Architecture & Prototype SMO Service Exposure & Discovery in O-RAN Opensource

Using Keycloak & JWTs to expose & secure services used by rApps

OSC NONRTRIC

12 Oct 2022

Enforcing Service Exposure / Access

Why we need selective and controlled access to services

Securely enforce exposure without changing your code

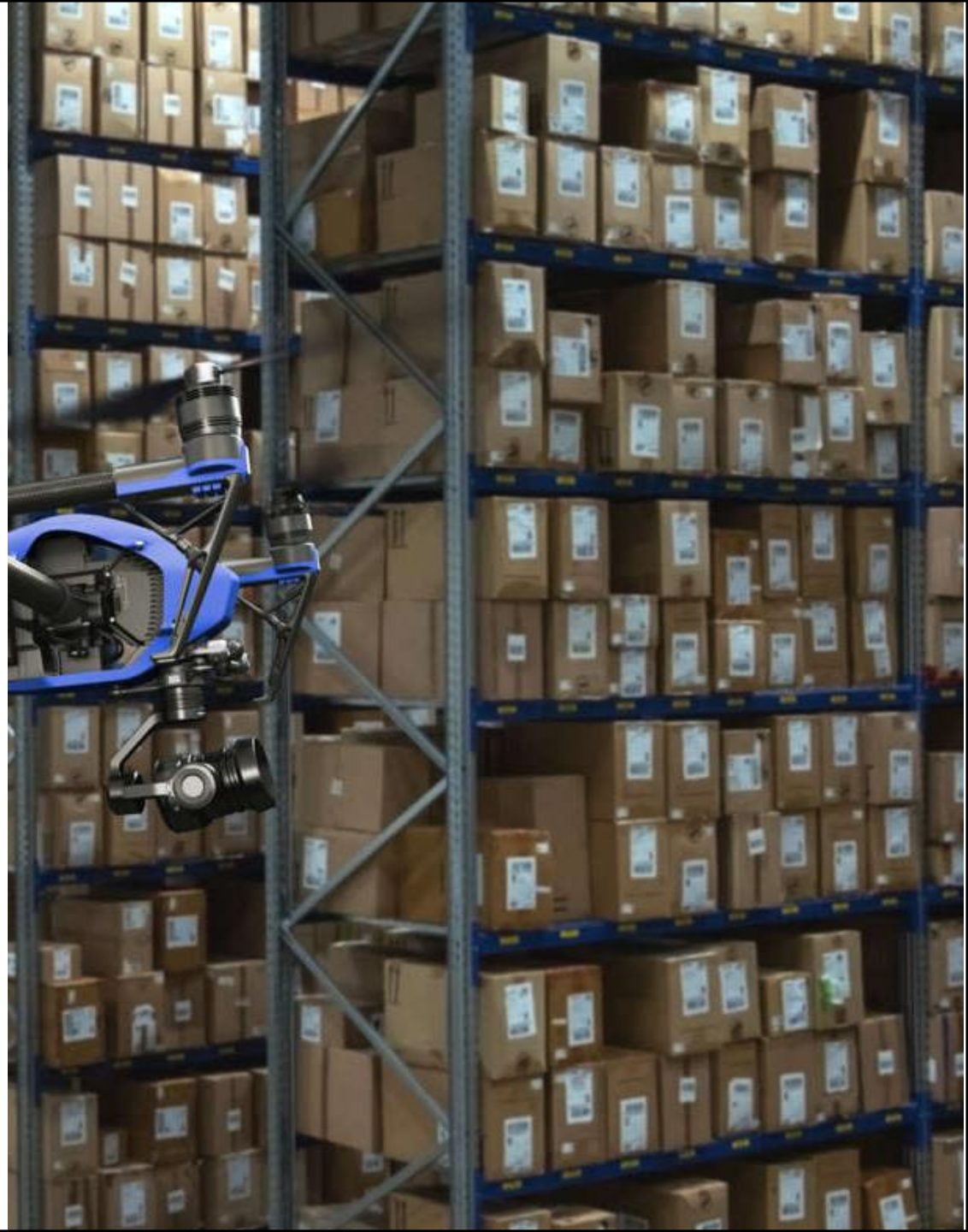
What is Service Exposure?
And why is it important?

— Apps (***rApps***) need to use SMO services, and provide service to other Apps

— Apps & SMO service may be multivendor

— We need *selective & controlled exposure* of these services

— New standardised ***O-RAN R1*** *interface*



How to do Service Exposure?

- Ensure that services cannot be accessed without a carefully allocated ‘Token’
- Apps (consumers) are allocated a ‘Token’ when deployed or instantiated (and continuously updated)
- Without changing Provider or Invoker!
- Service Registration & Discovery (*more on this later*)
- Even more fine-grained access policies (*more on this later*)

What do we show here?

- API Gateway
- How to implement exposure (authorisation) Platform services (*provider*)
- How to apply exposure (authorisation) policies to rApp µservices (*provider*)
- How to continuously create Tokens for rApps (*consumer*)

- Use/Integrate 3GPP-spec'ed CAPIF core functionality for Registry/Discovery

- Use/Integrate OPA Policies for more fine-grained access

rApp request flow

Invoker sends request to Provider
(Addressed via Istio Gateway)

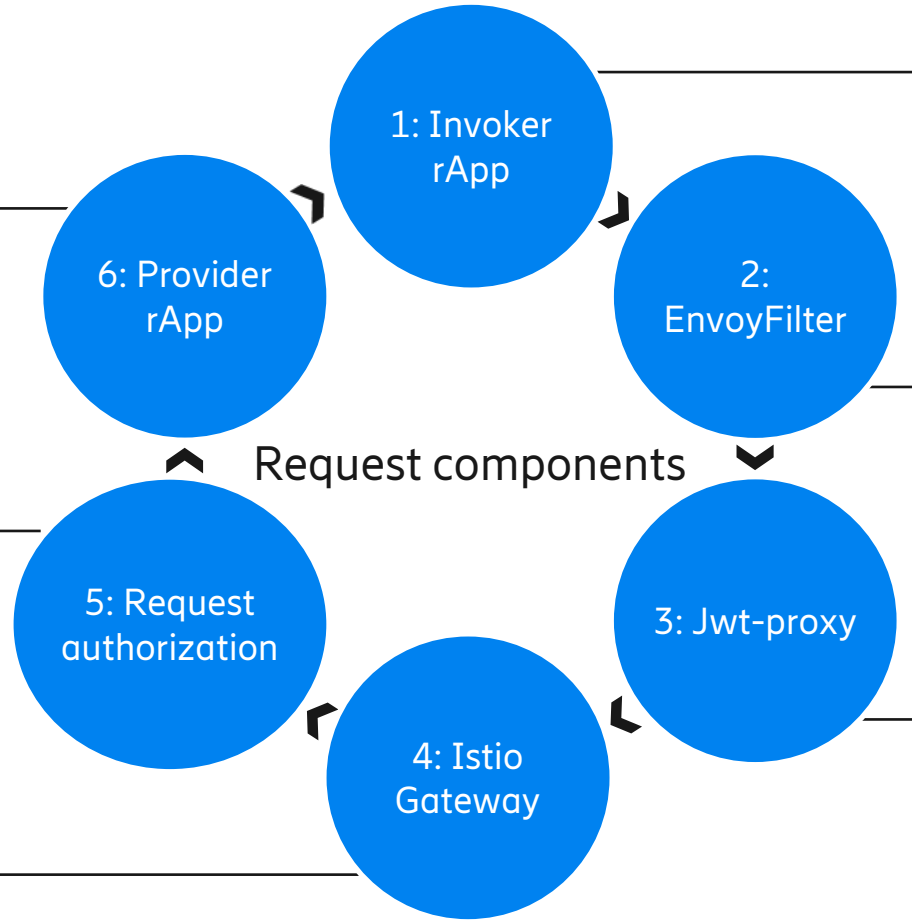
Request is intercepted by EnvoyFilter

Jwt-proxy retrieves/reuses JWT from Keycloak.
The request's header is updated to include the JWT .

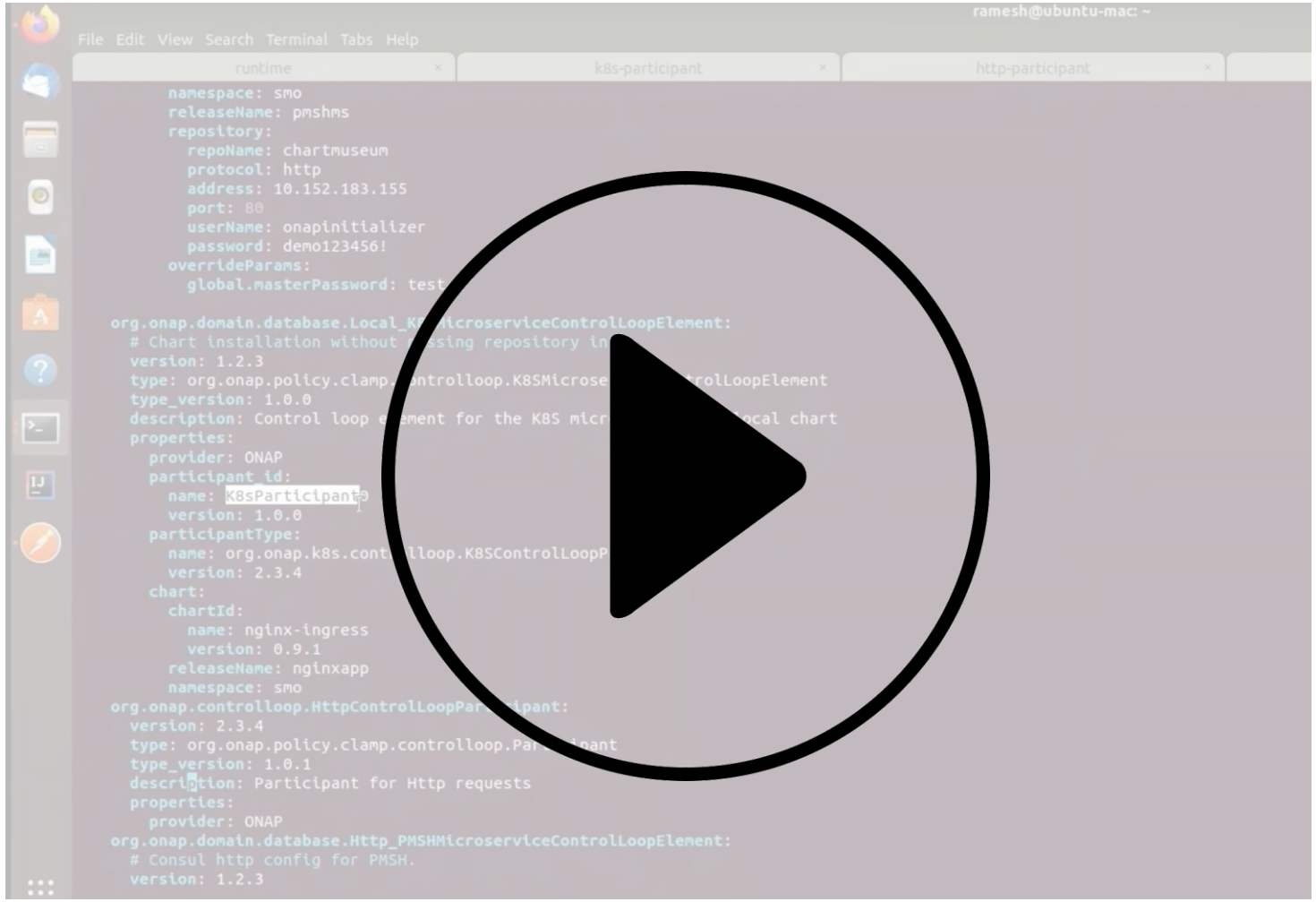
Gateway routes the request to the appropriate service (with JWT included)

The JWT is checked using either the Istio internal authorization mechanism or an external authorizer like OPA.

Provider send response back in the other direction (using reverse path – via Istio Gateway).



Demo


ramesh@ubuntu-mac: ~
File Edit View Search Terminal Tabs Help
runtime
k8s-participant
http-participant
namespace: smo
releaseName: pmshms
repository:
repoName: chartmuseum
protocol: http
address: 10.152.183.155
port: 80
userName: onapinitializer
password: demo123456!
overrideParams:
global.masterPassword: test
Chart installation without passing repository in
version: 1.2.3
version: 1.0.0
version: 2.3.4
chartId:
name: nginx-ingress
version: 0.9.1
releaseName: nginxapp
namespace: smo
version: 2.3.4
version: 1.0.1
Participant for Http requests
provider: ONAP
Consul http config for PMSH.
version: 1.2.3

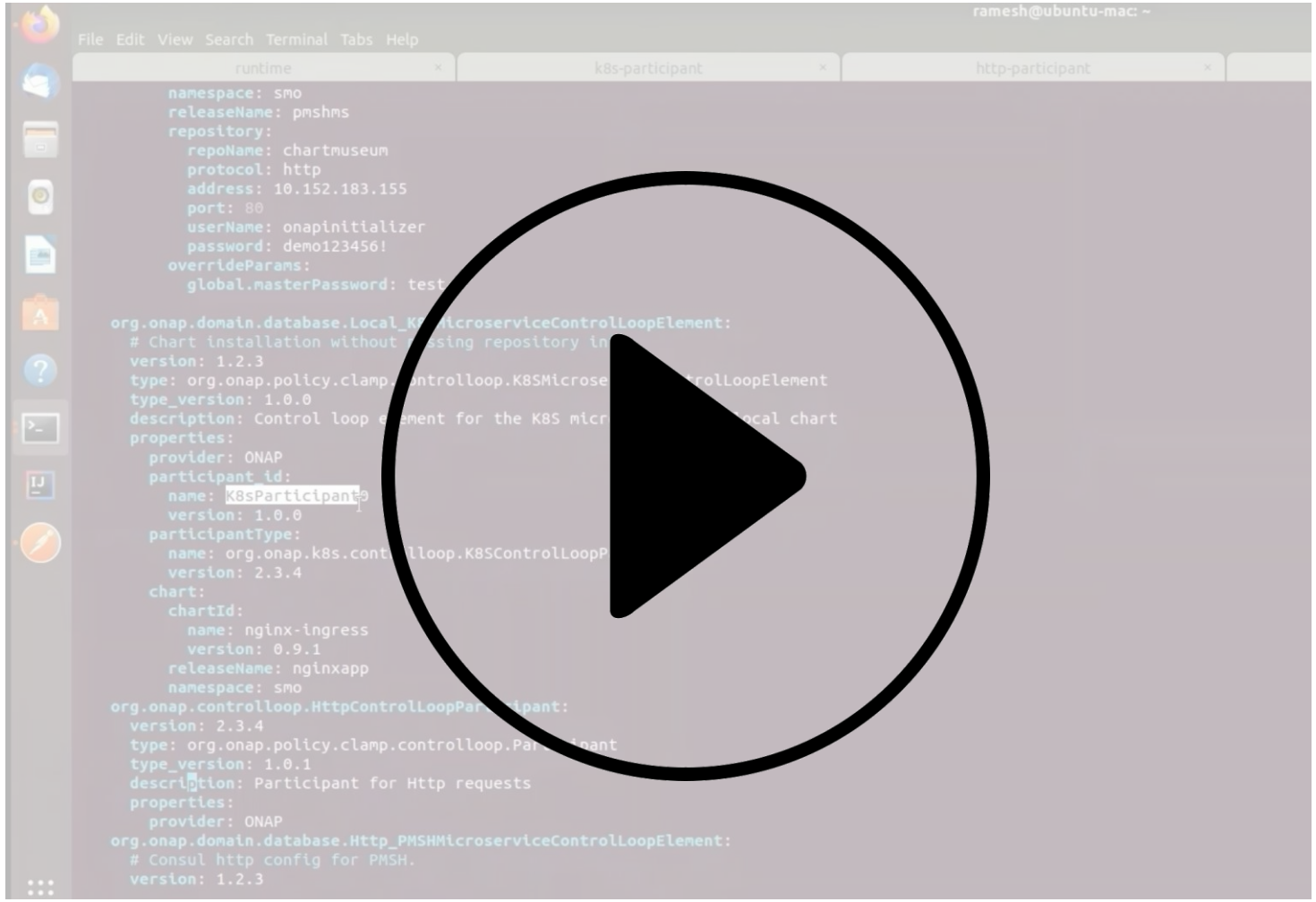
Bonus Topic

Standardising Service Exposure

3GPP CAPIF & O-RAN R1-SME

- We need to:
  - find services
  - register service providers (incl. rApps)
  - control service invokers (including rApps)
- 3GPP specifies CAPIF APIs for Service Registry
- O-RAN specifies R1 Service Catalog

Demo

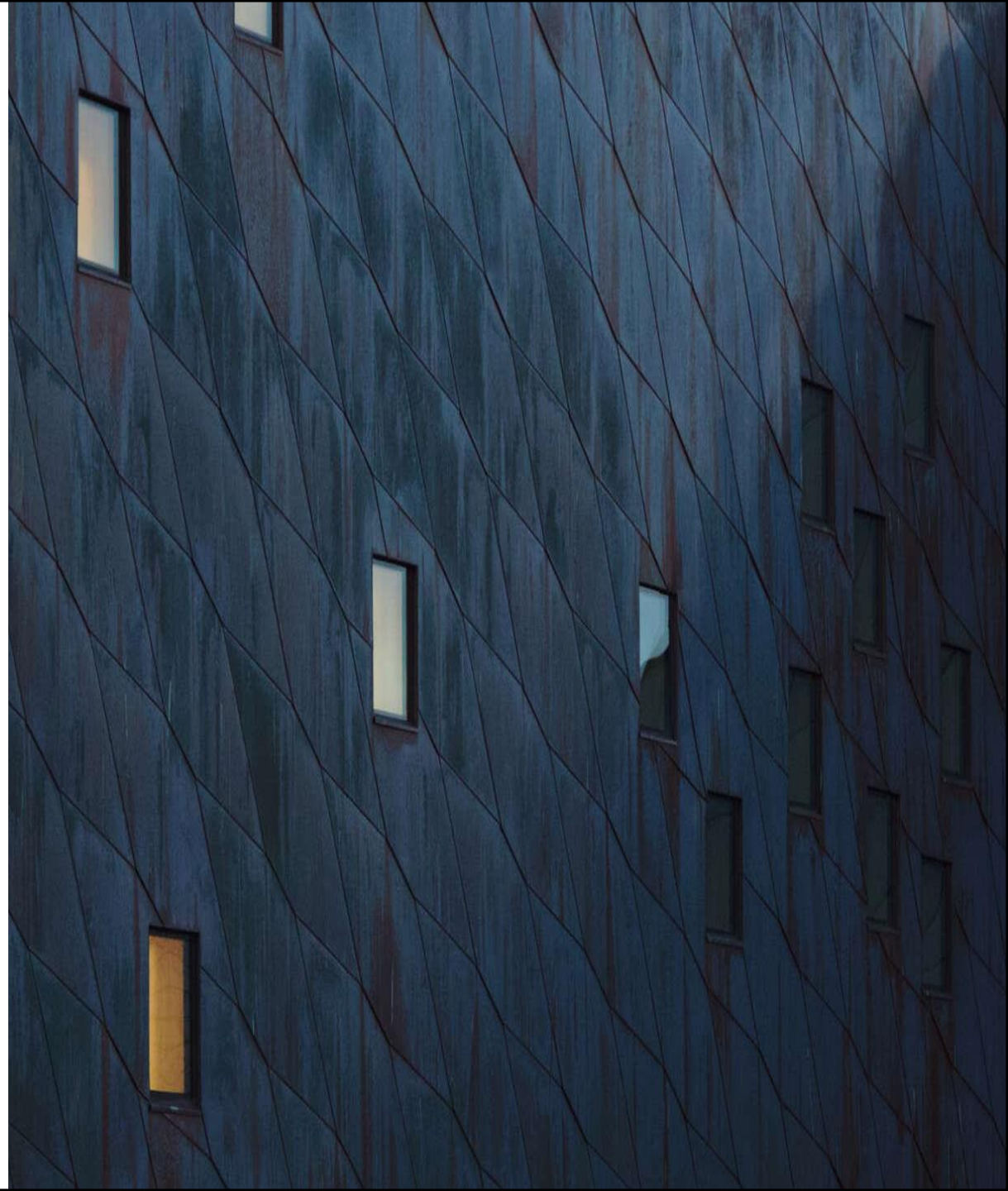

ramesh@ubuntu-mac: ~
File Edit View Search Terminal Tabs Help
runtime
k8s-participant
http-participant
namespace: smo
releaseName: pmshms
repository:
repoName: chartmuseum
protocol: http
address: 10.152.183.155
port: 80
userName: onapinitializer
password: demo123456!
overrideParams:
global.masterPassword: test
Chart installation without passing repository in
version: 1.2.3
version: 1.0.0
version: 2.3.4
chartId:
name: nginx-ingress
version: 0.9.1
releaseName: nginxapp
namespace: smo
version: 2.3.4
version: 1.0.1
Participant for Http requests
provider: ONAP
Consul http config for PMSH.
version: 1.2.3

Bonus Topic

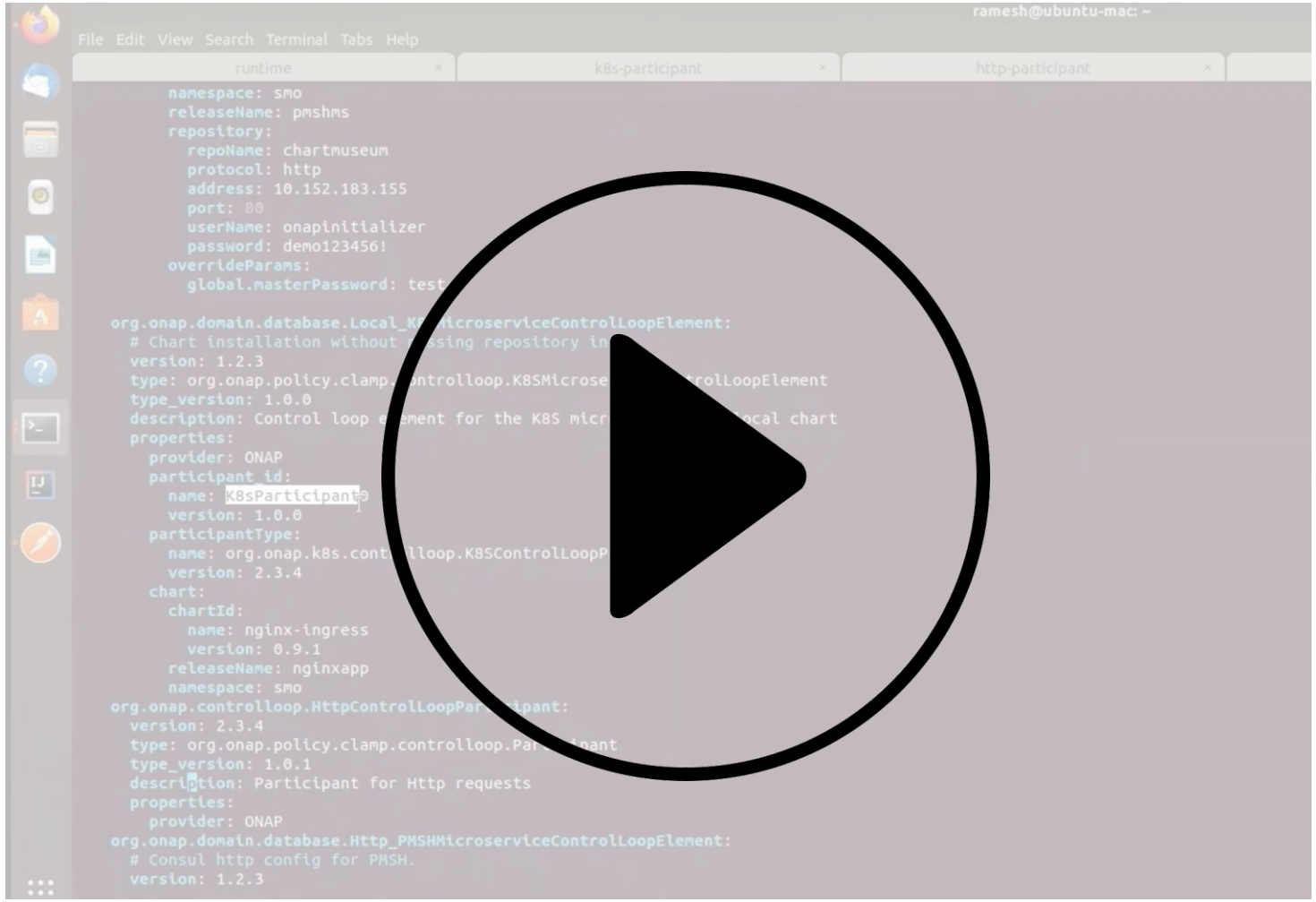
Enforcing more fine-grained exposure / access

Even more fine grained – OPA policies

- "Open Policy Agent"
- OPA policy checks at service invocation-time
- OPA policies can be included with app/service deployment charts
- OPA polices can be hosted on a bundle server and injected into your app through a sidecar



Demo


ramesh@ubuntu-mac: ~
File Edit View Search Terminal Tabs Help
runtime
k8s-participant
http-participant
namespace: smo
releaseName: pmshms
repository:
repoName: chartmuseum
protocol: http
address: 10.152.183.155
port: 80
userName: onapinitializer
password: demo123456!
overrideParams:
global.masterPassword: test
Chart installation without passing repository in
version: 1.2.3
version: 1.0.0
version: 2.3.4
chartId:
name: nginx-ingress
version: 0.9.1
releaseName: nginxapp
namespace: smo
version: 2.3.4
version: 1.0.1
Participant for Http requests
provider: ONAP
Consul http config for PMSH.
version: 1.2.3

Wrapping Up

Questions?

Ericsson Software Technology

O-RAN ALLIANCE

ONAP
OPEN NETWORK AUTOMATION PLATFORM