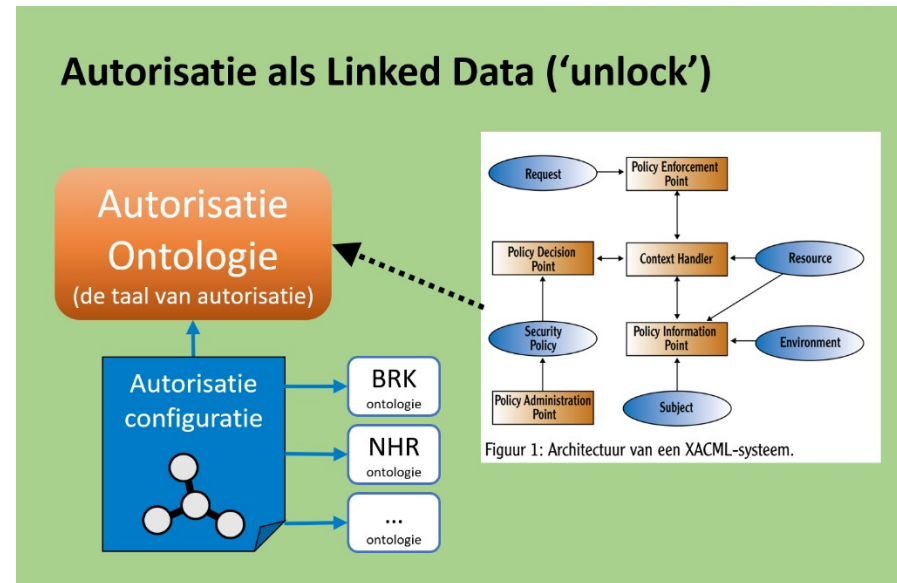
Vooral gericht op DRM

Vooral (kostbare) gesloten software

Policies zijn niet heel leesbaar

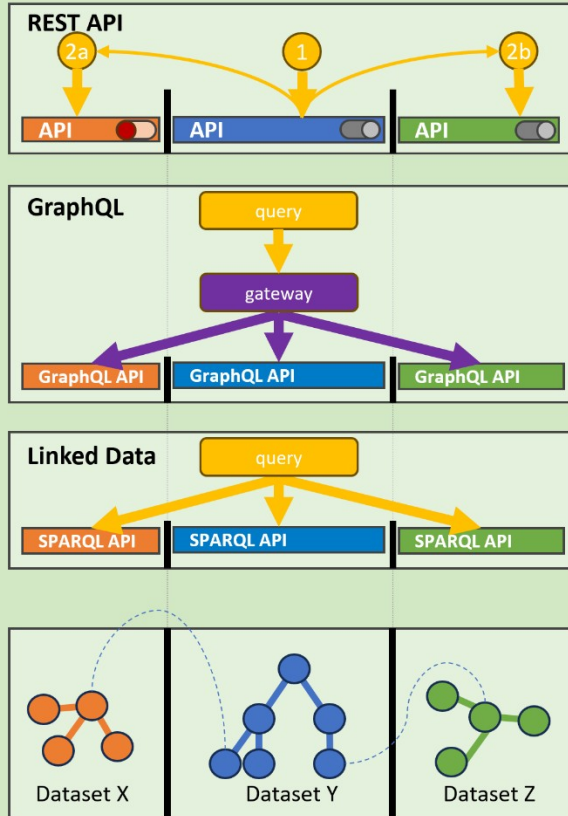
Lock/Unlock

Authorization Ontology (research)

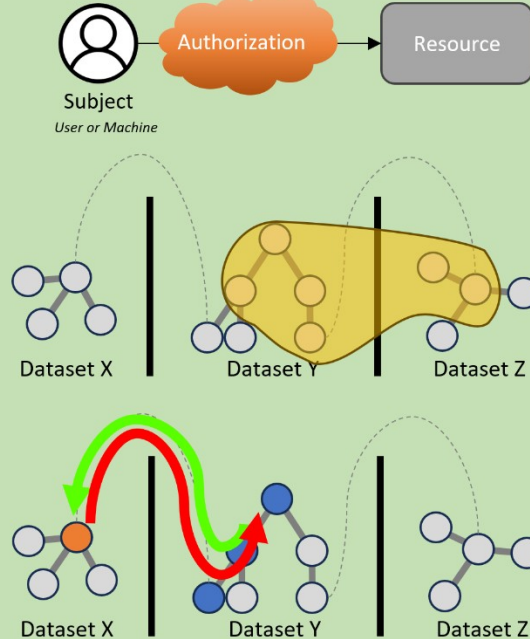


Lock-Unlock: lock de data, unlock het potentieel

Federatieve bevraging

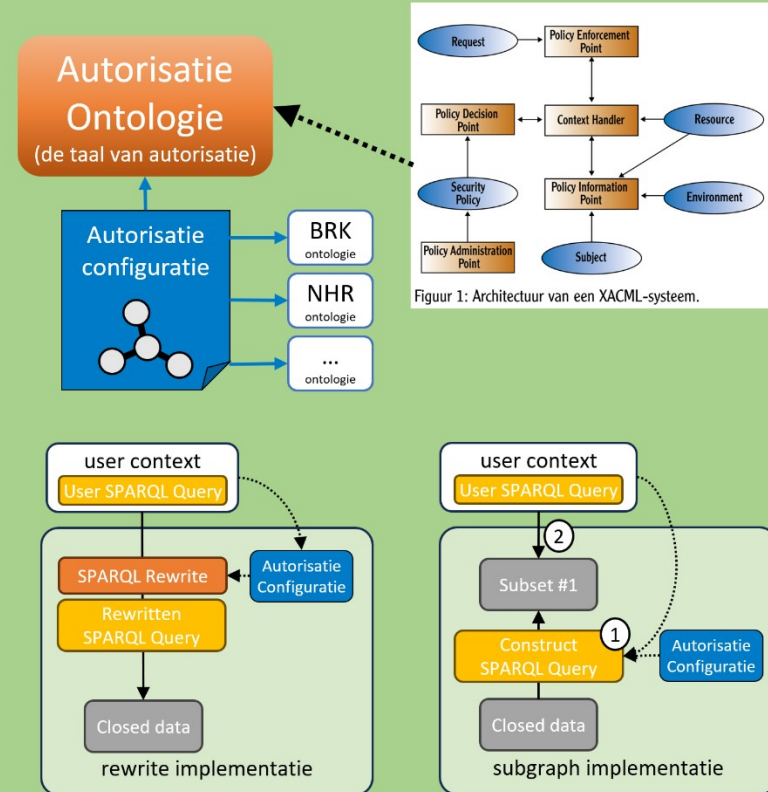


Afscherming ('lock')



Horizontale subset	?	✓
Verticale subset	?	✓
Richting beperken	?	✓
Vrije query	?	✓

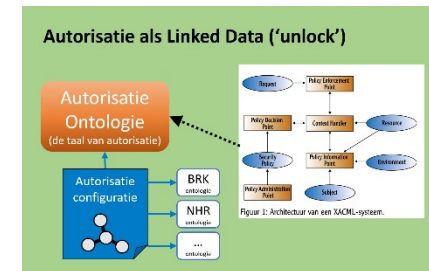
Autorisatie als Linked Data ('unlock')



Figuur 1: Architectuur van een XACML-systeem.

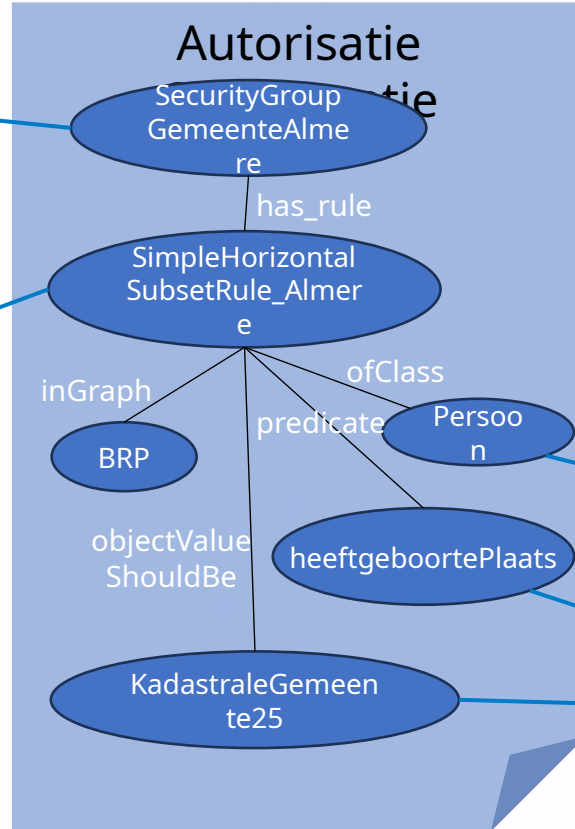
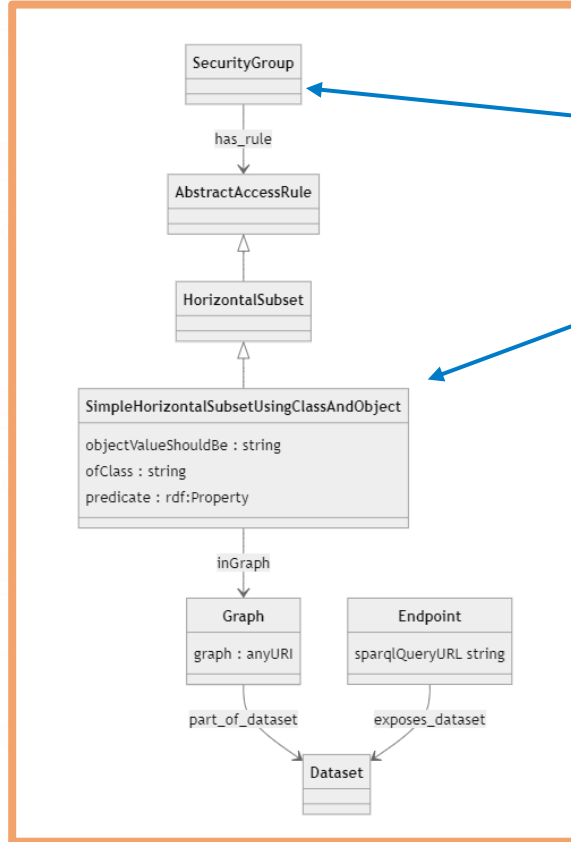
Lock/Unlock

- Integrale GebruikersOplossing
- Kadaster Knowledge Graph – Open Data
- Onderzoek: **Lock de data, unlock het potentieel**
- Opdracht van R-FDS (Realisatie IBDS)
- Kadaster DataScienceTeam – 2023/2024

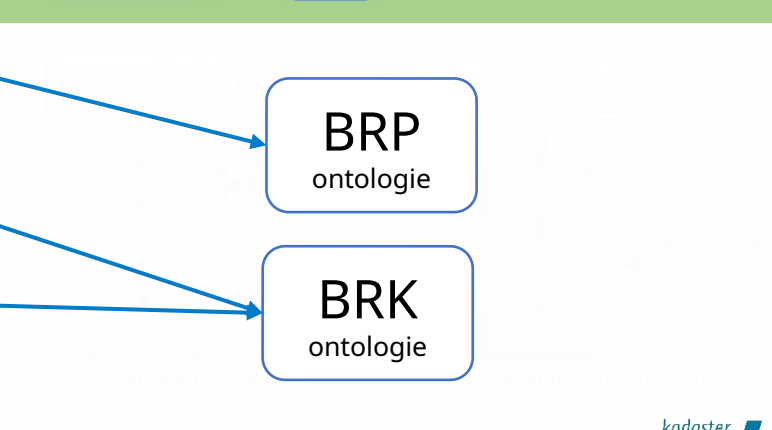
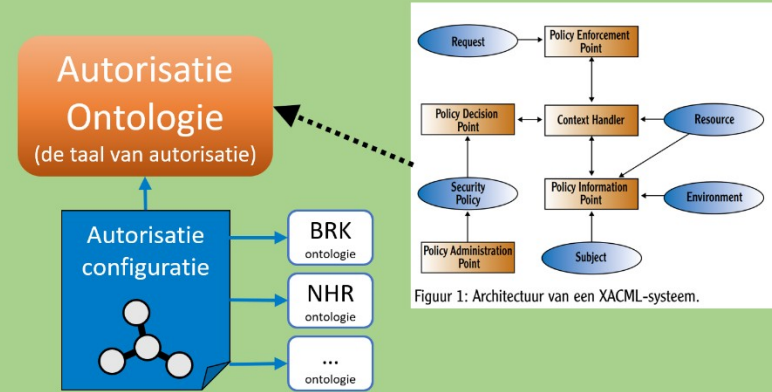


Lock-Unlock: lock de data, unlock het potentieel

Autorisatie Ontologie (de taal van autorisatie)

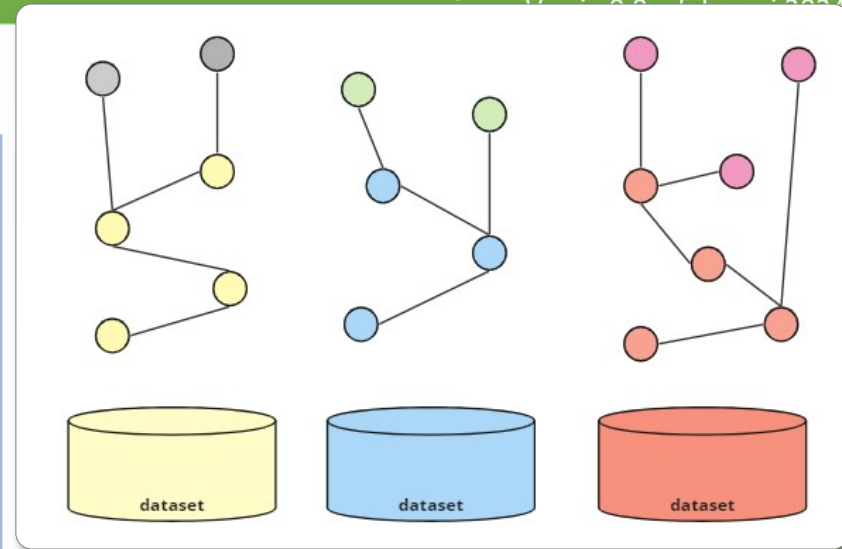
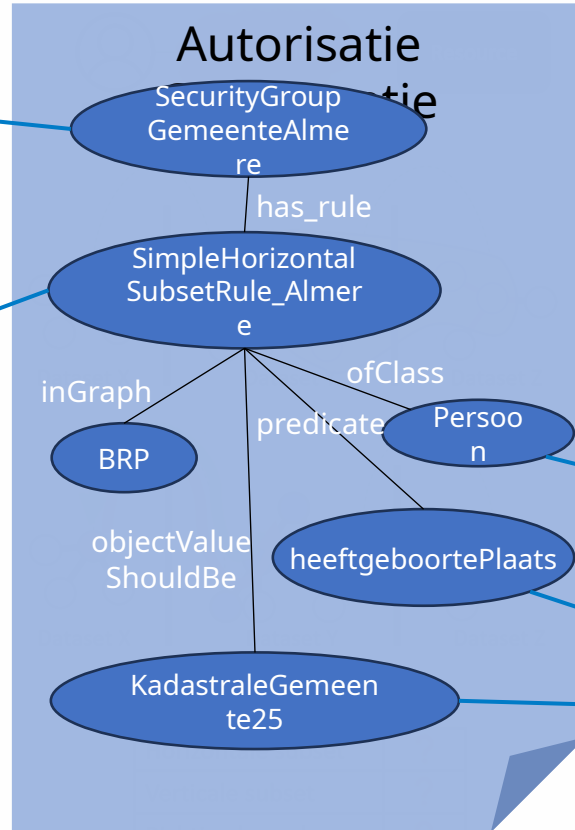
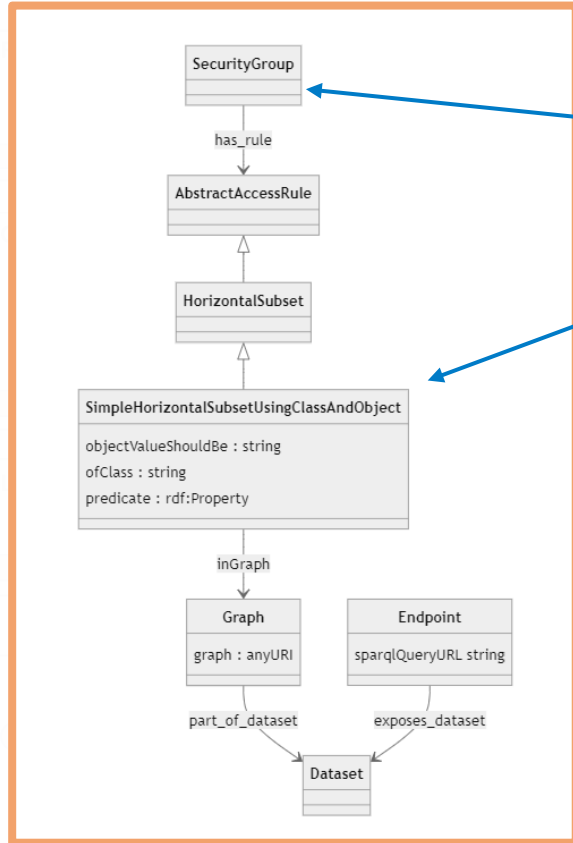


Autorisatie als Linked Data ('unlock')



Lock-Unlock: lock de data, unlock het potentieel

Autorisatie Ontologie (de taal van autorisatie)

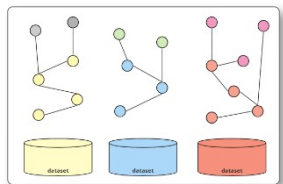


BRP
ontologie

BRK
ontologie

Lock/Unlock

Voordelen



Taal van XACML

Polities bij 'silo'

Semantisch standard

SPARQL/SHACL

Mogelijkheden voor
interoperabiliteit
naar andere talen?

Nadelen

Nieuw (! Slechts 1 onderzoek)

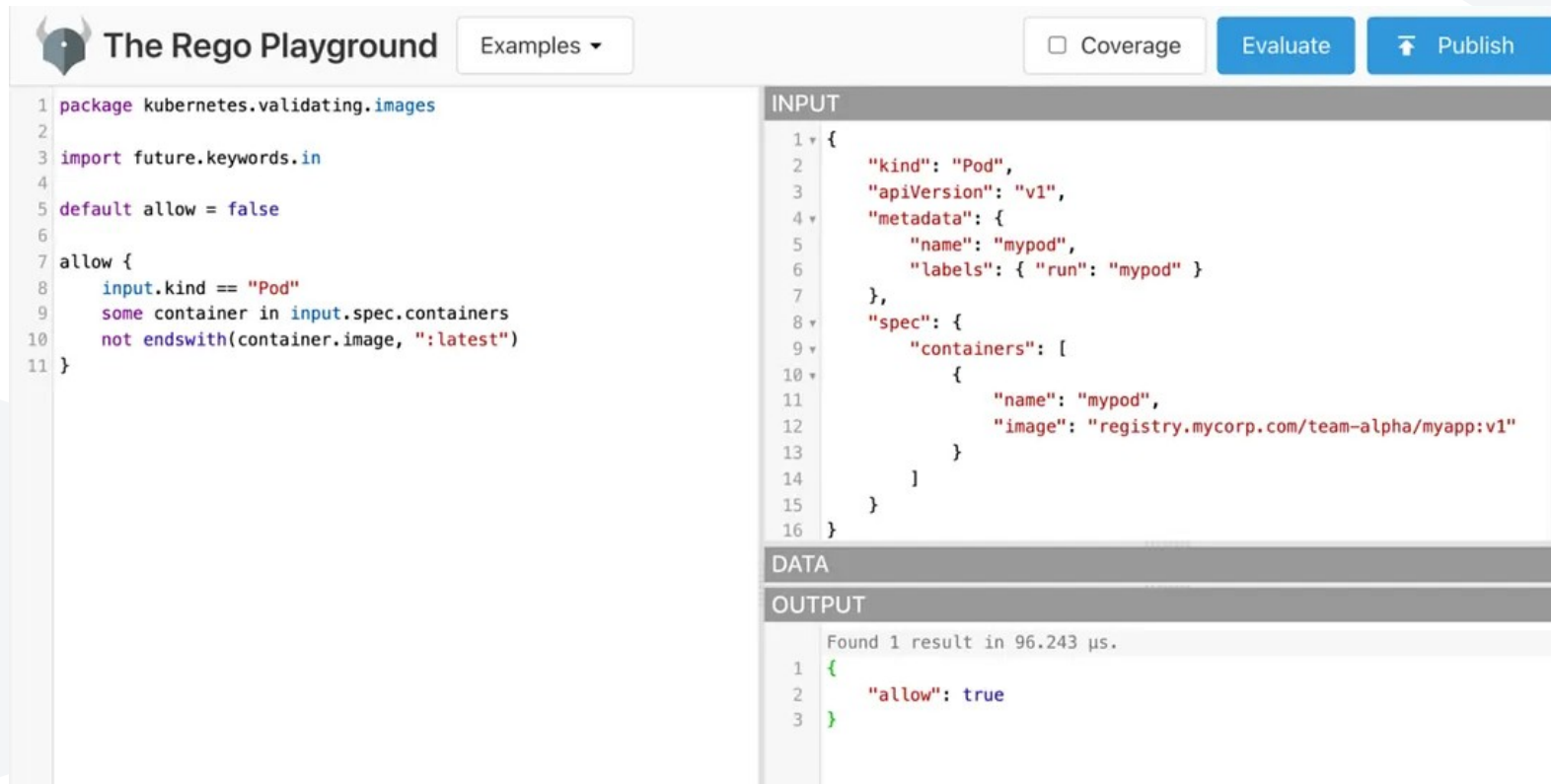
Semantische standaard ... dus
alleen toepasbaar in Linked Data?

OPA/Rego-lang

- CNCF - graduated 2021
- Vrije expressietaal
- Open source
- Go, WASM



OPA/Rego-lang



The Rego Playground interface displays a Rego policy on the left and its evaluation results on the right. The policy is a Kubernetes validating webhook that checks if a Pod's image is the latest version. The input is a JSON representation of a Pod. The output shows that the policy evaluates to true, meaning the Pod is allowed.

The Rego Playground Examples ▾ ☐ Coverage Evaluate Publish

```
1 package kubernetes.validating.images
2
3 import future.keywords.in
4
5 default allow = false
6
7 allow {
8   input.kind == "Pod"
9   some container in input.spec.containers
10  not endswith(container.image, ":latest")
11 }
```

INPUT

```
1 {
2   "kind": "Pod",
3   "apiVersion": "v1",
4   "metadata": {
5     "name": "mypod",
6     "labels": { "run": "mypod" }
7   },
8   "spec": {
9     "containers": [
10      {
11        "name": "mypod",
12        "image": "registry.mycorp.com/team-alpha/myapp:v1"
13      }
14    ]
15  }
16 }
```

DATA

OUTPUT

Found 1 result in 96.243 μs.

```
1 {
2   "allow": true
3 }
```



OPA/Rego-lang

Voordelen

Zeer populair

Volledig open source

Redelijk leesbare policies

Online playground

Nadelen

Programmeertaal

Lastig modulair te bouwen

Alleen PDP is open source

Cedar Policy

- Amazon – 2023
- Amazon Verified Permissions
- Vrije expressie-taal (ook JSON)
- Open-source
- Rust, Go, Java



Cedar Policy

```
1  // Template to grant a user or group read access to a document or folder.
2  @id("template")
3  permit (
4      principal in ?principal,
5      action == Action::"read",
6      resource in ?resource
7  );
8
9  // If a document is public, then anyone can read it.
10 permit (
11     principal,
12     action == Action::"read",
13     resource
14 )
15 when { resource.isPublic };
16
17 // A document's owner (or owners of the parent folder) can read, write to,
18 // or share the document.
19 permit (
20     principal,
21     action in [Action::"read", Action::"write", Action::"share"],
22     resource
23 )
24 when
25 { resource in principal.ownedDocuments || resource in principal.ownedFolders };
```



Cedar Policy

Voordelen

Marktleider voor de cloud

Redelijk leesbare policies

Nadelen

Programmeertaal

Lastig modulair te bouwen

Geen extra eisen

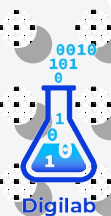
Cerbos/CEL

- Google - 2021
- YAML, JSON
- Gestructureerd
- Open-source
- Go, Java, .NET, PHP, Python

Cerbos/CEL

```
---
apiVersion: api.cerbos.dev/v1
resourcePolicy:
  resource: "album:object" ①
  version: "default" ②
  scope: "acme.corp" ③
  importDerivedRoles:
    - apatr_common_roles ④
  variables:
    import: ⑤
    - apatr_common_variables
    local: ⑥
    is_corporate_network: |-
      P.attr.ip_address.inIPAddrRange("10.20.0.0/16")
  rules:
    - actions: ['*'] ⑦
      effect: EFFECT_ALLOW
      derivedRoles:
        - owner ⑧

    - actions: ['view']
      effect: EFFECT_ALLOW
      roles:
        - user ⑨
      condition:
        match:
          expr: request.resource.attr.public == true
      output: ⑩
      when:
        ruleActivated: |-
          "view_allowed:%s".format([request.principal.id])
        conditionNotMet: |-
          "view_not_allowed:%s".format([request.principal.id])
```



Cerbos/CEL

Voordelen

Marktleider voor de cloud

Modulair te bouwen

Ruim aanbod SDK's

Online playground

Nadelen

Minder leesbare policies



“

Een computer is een dom ding.
Als je het niet precies vertelt wat
je wilt, doet het precies wat je niet
wilt.

- G.J.

”



Digilab

Ad Hoc Panel

- Wie **weet** hier iets over?
- Wie wil hier iets over **zeggen**?
- Nieuwe stelling = nieuw panel



Ad Hoc Panel

ODRL

OPA/Rego-lang



Ad Hoc Panel

ODRL

Authorization
Ontology

OPA/Rego-lang

ODRL



Ad Hoc Panel

ODRL

Authorization
Ontology

Cedar

OPA/Rego-lang

ODRL

Cerbos/CEL

Ranking

- **Open vs Closed?**
- **Populariteit?**
- **Standaard vs De facto standaard?**
- **Flexibiliteit?**
- **Leesbaarheid** (mens EN machine),
Onderhoudbaarheid?
- **Interoperabiliteit?**



Ad Hoc Panel

ODRL

OPA/Rego-lang

Authorization
Ontology

ODRL

Cedar

Cerbos/CEL

**De beste oplossing voor
federatieve toegangsverlening**

Ad Hoc Panel

**One language
to rule them all ... ?**

ODRI
Authorization
Ontology
Cedar
OPA/Rego-lang
ODRL
Cerbos/CEL

De beste oplossing voor
federatieve toegangsverlening

Vragen, suggesties?



Mattermost



Project
Federatieve Toegangsverlening

Digilab

digilab.overheid.nl

