Keyfactor
Tech Days
2023

Containerized 5G PKI & Enterprise PKI

Ibrahim Akkulak

Senior Security Consultant

Rakuten Symphony

Ellen Boehm

SVP IoT Strategy & Operations

Keyfactor

Abstract

Part 1 Containerized 5G PKI

- 5G PKI & Architectures & HA model
- Journey from RSA to ECDSA

Part 2 Automation in PKI

- Automating enrollments with standard protocols
- Automating Re-enrollments with Keyfactor Command

Part 1 EJBCA:

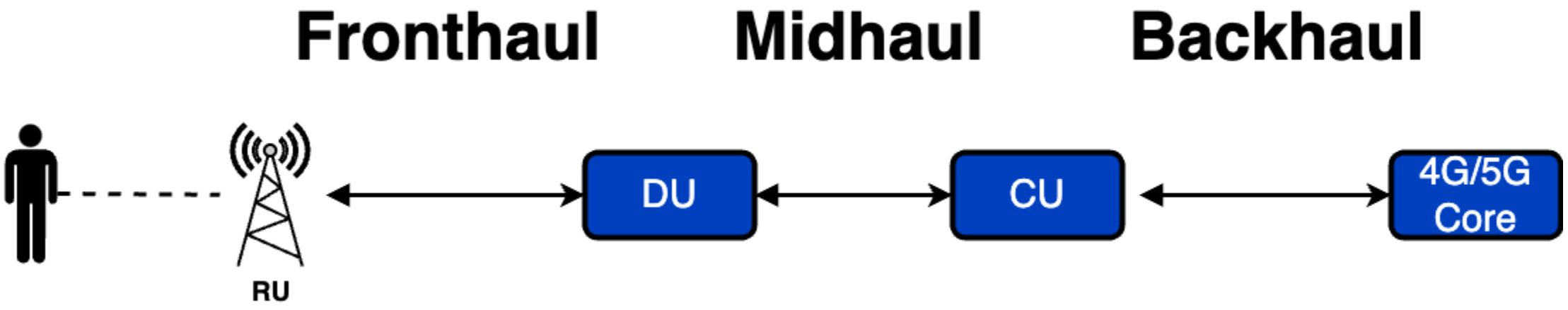
Containerized 5G PKI

Challenges & Solutions

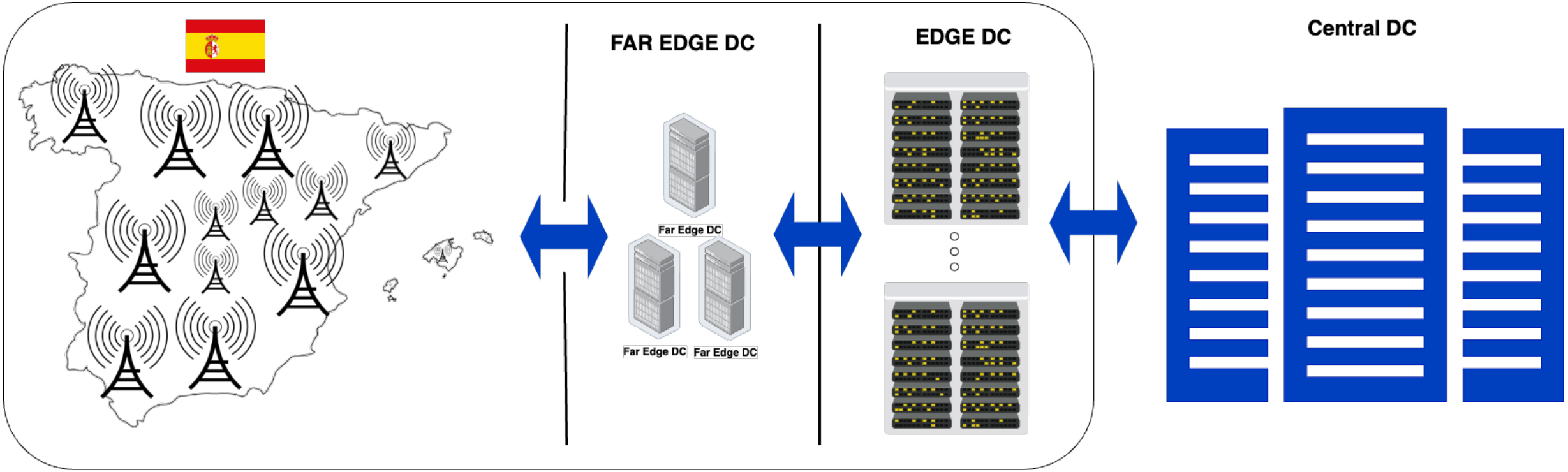
Containerized 5G PKI

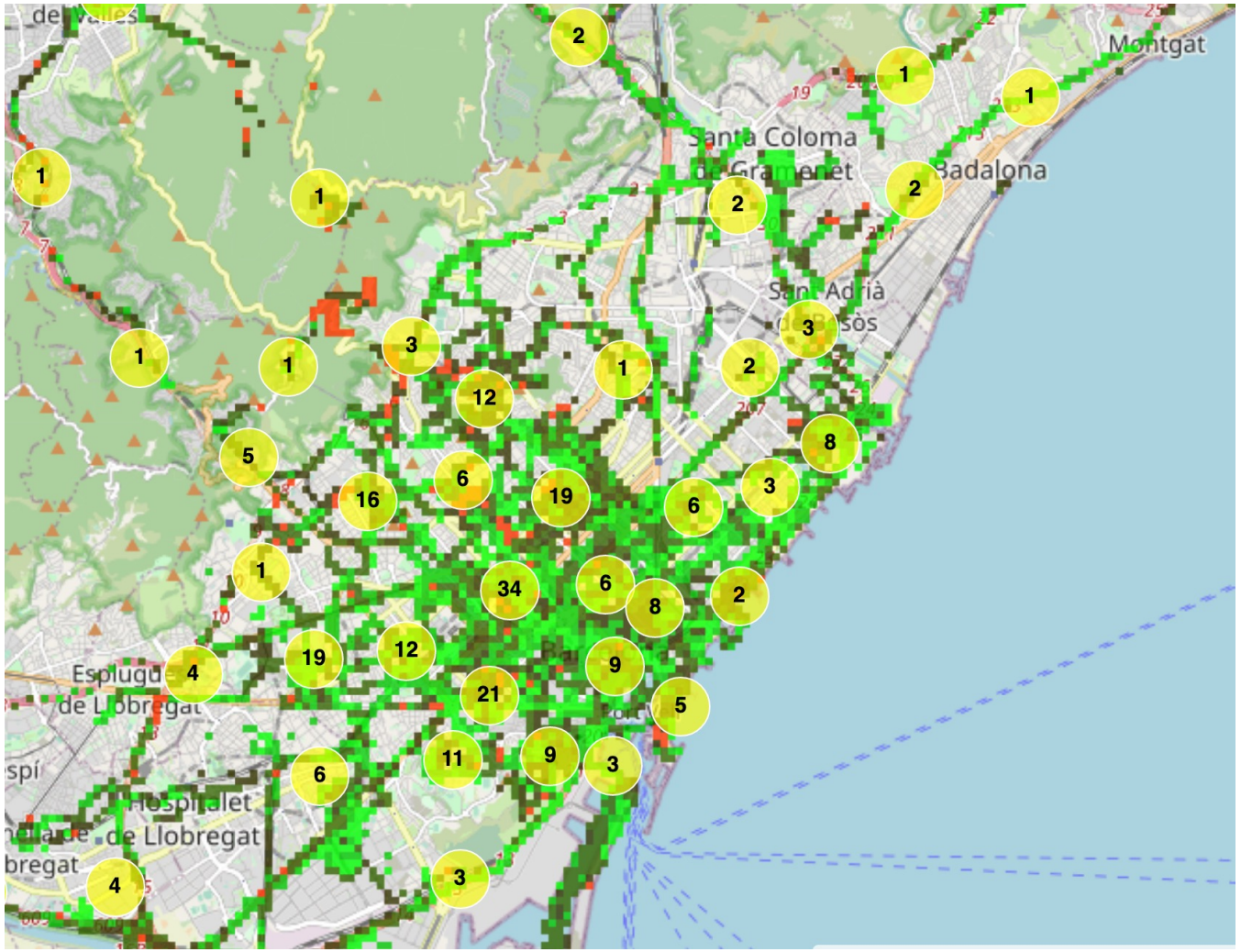
- 5G Network
- 5G PKI Use-case
- Containerized 5G PKI

5G Open RAN



5G Overview


FAR EDGE DC
EDGE DC
Central DC
Far Edge DC
Far Edge DC
Far Edge DC



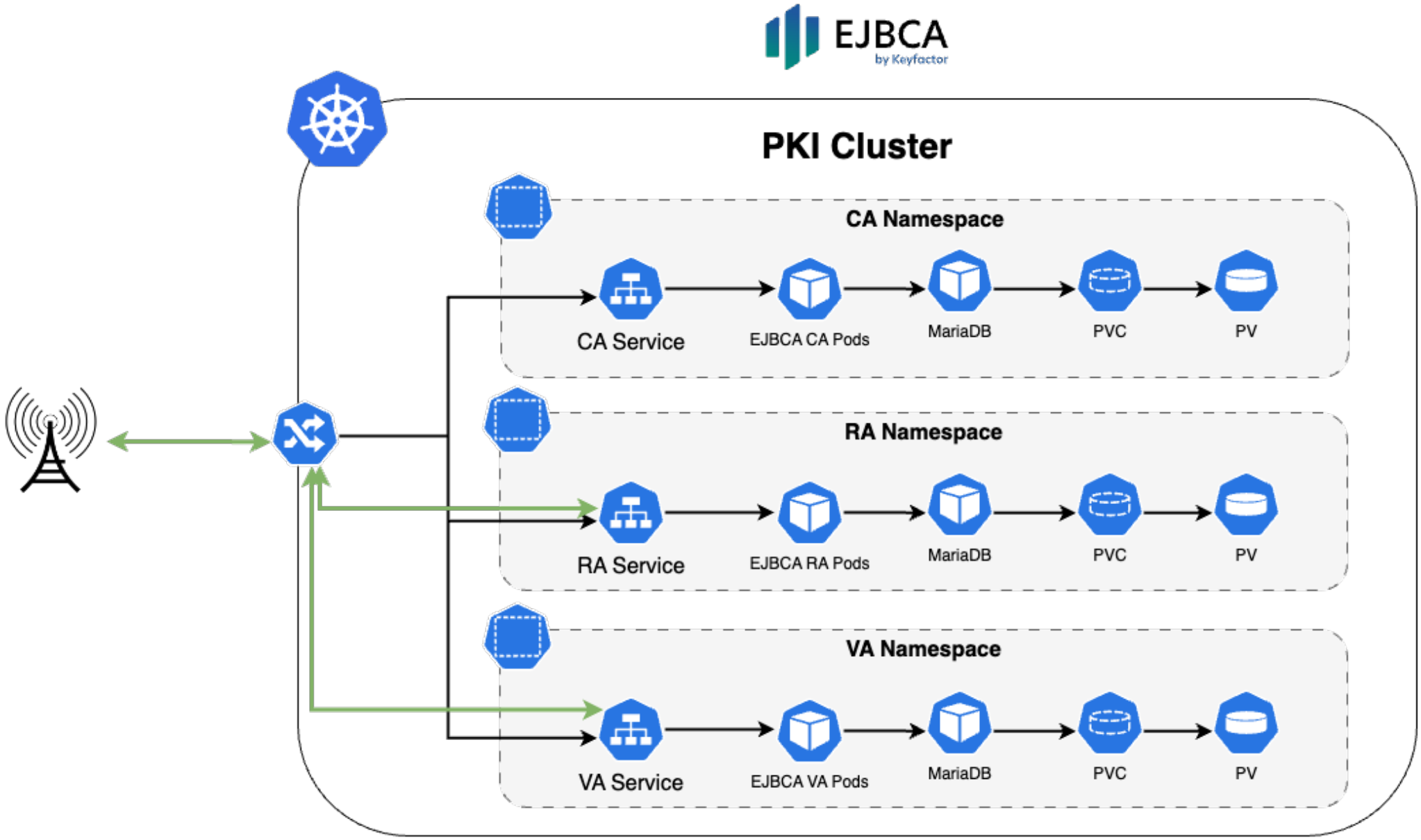
Barcelona 4G Cell Sites

How many Certificates are required?

5G RU	4G RU	4G/5G DU	4G/5G CU
~ roughly 20k of sites	~ roughly 20k of sites	~ roughly 1000	~ roughly 100

“

5G Networks in European countries requires roughly **50k active** certificates


EJBCA
by Keyfactor
PKI Cluster
CA Namespace
CA Service
EJBCA CA Pods
MariaDB
PVC
PV
RA Namespace
RA Service
EJBCA RA Pods
MariaDB
PVC
PV
VA Namespace
VA Service
EJBCA VA Pods
MariaDB
PVC
PV

Containerized PKI?

Why we go with containerized PKI?

1. Industry standard
2. Shift left strategy – DevSecOps
3. Fast & reliable & secure redployment with Helm Charts [1]
4. Zero trust deployment & Automation

[1] https://github.com/Keyfactor/ejbca-ce-helm-meetup

ECDSA Journey

The journey from RSA certificates to ECDSA

RSA to ECDSA Journey

Challenges:

- Building inventory
- Testing ECDSA certificates with applications
- Guidances

1. Regulatory Requirements

Germany (New TR-02102-2 – released Jan 2023)

NIST

Why we took the journey?

- Regulatory
- More secure
- Future readiness

BSI recommends RSA only until 2024

Only specific signatures

Enforcement of TLS 1.3 is required after 2024

2. Inventory

Build an inventory of certificate specification requirements

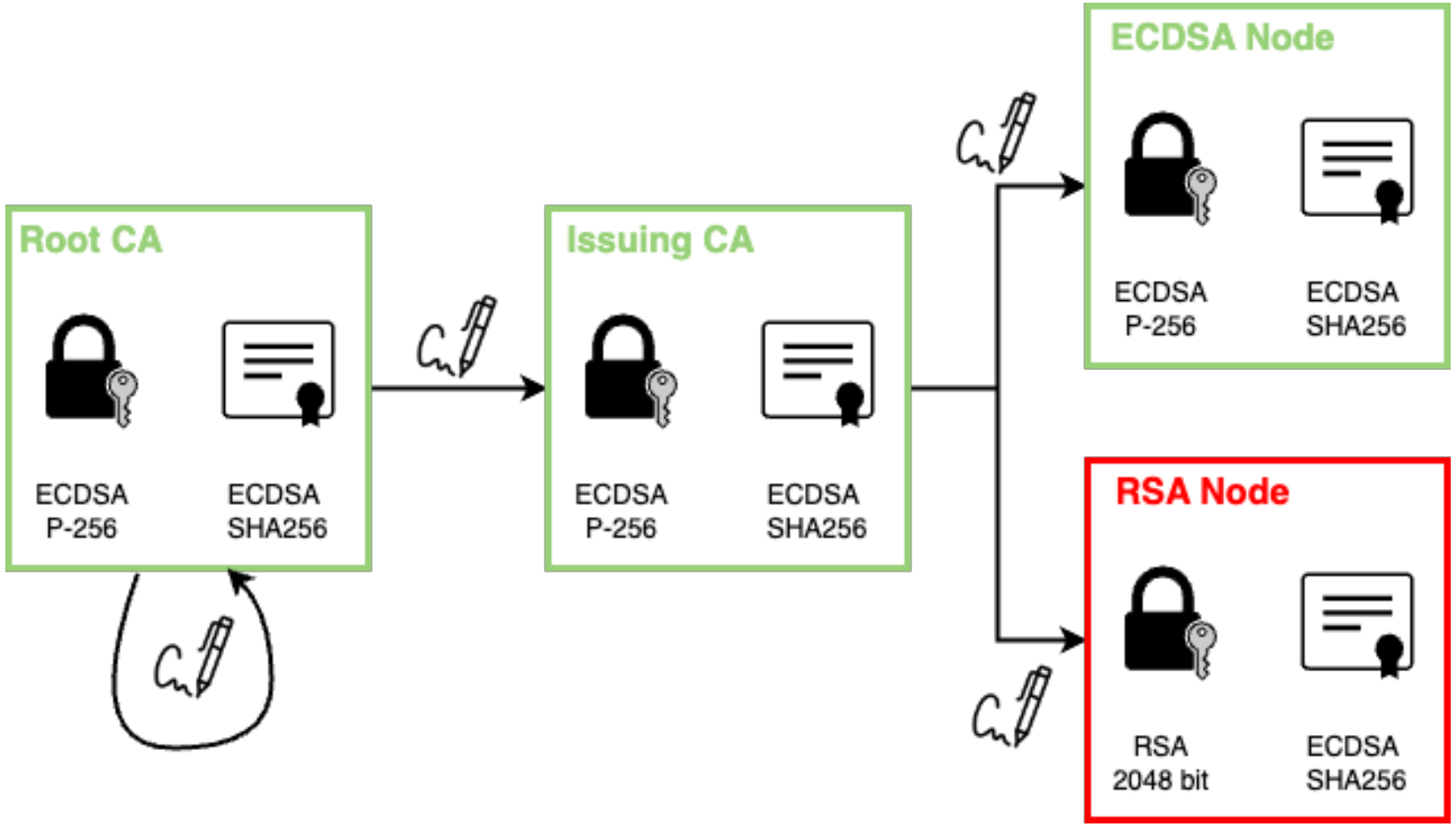
- ☑ End Entities
- ☑ Certificate specification requirements
- ☑ Supported Key types e.g. RSA, ECDSA
- ☑ Amount of Certificates
- ☑ Migration Roadmad list

3. ECC Support

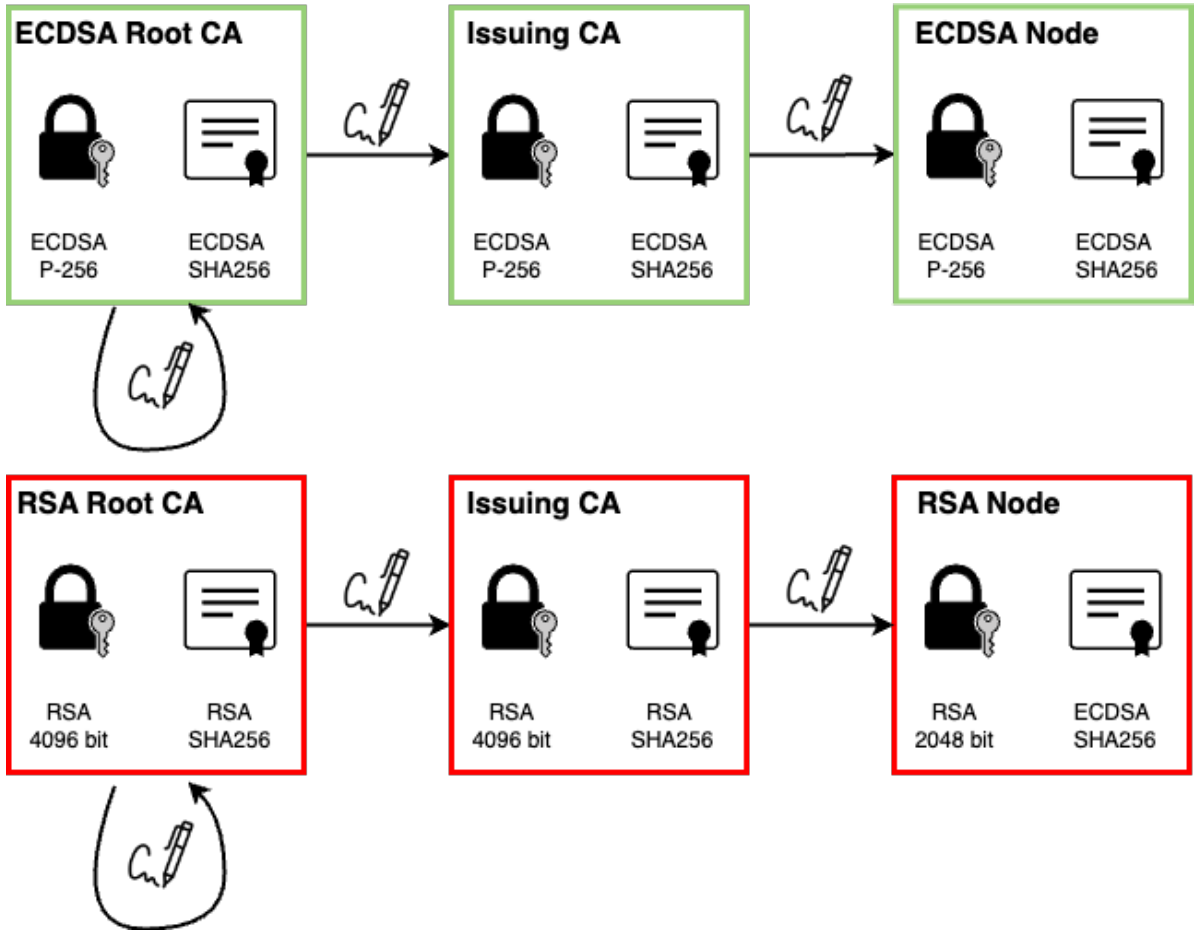
Testing applications & supporting certificate consumers on implementation

- ✓ Test ECDSA with all End entities
- ✓ Writing guidances
- ✓ Signing vs. TLS ciphersuite

3.1 Signing vs. TLS Ciphersuites



Interim PKI?


ECDSA Root CA
ECDSA
P-256
ECDSA
SHA256
Issuing CA
ECDSA
P-256
ECDSA
SHA256
ECDSA Node
ECDSA
P-256
ECDSA
SHA256
RSA Root CA
RSA
4096 bit
RSA
SHA256
Issuing CA
RSA
4096 bit
RSA
SHA256
RSA Node
RSA
2048 bit
ECDSA
SHA256

4. Interim PKI (optional)

Creating another interim RSA PKI for end entities which are not supporting ECDSA.

- To much overhead & Maintaining 2 PKI
- Confusing the consumers
- Building trust between Root CA's

4. Rollout

Production Operation & Maintenance

- [x] Enroll Certificates
- [x] Maintain & Operate
- [x] Reporting

Lessons Learned

- Many places for improvements for crypto agility
- Automation is key
- Collaborative work
- Documentation is key!

22

Part 2: Automation

5G PKI & Enterprise PKI

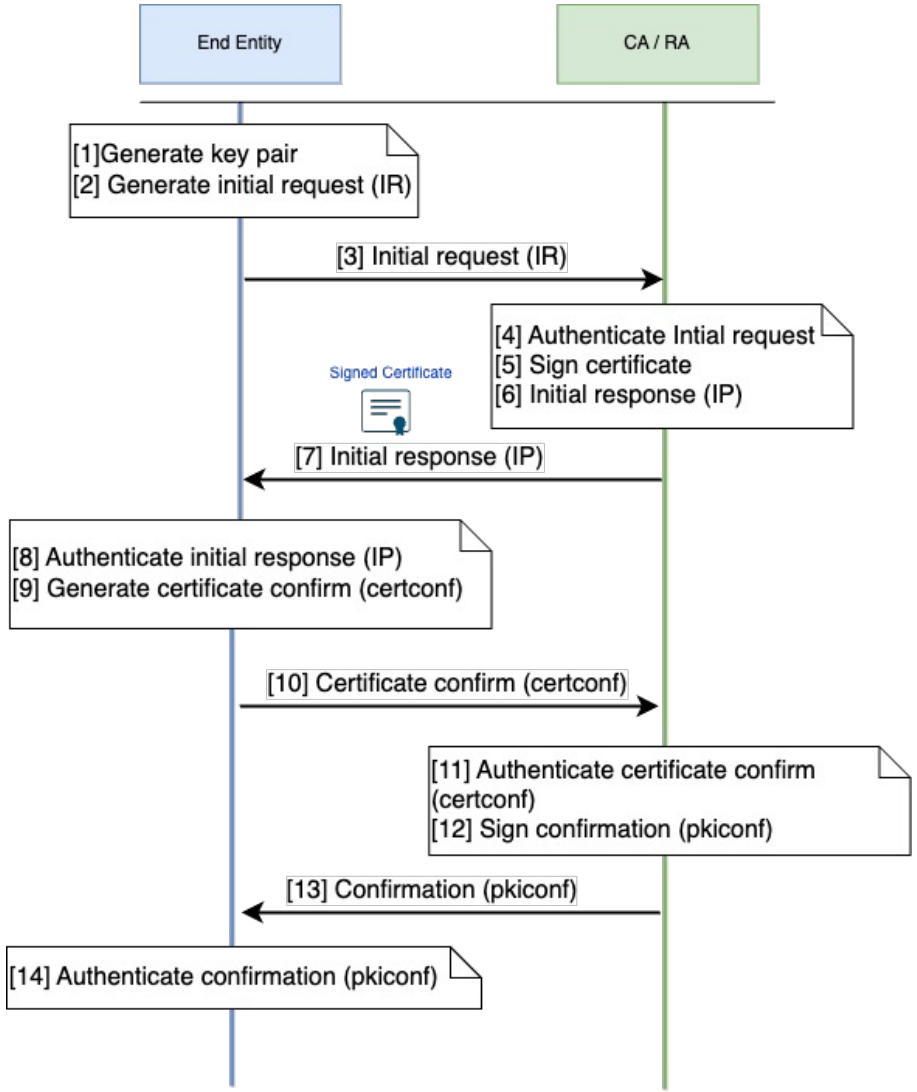
Challenges & Solutions

PKI Protocols (CMPv2)

Automating enrollments with PKI Protocols

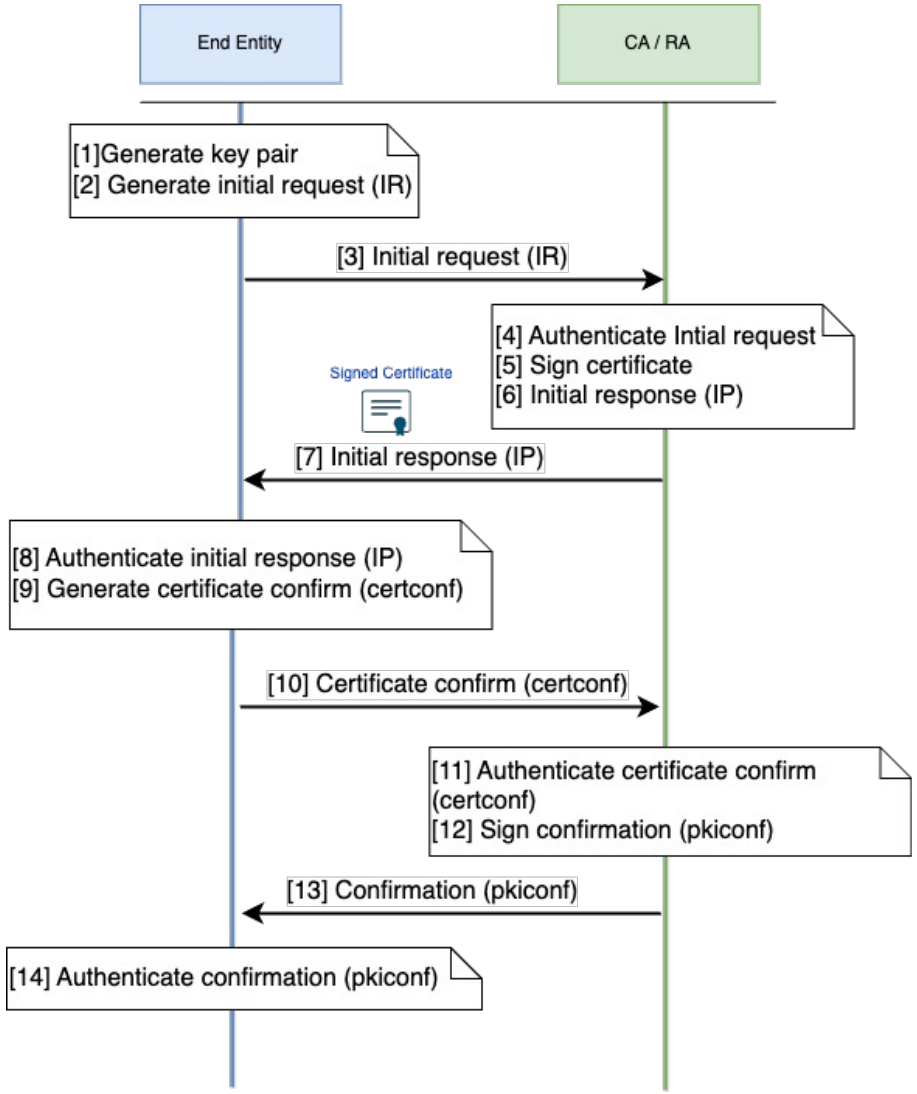
CMPv2 Protocol – Vendor Mode

1. Pre-registration of each Basestation



CMPv2 Protocol - Client Mode

1. Containerized Network Functions (NF) as CU or DU



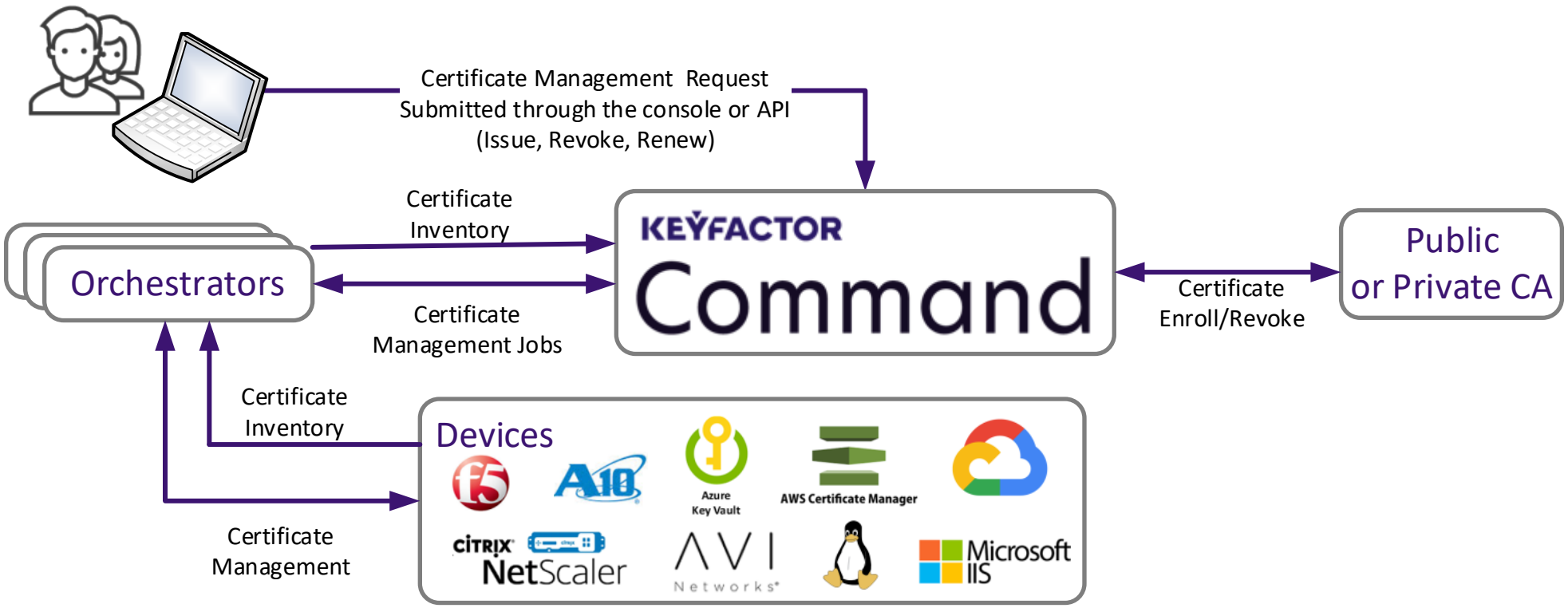
Automation

Automating enrollments, re-enrollment, keystores and truststores with Keyfactor Orchestrator

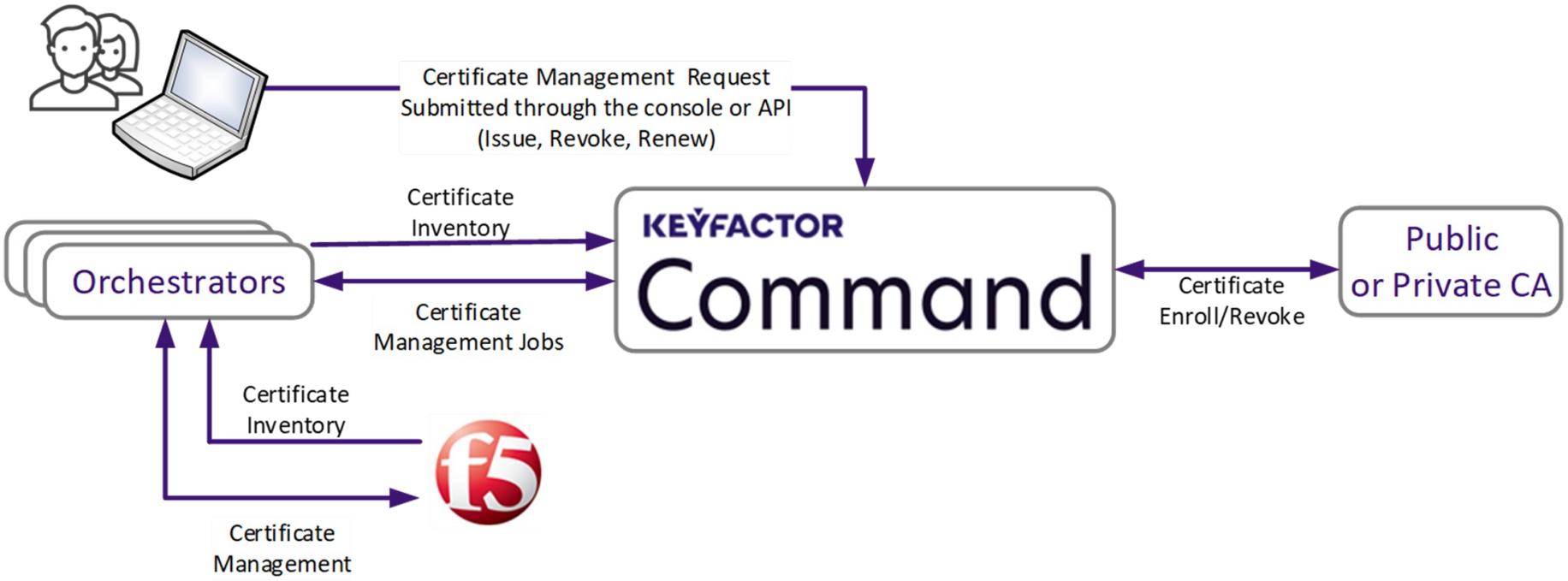
Problem

- Automating enrollments with Protocols
- Automating
  - enrollments,
  - re-enrollements,
  - keystores,
  - truststores

Keyfactor Orchestration



Keyfactor + F5 Big IP



Thanks!

Ibrahim Akkulak

Senior Security Consultant

Rakuten Symphony

Ellen Boehm

SVP IoT Strategy & Operations

Keyfactor