

CDK-BASED CONTINUOUS DEPLOYMENT FOR OSS


AWS User Group Tampere


March Meetup

7.3.2023

Laura Vuorenoja
Technology Strategist
OP Lab



 [@lauravuo](#)

 [@vuorenoja](#)

 [@lauravuo@fosstodon.org](mailto:lauravuo@fosstodon.org)



AGENDA

INTRODUCTION

PROJECT

FINDY AGENCY & AWS

PIPELINE


EXPERIENCE

Q&A

JANE OF ALL TRADES

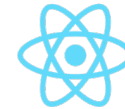
 @lauravuo

 @vuorenoja

 @lauravuo@fosstodon.org



Laura Vuorenoja
Technology Strategist
OP Lab



symbian



2005

2010

2015

2020

NOKIA

CYBERCOM
GROUP

tieto QUALCOMM

DB
DREAMBROKER

NEW
THINGS
CO

OP Lab



OP LAB

INNOVATION UNIT

OP Financial Group

~30 PEOPLE

Offices at Helsinki & Oulu

VARIOUS TASKS

Strategy work

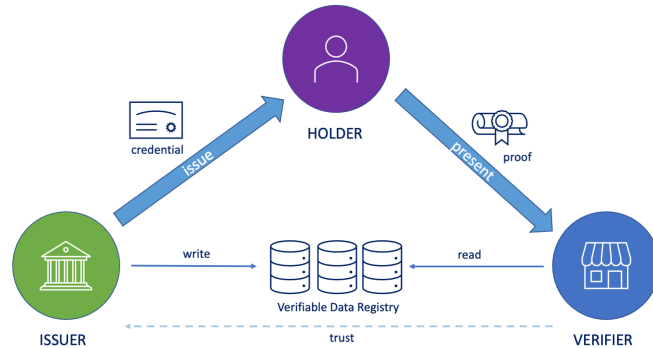
Company-wide innovation acceleration

Experimentation with new business and technologies

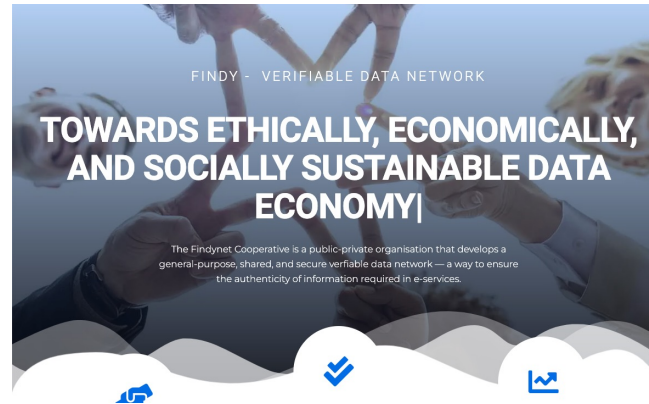
SSI EXPERT SINCE 2018

Pioneering research on self-sovereign identity

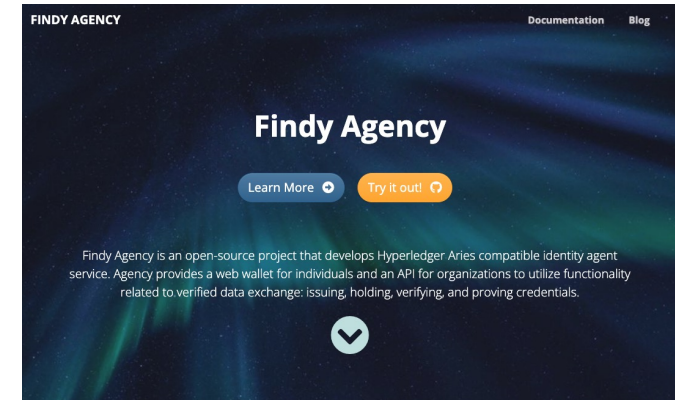
SELF-SOVEREIGN IDENTITY



New way of
handling identity
data – worldwide
movement

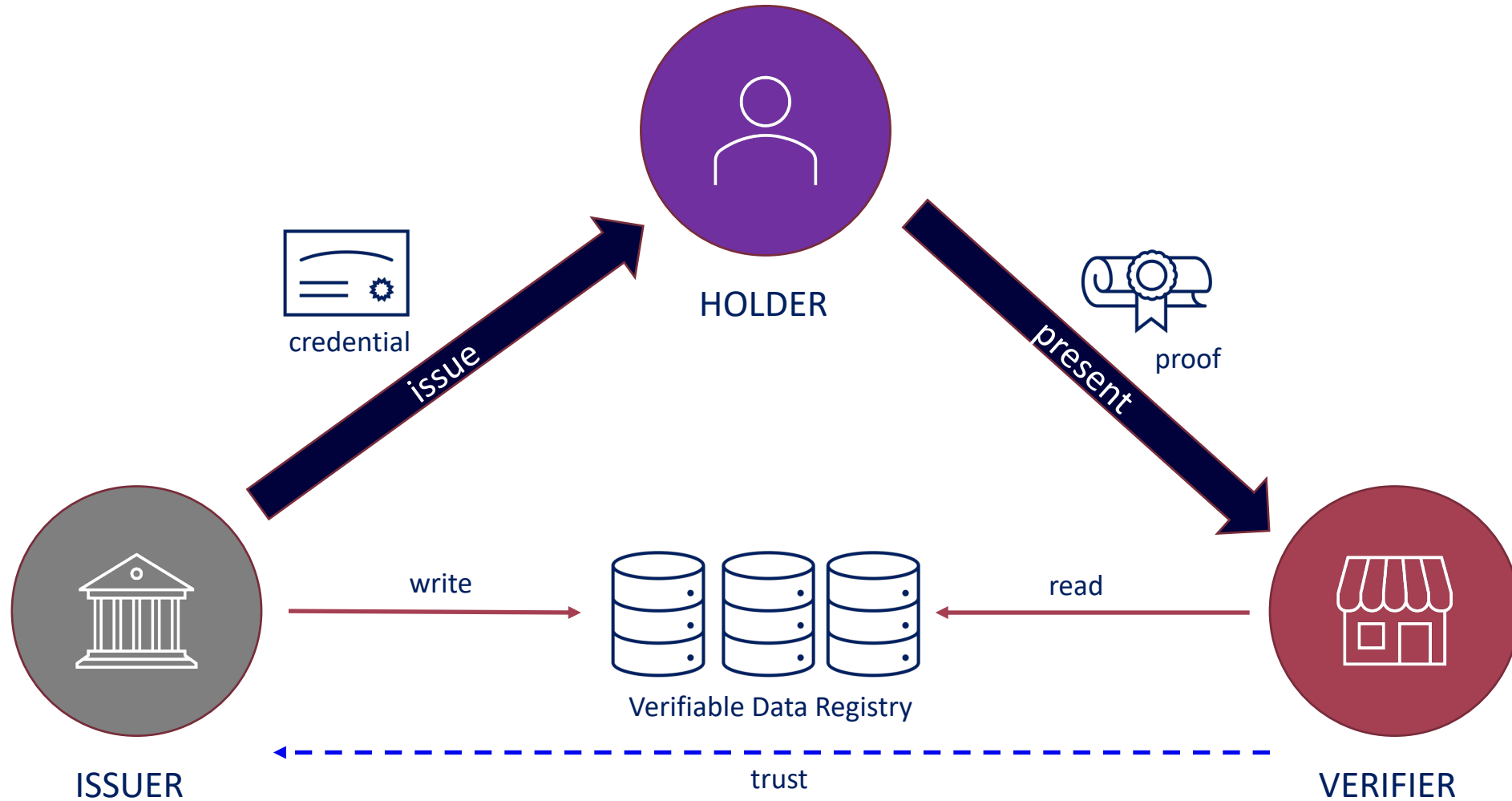


The Findynet
Cooperative –
public-private
effort

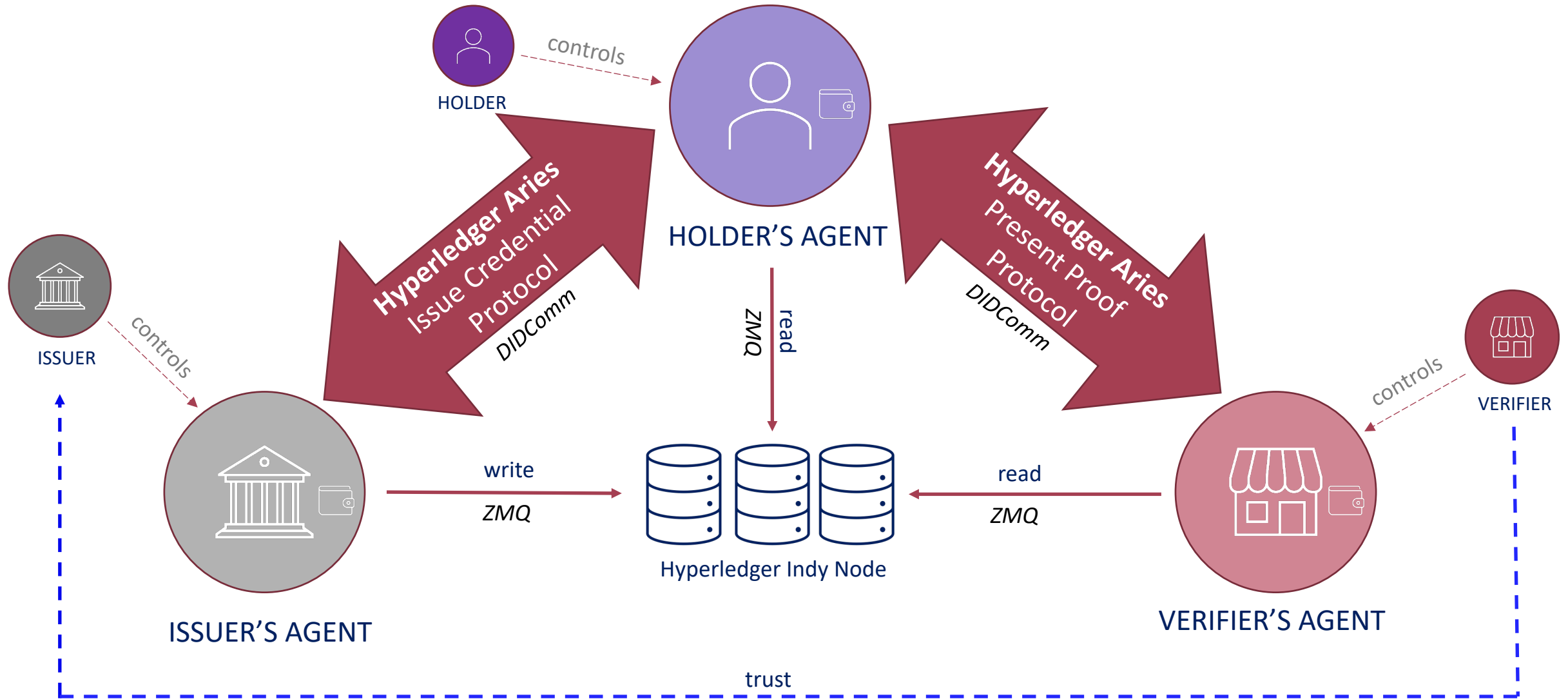


Findy Agency –
OSS developed by
OP Lab

VERIFIABLE CREDENTIALS



IMPLEMENTATION



FINDY AGENCY

FULLY OPEN-SOURCED

findy-network.github.io

HYPERLEDGER ARIES COMPATIBLE

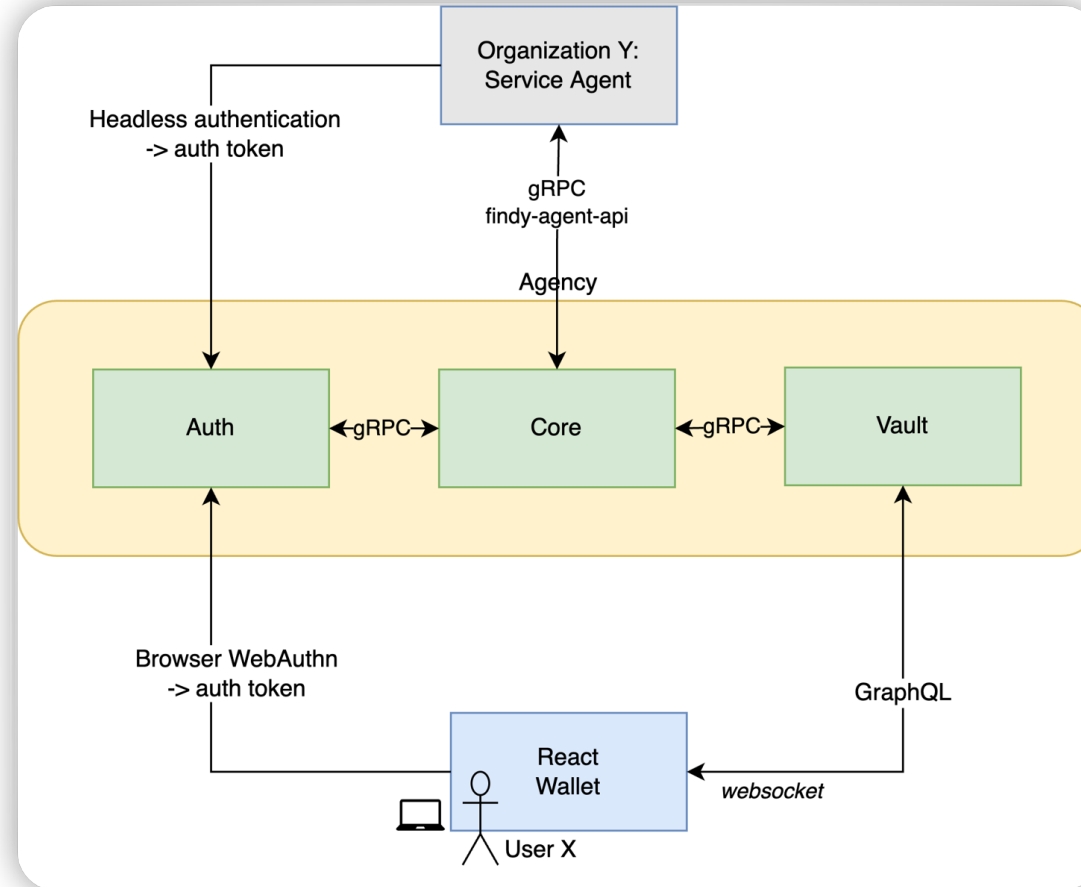
Interoperability as decentralization
guarantee

GO-MICROSERVICES

Outstanding performance

UNIQUE CLOUD- CENTRIC DESIGN

Pragmatic approach to sovereignty



FIDO2 AUTHENTICATION

First-class security both for individuals
and applications

gRPC-API

Streams simplifying development

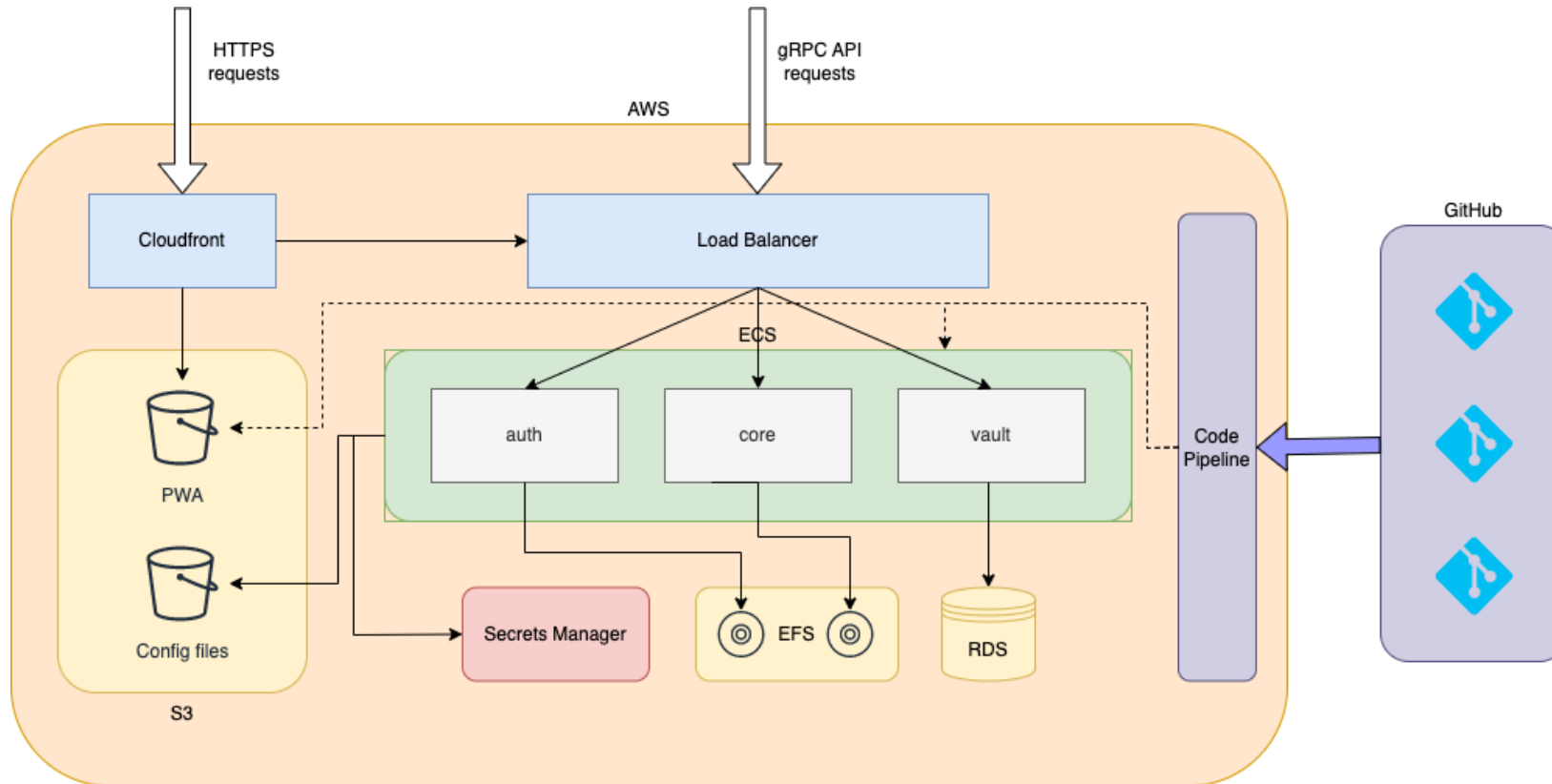
WEB WALLET

No need for mobile app

NO CODE

CLI provides all needed functionality
for rapid experiments and automation

AWS DEPLOYMENT



GITHUB PACKAGES

Container images available for anyone to download

ECS (FARGATE)

Container service orchestrates the agency backend

CLOUDFRONT + S3

Static web wallet application

CODE PIPELINE

New GitHub releases trigger version updates

EVOLUTION OF AGENCY IAC TOOLING

CloudFormation
Templates

CDK v1

CDK v2 & CDK
Pipelines

YAML

TYPESCRIPT in dev desktop

TYPESCRIPT in pipeline

```
Type: 'AWS::ECS::TaskDefinition'
Properties:
  ContainerDefinitions:
    - Essential: true
      HealthCheck:
        Command:
          - CMD-SHELL
          - 'curl -f http://localhost:8080/ready || exit 1'
        Interval: 30
        Retries: 10
        Timeout: 5
      Image: ghcr.io/findy-network/findy-agent
      MountPoints:
        - ContainerPath: /root
          ReadOnly: false
          SourceVolume: CoreVolume
      Name: findy-agency-core
      PortMappings:
        - ContainerPort: 8080
          Protocol: tcp
          ContainerPort: 50051
```

```
// Create container with environment variables, port configurations etc.
const container = task.addContainer(containerName, {
  image: ContainerImage.fromRegistry(imageURL),
  environment: environment.plainValues,
  secrets: mapSecrets(environment.secretSource, environment.secretValues)
  logging: new AwsLogDriver({
    streamPrefix: containerName,
    logRetention: RetentionDays.ONE_MONTH,
  }),
  healthCheck,
  portMappings: ports.map((containerPort) => ({ containerPort })),
});
```

```
// Create pipeline
const pipeline = this.createPipeline(
  githubConnectionArn,
  infraInput,
  frontendInput
);

// Add app to pipeline
const deploy = new InfraPipelineStage(this, "Deploy", {
  env: props.env,
});
const deployStage = pipeline.addStage(deploy);
```



CDK PIPELINES

CD PIPELINE FOR CDK APPS

Sets up a CodePipeline that builds, tests and deploys new version

SELF-UPDATING

Deployed only once from developer desktop

MULTIPLE ACCOUNTS OR REGIONS

Same application can be deployed to several targets using additional stages

OPINIONATED

The CDK way or the highway

SETUP

☰ README.md

Prerequisites

Note that the none of the following steps are optional.

1. Clone this repository to your own desktop. The initial [CDK pipeline](#) creation is done from your local computer according to these instructions. After the creation, the pipeline automatically reconfigures itself to deploy new stages or stacks.
2. `cd` to this folder: `cd aws-ecs`
3. Make sure you have installed [AWS CLI](#), node.js, AWS CDK, and Typescript:


```
# node
nvm install

# aws cdk
npm install -g aws-cdk

# typescript
npm install -g typescript
```
4. You need AWS Account. Create IAM user with full AWS access rights, and [copy the AWS Access keys via console](#) if you don't have them already.
5. You should have a domain available for the installation
 - If you have an existing domain, [create a public hosted zone to AWS Route53](#), and store the hosted zone nameservers to your domain settings (via the domain registrar UI).
 - If you [buy the domain via AWS](#), AWS will create the needed hosted zone for you automatically.
6. [Create GitHub codestar connection](#) so that the pipeline can clone the needed source code repositories and trigger automatic version updates. The connection is not used to access your repositories, only the public Findy Agency repositories, so you can for example create a dummy repository for it (if you don't want to allow full access).
7. Declare following environment variables:


```
# default region for AWS e.g. eu-north-1
export AWS_DEFAULT_REGION=<xxx>

# IAM user access key ID
export AWS_ACCESS_KEY_ID=<xxx>

# IAM user secret access key
export AWS_SECRET_ACCESS_KEY=<xxx>
```

TYPESCRIPT CDK APPLICATION

App contains all needed agency services

github.com/findy-network/findy-agent-infra

PREREQUISITIES

AWS Route53 Hosted Zone

GitHub codestar connection

Agency configuration

SETUP STEPS

1. Storing values for pipeline to parameter store (via bash script)
2. Bootstrapping CDK, synthing for the first time and storing context to parameter store
3. Storing values for deployment to secrets manager (via bash script)
4. Deploying pipeline

AWS CONSOLE

CodePipeline

Developer Tools > CodePipeline > Pipelines

Pipelines Info Refresh Notify View history Release change Delete pipeline Create pipeline

findyagencycp

Name	Most recent execution	Latest source revisions	Last executed
FindyAgencyPipeline	✔ Succeeded	findy-network_findy-agent - 706ba635 Merge pull request #300 from findy-network/dependabot/go_modules/dev/github.com/... findy-network_findy-agent-vault - 368b224d Merge pull request #142 from findy-network/release-make findy-network_findy-agent-auth - 3931fa0c Merge pull request #75 from findy-network/translator findy-network_findy-wallet-pwa - 1ac824f3 Merge pull request #338 from findy-network/use-overrides-to-fix-qr-reader-react-... findy-network_findy-agent-infra - 3da7c65d Merge pull request #119 from findy-network/dependabot/npm_and_yarn/aws-ecs/dev/c...	12 hours ago

CloudFormation

CloudFormation > Stacks > Deploy-FindyAgencyInfraStack

Deploy-FindyAgencyInfraStack Delete Update Stack actions Create stack

Stack info **Events** Resources Outputs Parameters Template Change sets

Overview

Stack ID	arn:aws:cloudformation:eu-central-1:123456789012:stack/Deploy-FindyAgencyInfraStack/	Description	-
Status	✔ UPDATE_COMPLETE	Status reason	-
Root stack	-	Parent stack	-
Created time	2022-09-26 14:44:26 UTC+0300	Deleted time	-
Updated time	2023-02-16 04:26:51 UTC+0200		
Drift status	⊖ NOT_CHECKED	Last drift check time	-
Termination protection	Disabled	IAM role	

STAGES 1-2/5

Source Succeeded
Pipeline execution ID: 02aa4d8e-c2ab-4e95-a500-dd61539abb7

findy-network_fi... GitHub (Version 2) Succeeded - 13 hours ago 706ba635	findy-network_fi... GitHub (Version 2) Succeeded - 13 hours ago 3931fa0c	findy-network_fi... GitHub (Version 2) Succeeded - 13 hours ago 3da7c65d	findy-network_fi... GitHub (Version 2) Succeeded - 13 hours ago 368b224d	findy-network_fi... GitHub (Version 2) Succeeded - 13 hours ago 1ac824f3
---	---	---	---	---

1ac824f3 findy-network_findy-wallet-pwa: Merge pull request #338 from findy-network/use-overrides-to-fix-qr-reader-react-
368b224d findy-network_findy-agent-vault: Merge pull request #142 from findy-network/release-make
3da7c65d findy-network_findy-agent-infra: Merge pull request #119 from findy-network/dependabot/npm_and_yarn/aws-ecs/dev/c
3931fa0c findy-network_findy-agent-auth: Merge pull request #75 from findy-network/translator
706ba635 findy-network_findy-agent: Merge pull request #300 from findy-network/dependabot/go_modules/dev/github.com/

Disable transition

Build Succeeded
Pipeline execution ID: 02aa4d8e-c2ab-4e95-a500-dd61539abb7

SynthStep
AWS CodeBuild
Succeeded
- 13 hours ago
Details

1ac824f3 findy-network_findy-wallet-pwa: Merge pull request #338 from findy-network/use-overrides-to-fix-qr-reader-react-
368b224d findy-network_findy-agent-vault: Merge pull request #142 from findy-network/release-make
3da7c65d findy-network_findy-agent-infra: Merge pull request #119 from findy-network/dependabot/npm_and_yarn/aws-ecs/dev/c
3931fa0c findy-network_findy-agent-auth: Merge pull request #75 from findy-network/translator
706ba635 findy-network_findy-agent: Merge pull request #300 from findy-network/dependabot/go_modules/dev/github.com/

Disable transition

```
const githubConnectionArn = StringParameter.valueForStringParameter(
  this,
  "/findy-agency/github-connection-arn"
);
const infraInput = CodePipelineSource.connection(
  "findy-network/findy-agent-infra",
  "master",
  {
    connectionArn: githubConnectionArn, // Created using the AWS console
  }
);
```

SOURCE

Changes to any backend service, frontend or infra app master branch triggers the pipeline

```
const pipeline = new CodePipeline(this, "Pipeline", {
  pipelineName: "FindyAgencyPipeline",
  synth: new CodeBuildStep("SynthStep", {
    input: infraInput,
    additionalInputs: {
      "../findy-wallet-pwa": frontendInput,
    },
  },
  installCommands: ["npm install -g aws-cdk"],
  buildEnvironment: {
    environmentVariables: {
      CDK_CONTEXT_JSON: {
        type: codebuild.BuildEnvironmentVariableType.PARAMETER_STORE,
        value: "/findy-agency/cdk-context",
      },
    },
  },
  commands: [
    "cd aws-ecs",
    `echo "$CDK_CONTEXT_JSON" > cdk.context.json`,
    "cat cdk.context.json",
    "npm ci",
    "npm run build",
    "npx cdk synth",
    "npm run pipeline:context",
  ],
});
```

BUILD

Performs synth: compiles the Typescript code to CloudFormation template

STAGES 3-4/5

UpdatePipeline Succeeded
Pipeline execution ID: 02aa4d8e-c2ab-4e95-a500-dd61539abb7

SelfMutate ⓘ
AWS CodeBuild
Succeeded
- 13 hours ago
[Details](#)

- [1ac824f3](#) findy-network_findy-wallet-pwa: Merge pull request #338 from findy-network/use-overrides-to-fix-qr-reader-react- ⋮
- [368b224d](#) findy-network_findy-agent-vault: Merge pull request #142 from findy-network/release-make ⋮
- [3da7c65d](#) findy-network_findy-agent-infra: Merge pull request #119 from findy-network/dependabot/npm_and_yarn/aws-ecs/dev/c ⋮
- [3931fa0c](#) findy-network_findy-agent-auth: Merge pull request #75 from findy-network/translator ⋮
- [706ba635](#) findy-network_findy-agent: Merge pull request #300 from findy-network/dependabot/go_modules/dev/github.com/ ⋮

UPDATE PIPELINE

Modifies pipeline with new stages and assets if necessary

Assets Succeeded
Pipeline execution ID: 02aa4d8e-c2ab-4e95-a500-dd61539abb7

FileAsset1	FileAsset2	FileAsset3	FileAsset4
ⓘ	ⓘ	ⓘ	ⓘ
AWS CodeBuild	AWS CodeBuild	AWS CodeBuild	AWS CodeBuild
Succeeded - 13 hours ago	Succeeded - 13 hours ago	Succeeded - 13 hours ago	Succeeded - 13 hours ago
Details	Details	Details	Details

- [1ac824f3](#) findy-network_findy-wallet-pwa: Merge pull request #338 from findy-network/use-overrides-to-fix-qr-reader-react- ⋮
- [368b224d](#) findy-network_findy-agent-vault: Merge pull request #142 from findy-network/release-make ⋮
- [3da7c65d](#) findy-network_findy-agent-infra: Merge pull request #119 from findy-network/dependabot/npm_and_yarn/aws-ecs/dev/c ⋮
- [3931fa0c](#) findy-network_findy-agent-auth: Merge pull request #75 from findy-network/translator ⋮
- [706ba635](#) findy-network_findy-agent: Merge pull request #300 from findy-network/dependabot/go_modules/dev/github.com/ ⋮

ASSETS

Prepares and publishes all file assets (S3) and Docker images (ECR) for deployment

Deploy Succeeded
 Pipeline execution ID: 02aa4d8e-c2ab-4e95-a500-dd61539abb7

FindyAgencyInfraStack.Prepare
 AWS CloudFormation
 Succeeded - 13 hours ago

FindyAgencyInfraStack.Deploy
 AWS CloudFormation
 Succeeded - 13 hours ago

FindyAgencyBuildFrontendStep
 AWS CodeBuild
 Succeeded - 13 hours ago

FindyAgencyDeployBackendStep
 AWS CodeBuild
 Succeeded - 13 hours ago

FindyAgencyAdminOnboardStep
 AWS CodeBuild
 Succeeded - 13 hours ago

FindyAgencyDeployFrontendStep
 AWS CodeBuild
 Succeeded - 13 hours ago

FindyAgencyE2ETestStep
 AWS CodeBuild
 Succeeded - 13 hours ago

```
// Add app to pipeline
const deploy = new InfraPipelineStage(this, "Deploy", {
  env: props.env,
});
const deployStage = pipeline.addStage(deploy);

const ecsUpdateStep = this.createECSUpdateStep(
  deploy.clusterName,
  deploy.serviceArn
);
deployStage.addPost(ecsUpdateStep);

// Add frontend build step
const frontBuildStep = this.createFrontendBuildStep(frontendInput);
deployStage.addPost(frontBuildStep);

// Add frontend deploy step
const frontDeployStep = this.createFrontendDeployStep(
  frontBuildStep.primaryOutput
);
deployStage.addPost(frontDeployStep);

// Add admin onboard
const adminOnboardStep = this.createAdminOnboardTestStep(
  infraInput,
  ecsUpdateStep.primaryOutput
);
deployStage.addPost(adminOnboardStep);

// Add e2e test
const e2eTestStep = this.createE2ETestStep(
  frontendInput,
  adminOnboardStep.primaryOutput
);
deployStage.addPost(e2eTestStep);

// SNS topic for pipeline notifications
const notificationTopic = new Topic(this, "FindyAgencyPipelineNotification");
```

STAGE 5/5

PREPARE

Prepares infra stack

DEPLOY

Deploys infra stack

BUILD & DEPLOY FRONTEND

Build frontend code and deploy to S3

DEPLOY BACKEND

Update ECS service using CLI

ONBOARD ADMIN & E2E TEST

Configuration and testing

```
createE2ETestStep(
  input: CodePipelineSource,
  waitReadyOutput: cdk.pipelines.FileSet | undefined
) {
  return new CodeBuildStep("FindyAgencyE2ETestStep", {
    input,
    additionalInputs: { waitReadyOutput: waitReadyOutput! },
    projectName: "FindyAgencyE2ETest",
    commands: [
      // install findy-agent-cli
      "curl https://raw.githubusercontent.com/findy-network/findy-agent-cli/HEAD/install.sh > install.sh",
      "chmod a+x install.sh",
      "sudo ./install.sh -b /bin",

      // save certificate
      "echo Connecting to $AGENCY_API_URL",
      "./e2e/dl-cert.sh",

      // install needed deps
      "npm install nightwatch@2.6.15",
      "full_version=$(google-chrome --product-version)",
      "chrome_version=$(echo "${full_version%.*.*}"),
```

- 1ac824f3 findy-network_findy-wallet-pwa: Merge pull request #338 from findy-network/use-overrides-to-fix-qr-reader-react- []
- 368b224d findy-network_findy-agent-vault: Merge pull request #142 from findy-network/release-make []
- 3da7c65d findy-network_findy-agent-infra: Merge pull request #119 from findy-network/dependabot/npm_and_yarn/aws-ecs/dev/c []
- 3931fa0c findy-network_findy-agent-auth: Merge pull request #75 from findy-network/translator []
- 706ba635 findy-network_findy-agent: Merge pull request #300 from findy-network/dependabot/go_modules/dev/github.com/ []



YIKES 🤯

DETERMINISM?

Sometimes just retrying things works

DEBUGGING

CloudFormation Events-tab and “Request failed 400” is just not enough

THE CDK WAY

Still unclear what it is. Obviously not open-source way.

SECRET THINGS UNDER THE HOOD

With a little bit of extra cost



LIKES 🥰

CDK INSTEAD OF CLOUDFORMATION TEMPLATES

Writing, sharing and testing the definitions is easier

PIPELINE CREATES AND UPDATES DEPLOYMENT

Changes via version control

State is managed in the pipeline

Less custom hacks


MULTIPLE ACCOUNTS OR REGIONS


Support out-of-the-box


IT WORKS!

With a little bit of highway

THANK YOU!
QUESTIONS?

 [@lauravuo](#)

 [@vuorenoja](#)

 [@lauravuo@fosstodon.org](mailto:lauravuo@fosstodon.org)



Laura Vuorenoja
Technology Strategist
OP Lab
findy-network.github.io