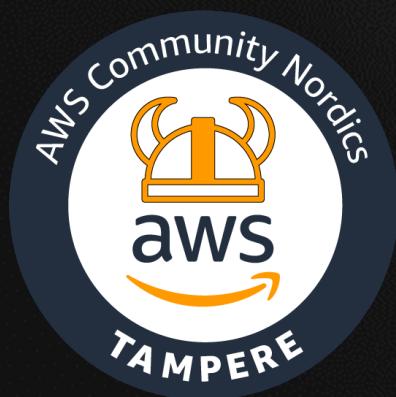


# CDK-BASED CONTINUOUS DEPLOYMENT FOR OSS

AWS User Group Tampere

March Meetup

7.3.2023



Laura Vuorenaja  
Technology Strategist  
OP Lab

 @lauravuo  
 @vuorenaja  
 @lauravuo@fosstodon.org



# AGENDA

INTRODUCTION

PROJECT

FINDY AGENCY & AWS

PIPELINE

EXPERIENCE

Q&A

# JANE OF ALL TRADES

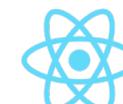
 [@lauravuo](https://twitter.com/lauravuo)  
 [@vuorenaja](https://twitter.com/vuorenaja)  
 [@lauravuo@fosstodon.org](https://fosstodon.org/@lauravuo)



Laura Vuorenaja  
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

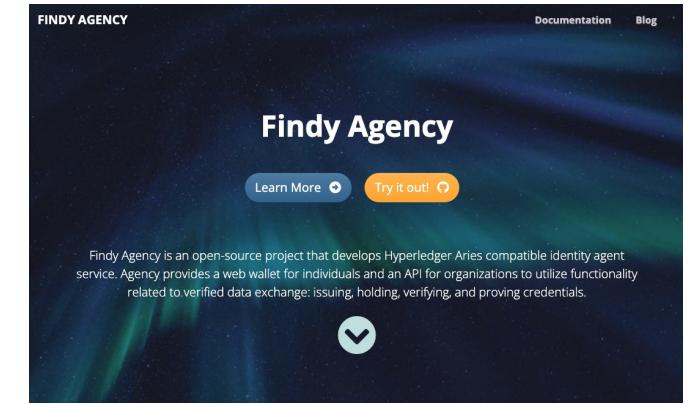
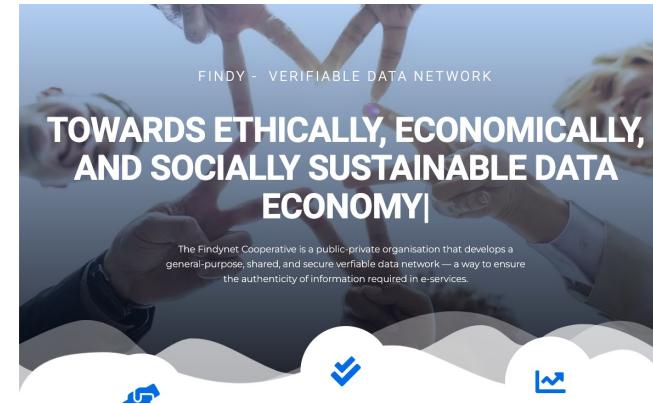
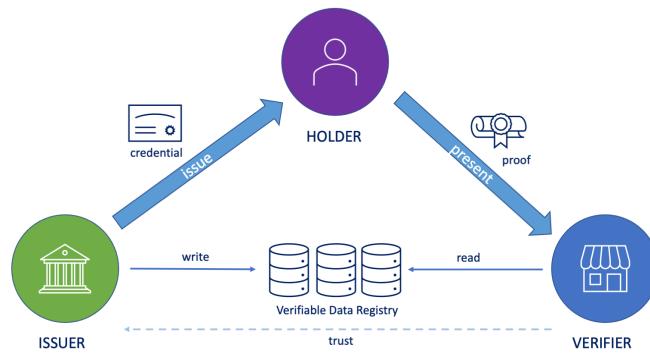
Company-wide innovation acceleration

Experimentation with new business and technologies

## SSI EXPERT SINCE 2018

Pioneering research on self-sovereign identity

# SELF-SOVEREIGN IDENTITY

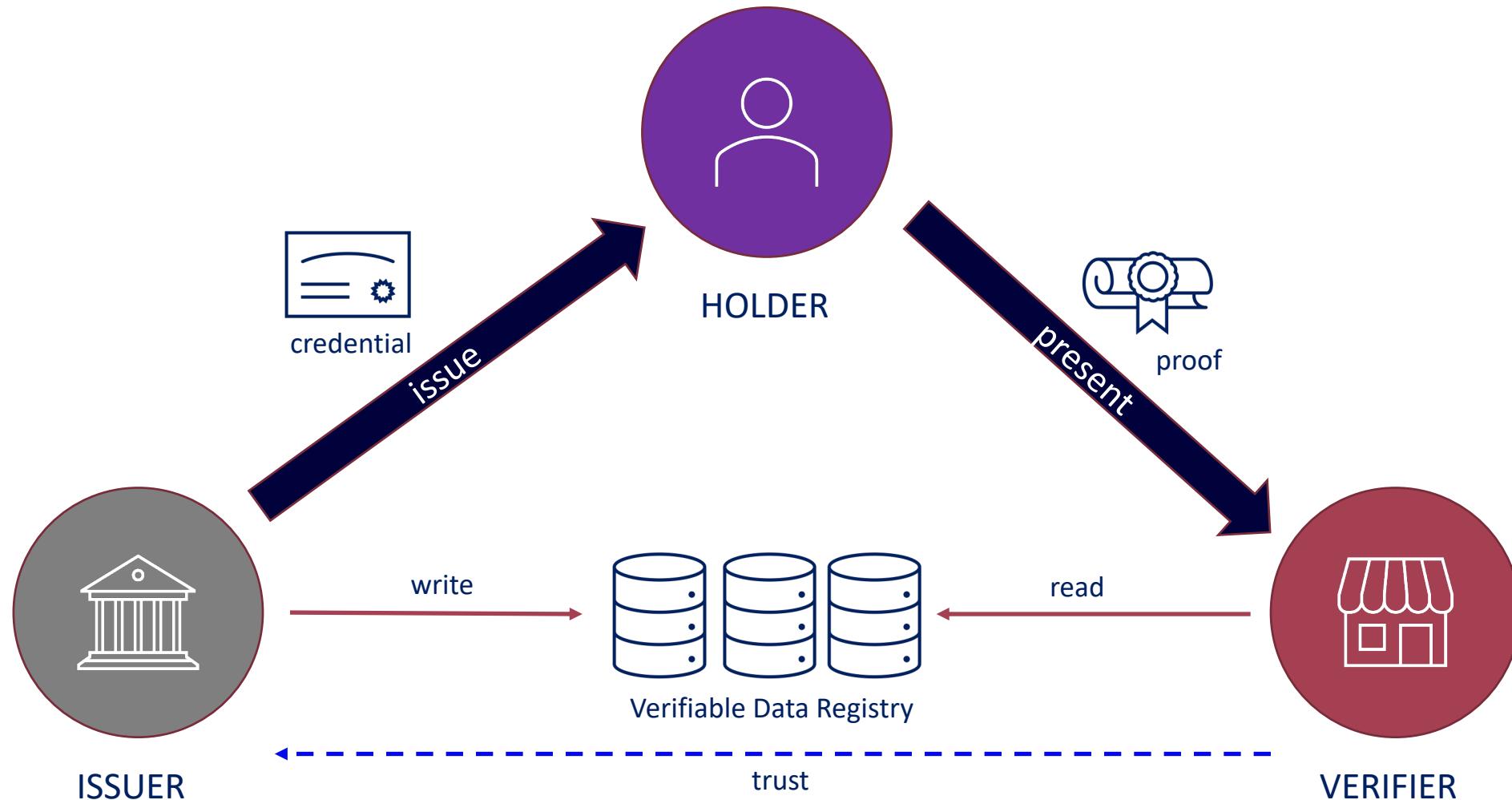


New way of handling identity data – worldwide movement

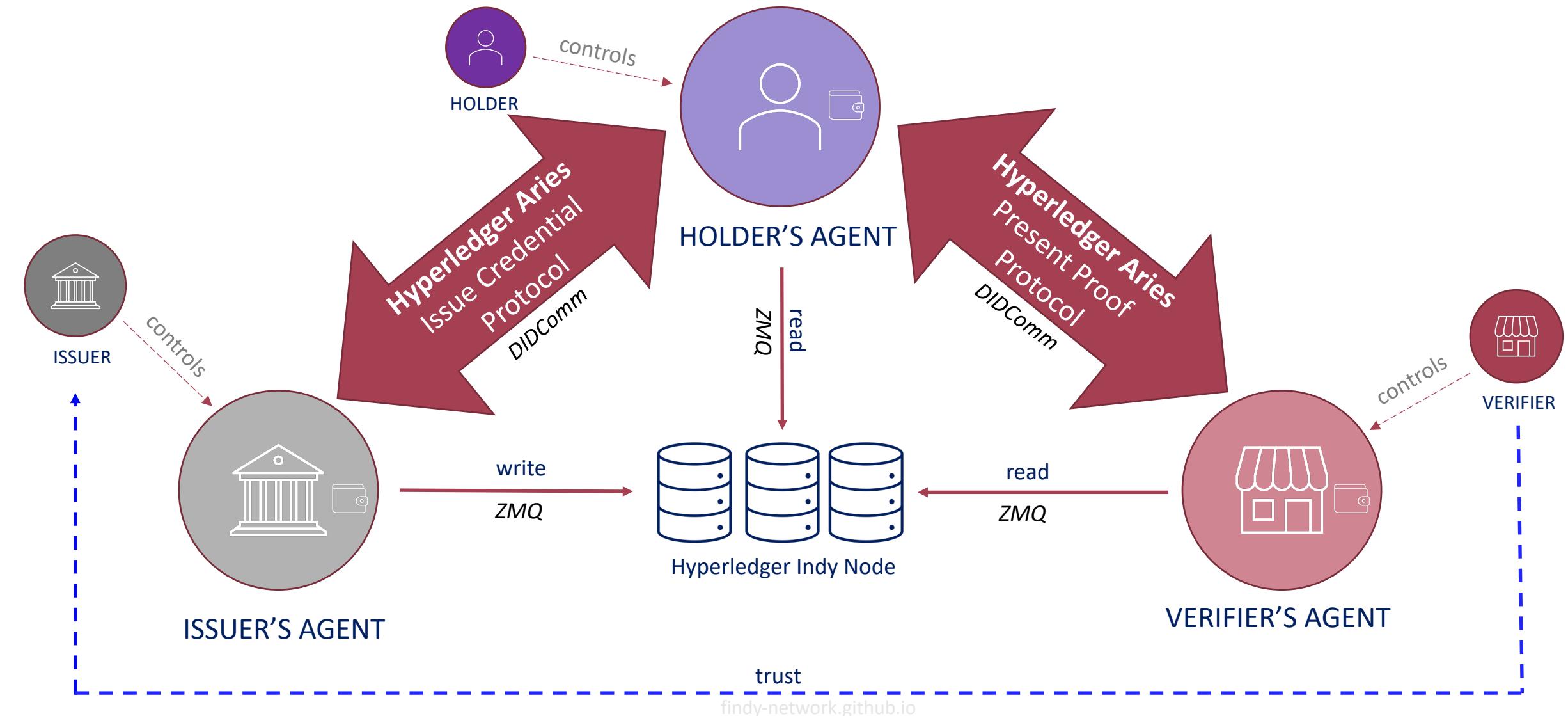
The Findynet Cooperative – public-private effort

Findy Agency – OSS developed by OP Lab

# VERIFIABLE CREDENTIALS



# IMPLEMENTATION



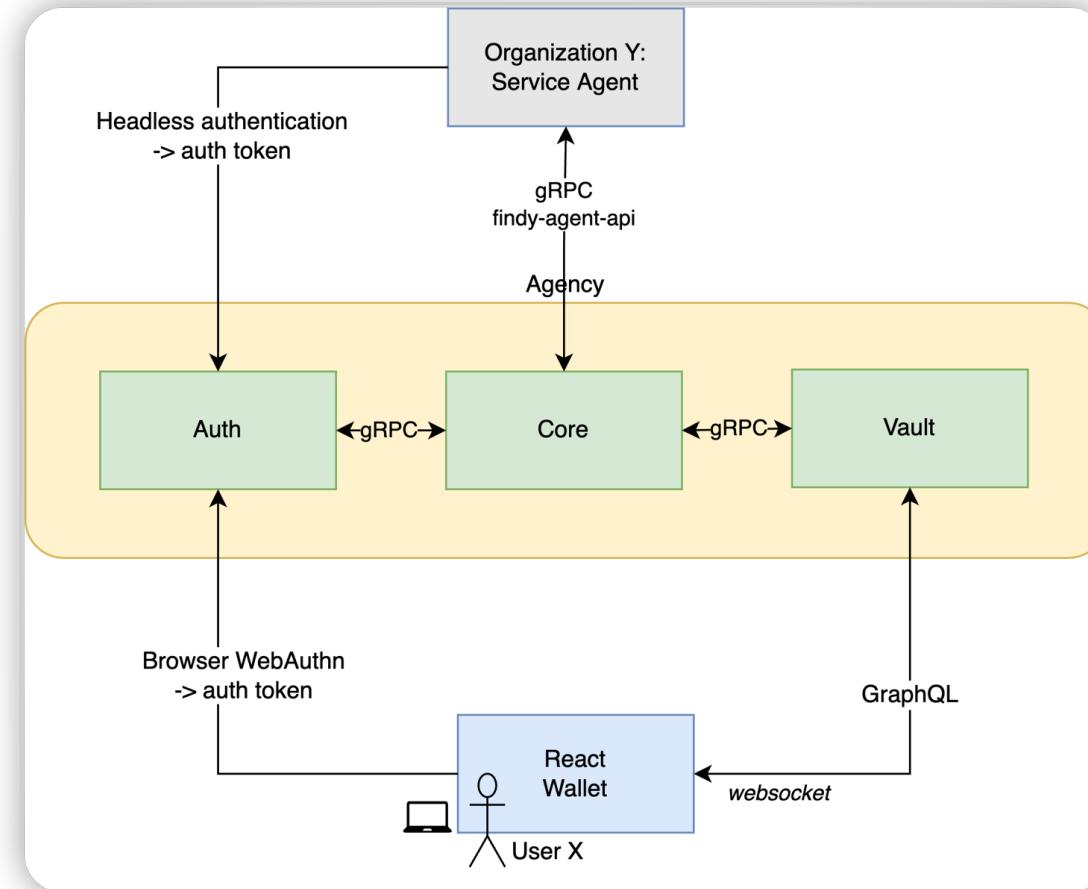
# FINDY AGENCY

**FULLY OPEN-SOURCED**  
[findy-network.github.io](https://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

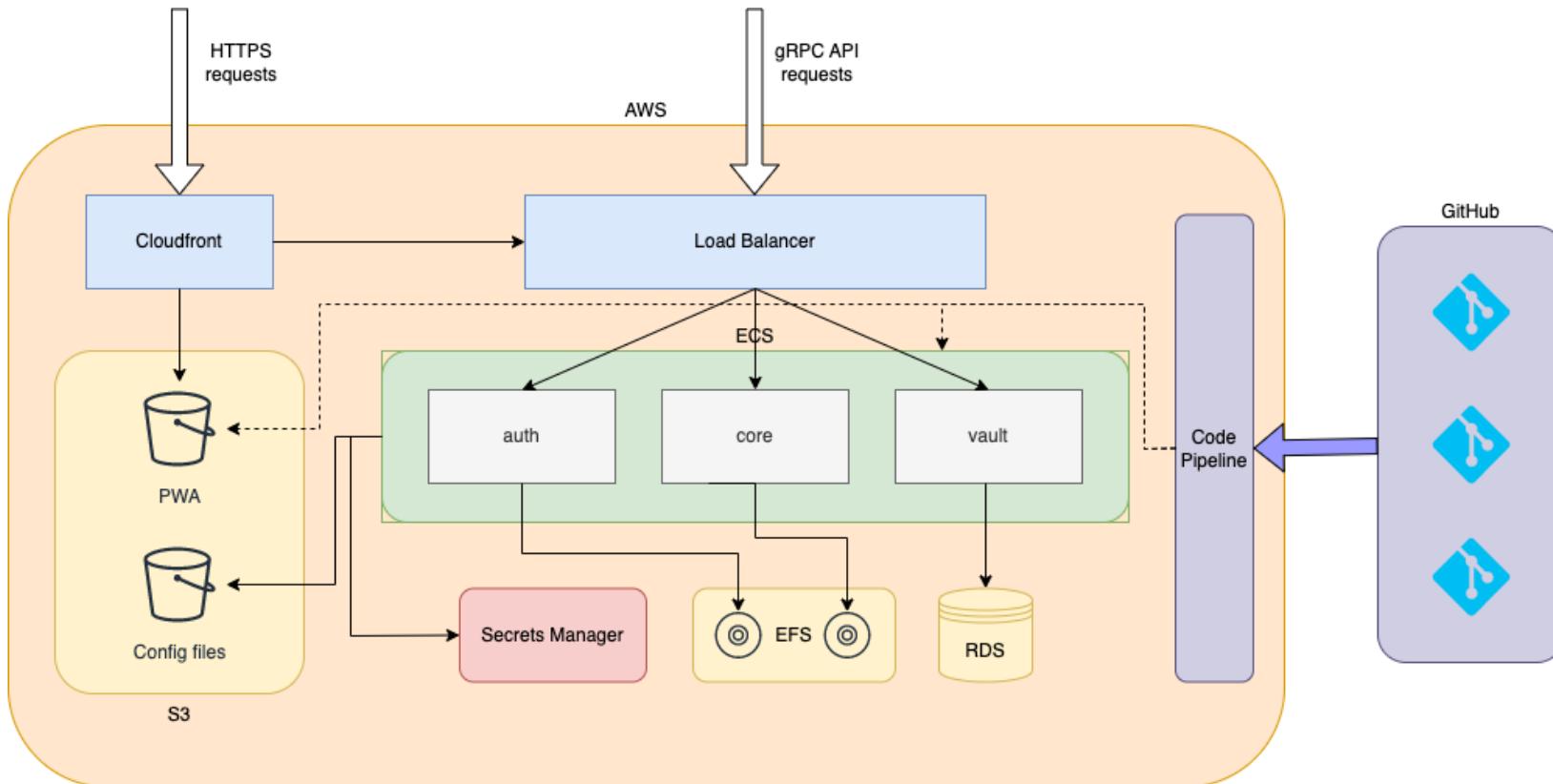
## WEB WALLET

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

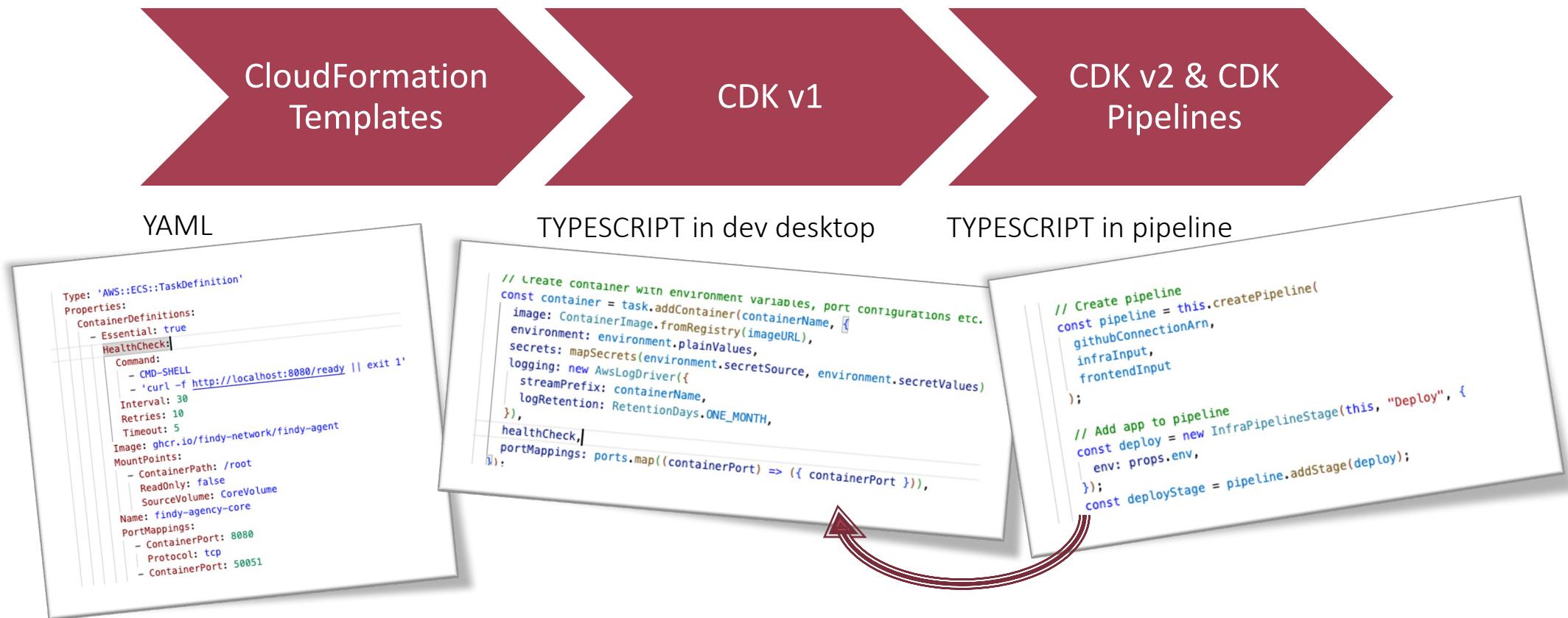
## CLOUDFRONT + S3

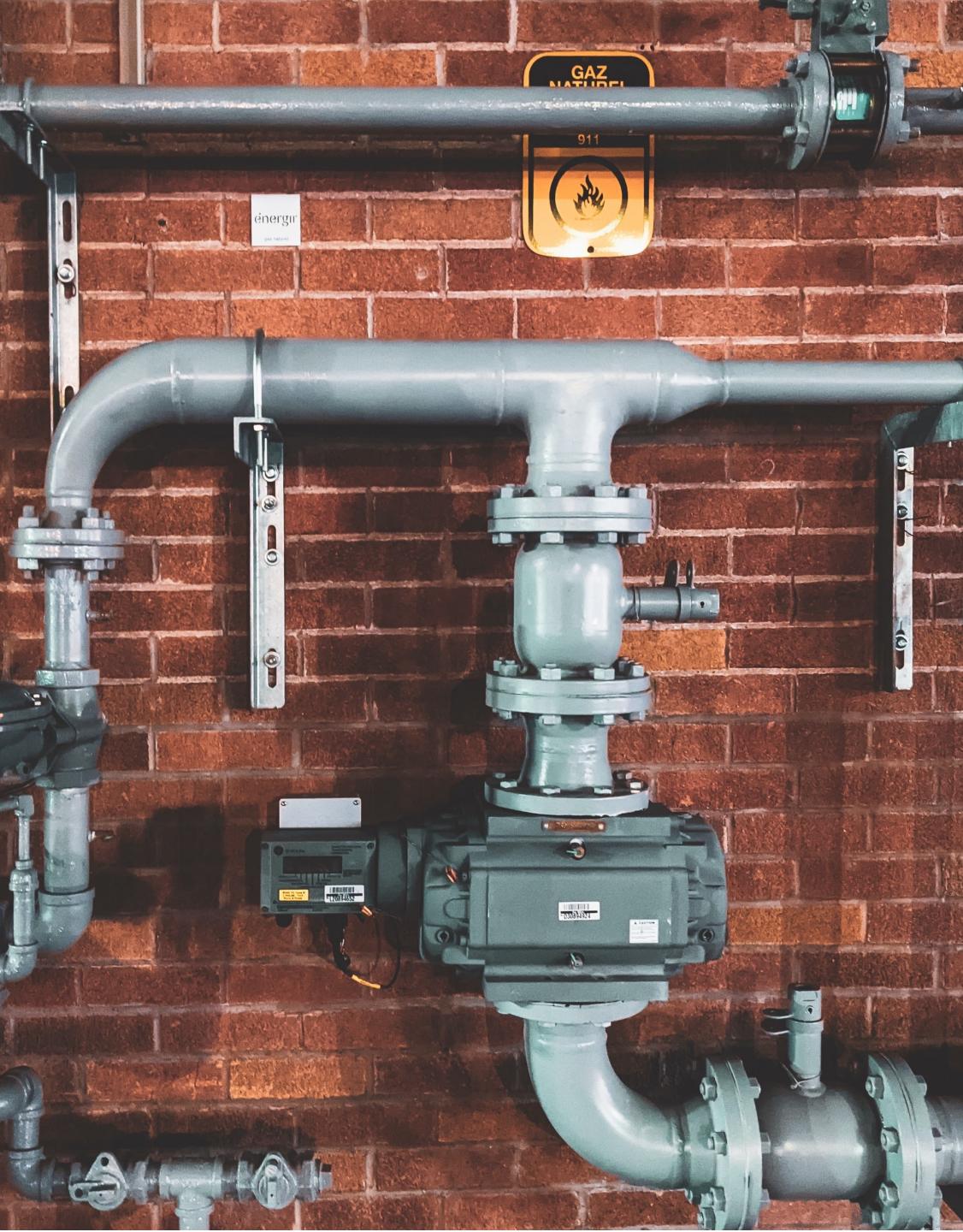
Static web wallet application

## CODE PIPELINE

New GitHub releases trigger version updates

# EVOLUTION OF AGENCY IAC TOOLING





# 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.

- 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.
- cd to this folder: cd aws-ecs
- 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
```
- 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.
- 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.
- 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).
- 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](https://github.com/findy-network/findy-agent-infra)

## PREREQUISITES

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

The screenshot shows the AWS CodePipeline console. At the top, there are buttons for 'Info' (disabled), 'Notify' (with a dropdown arrow), 'View history', 'Release change', 'Delete pipeline', and 'Create pipeline'. A search bar contains the text 'findyagency'. Below the header, there are three tabs: 'Name', 'Most recent execution', and 'Latest source revisions'. The 'Most recent execution' tab is selected, showing a single row for the 'FindyAgencyPipeline'. The status is 'Succeeded' with a green checkmark icon. To the right of the pipeline name, the status is also 'Succeeded'. The 'Latest source revisions' tab shows a list of commits from the GitHub repository 'findy-network/findy-agent':

- 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...

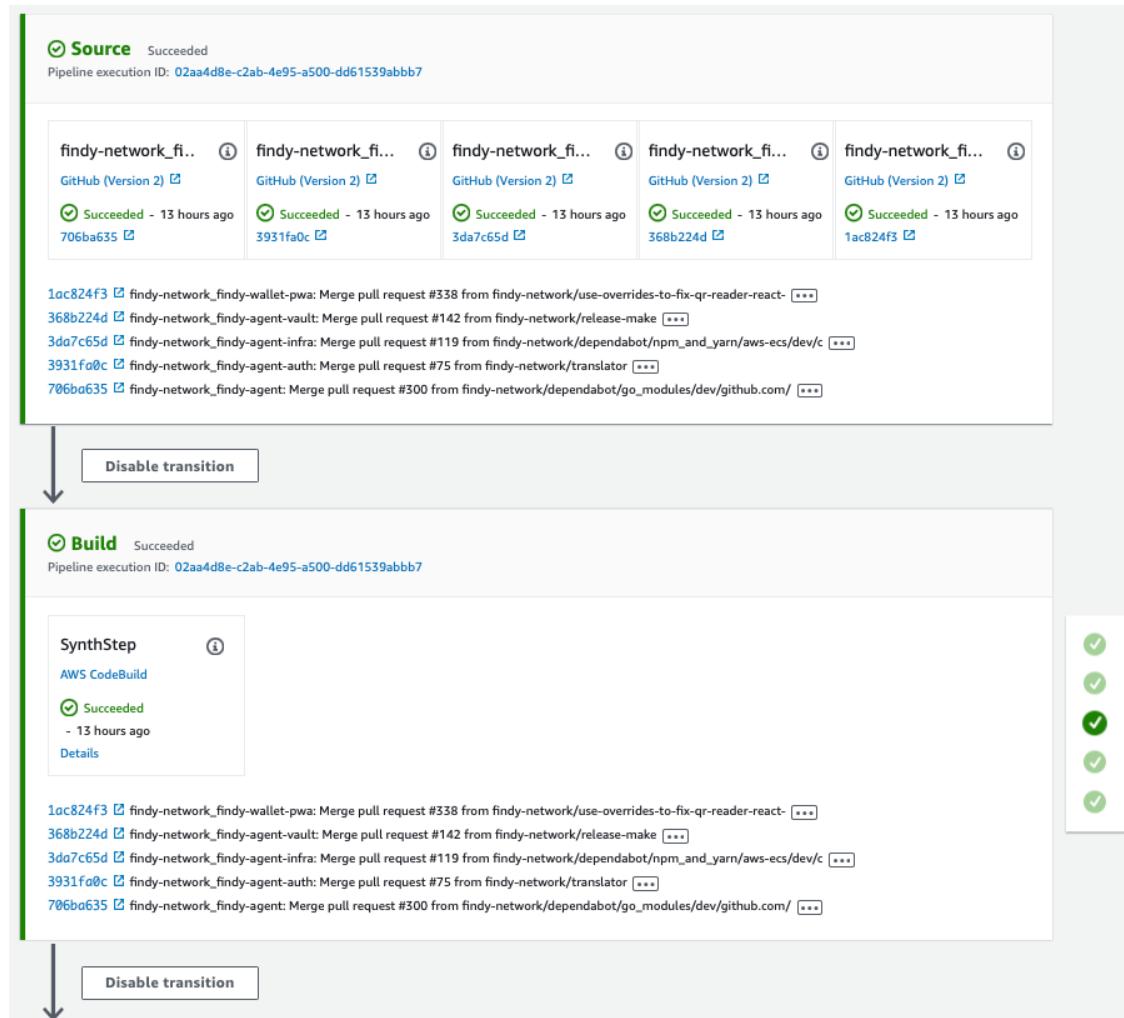
The 'Last executed' tab shows the pipeline was last executed 12 hours ago.

## CloudFormation

The screenshot shows the AWS CloudFormation console. At the top, there are buttons for 'Delete', 'Update', 'Stack actions ▾', and 'Create stack ▾'. Below the header, there are tabs: 'Stack info' (selected), 'Events' (circled in red), 'Resources', 'Outputs', 'Parameters', 'Template', and 'Change sets'. The 'Events' tab is currently active. The main area displays the 'Deploy-FindyAgencyInfraStack' stack information:

| Overview               |  |
|------------------------|--|
| Stack ID               | <a href="#">arn:aws:cloudformation:eu-central-1:123456789012:stack/Deploy-FindyAgencyInfraStack/</a> |
| Description            | -  |
| Status                 | <span>UPDATE_COMPLETE</span>   |
| 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   |
| Last drift check time  | -  |
| Drift status           | <span>NOT_CHECKED</span>   |
| IAM role               | -  |
| Termination protection | Disabled   |

# STAGES 1-2/5



## SOURCE

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

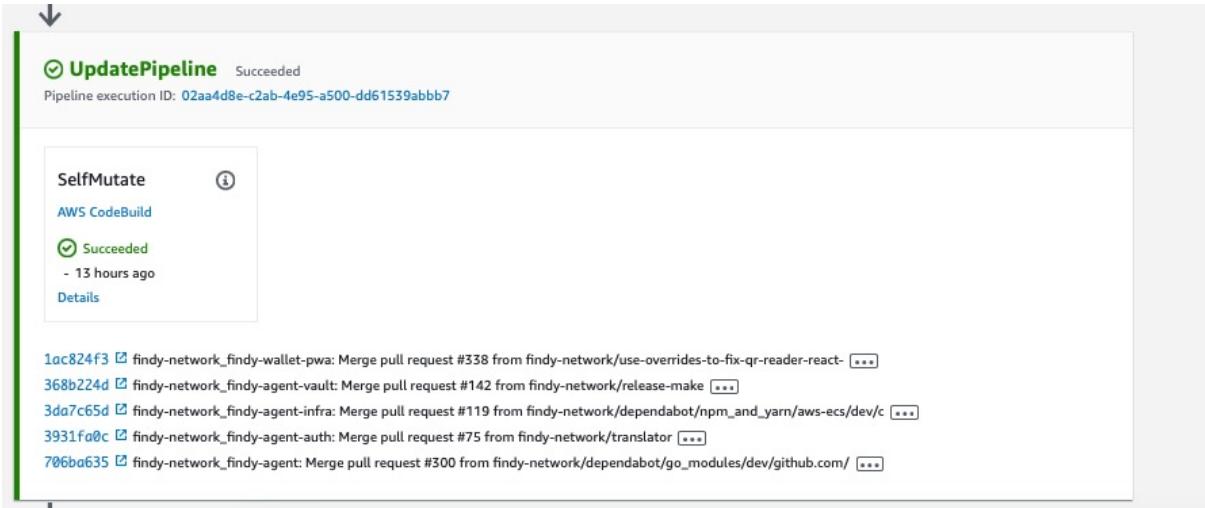
```
const githubConnectionArn = StringParameter.valueForStringParameter(
  this,
  "/findy-agency/github-connection-arn"
);
const infraInput = CodePipelineSource.connection(
  "findy-network/findy-agent-infra",
  "master",
  {
    connectionArn: githubConnectionArn, // Created using the AWS console
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

```
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

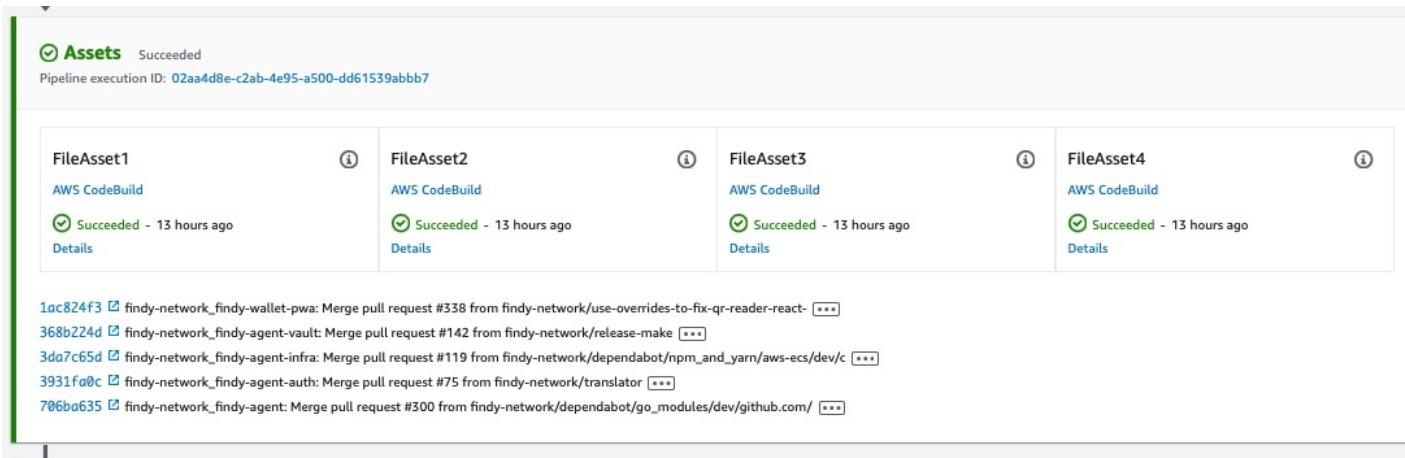
Performs synth: compiles the Typescript code to CloudFormation template

# STAGES 3-4/5



## UPDATE PIPELINE

Modifies pipeline with new stages and assets if necessary



## ASSETS

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



Deploy Succeeded

Pipeline execution ID: 02aa4d8e-c2ab-4e95-a500-dd61539abbb7

FindyAgencyInfraStack.Prepare



AWS CloudFormation

SUCCEEDED - 13 hours ago

Details



FindyAgencyInfraStack.Deploy



AWS CloudFormation

SUCCEEDED - 13 hours ago

Details



FindyAgencyBuildFrontendStep



AWS CodeBuild

SUCCEEDED - 13 hours ago

Details

FindyAgencyDeployBackendStep



AWS CodeBuild

SUCCEEDED - 13 hours ago

Details



FindyAgencyAdminOnboardStep



AWS CodeBuild

SUCCEEDED - 13 hours ago

Details

FindyAgencyDeployFrontendStep



AWS CodeBuild

SUCCEEDED - 13 hours ago

Details



FindyAgencyE2ETestStep



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/ [\*\*\*]

```
// 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, "FindyAgencyPipelineNotificationTopic");
```

# 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%.*.*}")',
    ],
  });
}
```

findy-network.github.io



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

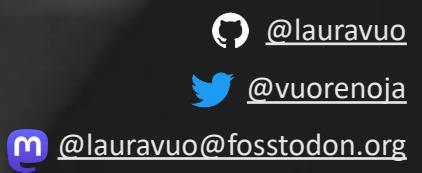
Support out-of-the-box

### IT WORKS!

With a little bit of highway

# THANK YOU!

# QUESTIONS?



Laura Vuorenaja  
Technology Strategist  
OP Lab  
[findy-network.github.io](https://findy-network.github.io)