Same Convenience as Let’s Encrypt but Enhanced Level of Trust

Automated Retrieval of Certificates in a Bank Datacenter

Bernd Strößenreuther / ING Germany

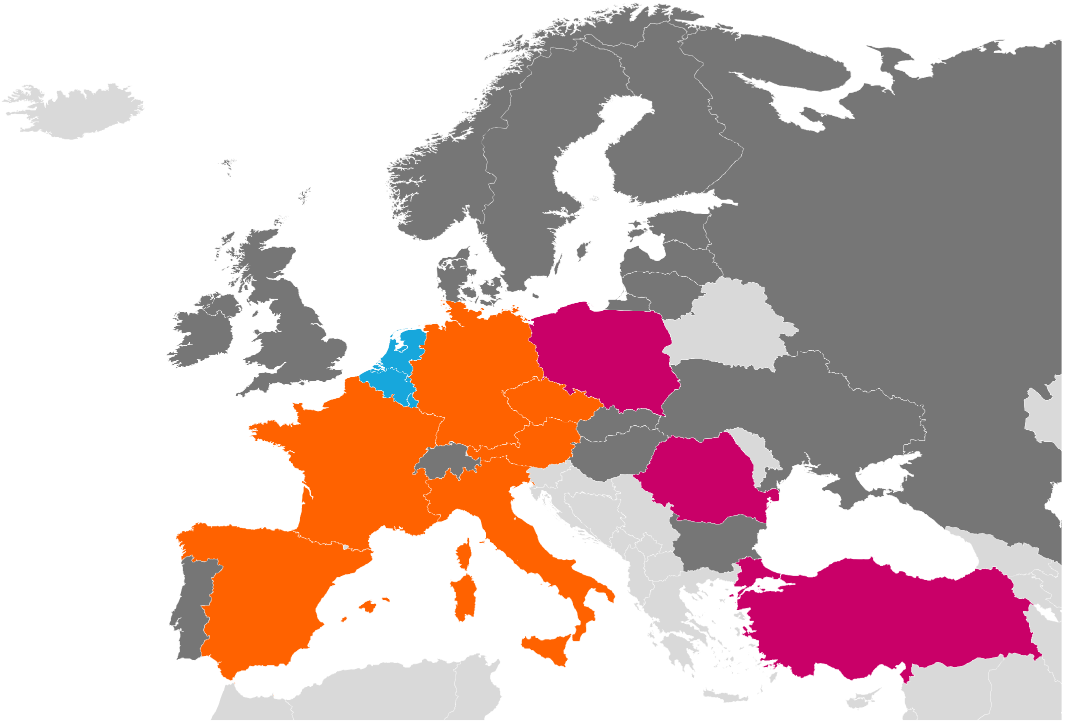
Frankfurt, 2019-09-12

thinkforward

ING

ING in Europe and worldwide

ING in Europe



🟦 Market leaders

🟧 Challengers

🟪 Growth Markets

⬛ Wholesale Banking only

ING worldwide

More than 38 million private customers, business and institutional clients

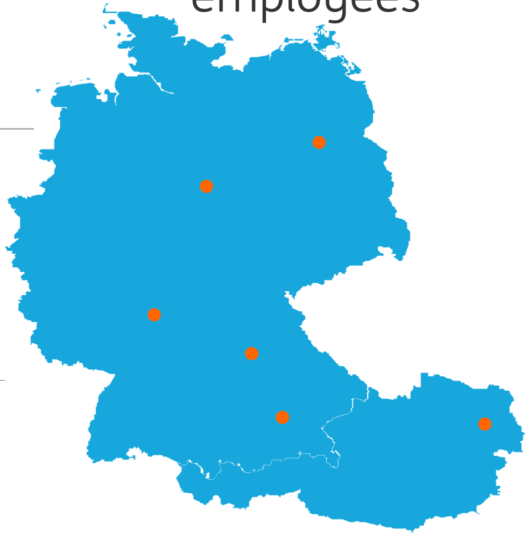
More than 40 countries in Europe, North America, South America, Asia and Australia

More than 51,000 employees

ING Offices in Germany and Austria

Location	Employees
Frankfurt Headquarters	Ca. 2,300
Hanover	Ca. 550
Nuremberg	Ca. 900
Representative office in Berlin	4
Wholesale Banking:	
Frankfurt	Ca. 300
Vienna	19
Essen – First Regional Office	
Vienna	> 250
Munich Headquarters	

Around 4,000 ING employees



1,600 Interhyp employees (incl. regional offices)

About me

Bernd Strößenreuther
Platform Architect
CoE IT

Bernd.Stroessenreuther@ing.de

ING-DiBa AG
Südwestpark 97, 90449 Nürnberg

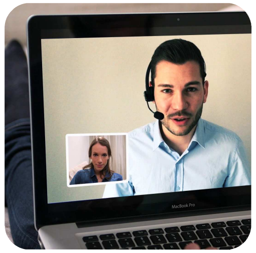
- OpenSource Lover
- contributing
- maintaining
- Linux User Groups
- Linux User since 20+ years

„We want to become the first agile bank in Germany.“

Nick Jue, CEO ING in Germany, Autumn 2017

Digital services for easy and stress-free banking

Video identification



Convenient identification from home

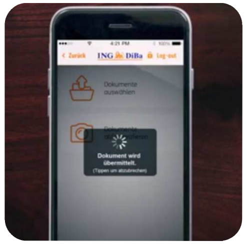
Photo transfer

Capture data from a printed invoice

Fingerprint

Fingerprint instead of TAN

Document upload



Photograph and send documents to ING

Account switching service

Payment partners automatically get informed about new account details

Mobile credit check

Mobile check for credit requests

Banking to go App

Check balance and recent transactions on mobile devices

Certificate Automation

Initial need: Java Platforms Team

- Java Platforms Team provides a platform around JBoss or Tomcat
- Central Ops Team for 100+ different Java Applications (24x7 call-on-duty)
- Stages DEV / TST / ACC / PRD
- Centrally managed (Puppet)
- In total: 3.000+ VMs

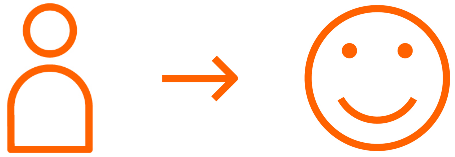
Encryption is good for you!

Encrypting network communication reduces the attack surface.

→ Engineers love encryption!

Java Platforms Team Used Wildcard Certificates

- Manual certificate handling
- Low number of certificates
- Validity period: 2 years
- Subject:
  C=DE, L=Frankfurt, O=ING-DiBa AG, CN=**srvja*e.corp.int**, emailAddress=…



Engineer → Happy!

Compliance → Considered to be insecure!

Individual Certificates for every instance

- Subject:
  `O=ING, OU=Services, OU=PKI, OU=`**`DEV`**`, OU=`**`G2pSearch`**`,`
  `CN=`**`srvja692e.corp.int`**
- One certificate per instance
- 3000+ VMs managed by Java Platforms Team
- Manual approval by a member of PKI Trusted Bone for every single certificate

→ This will never scale!!

More pain points:

- Adding a new application to CA‘s Web Interface takes a few weeks
  ≠ agil!

This would lead us to

#encryptionHate

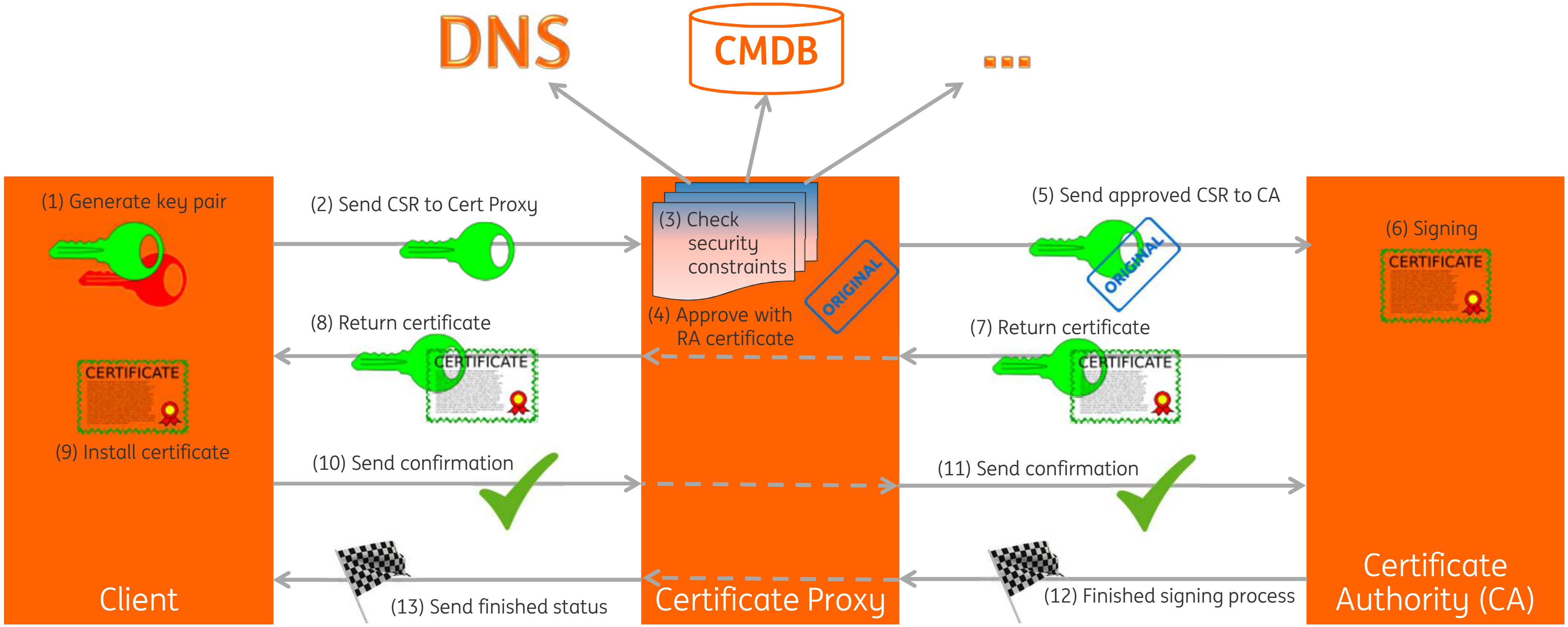
Automation required

We wanted something with the convenience of

Let’s Encrypt

but even stronger verification – stronger than DV (domain validation)

Replace PKI Trusted Bone by a Bot



Technology

CertProxy (Server)

- REST-Interface to Client
- Multiple (configurable) Policies (per Customer)
- Multiple Security Constraints

20 sec until having a valid certificate from ING PKI

CertProxy Client

- Shell-Script
- Cronjob for renewal of certificates

Our Experience

CMDB

- Improvment of data quality in CMDB

Production

- Rolled out tens of thousands of certificates from productive PKI

Time Saving

- Most renewals without human interaction

Additional Benefit

- We can use short certificate livetimes (currently: 90 days)

Spreading

- Meanwhile also used by multiple other teams in Germany and internationally

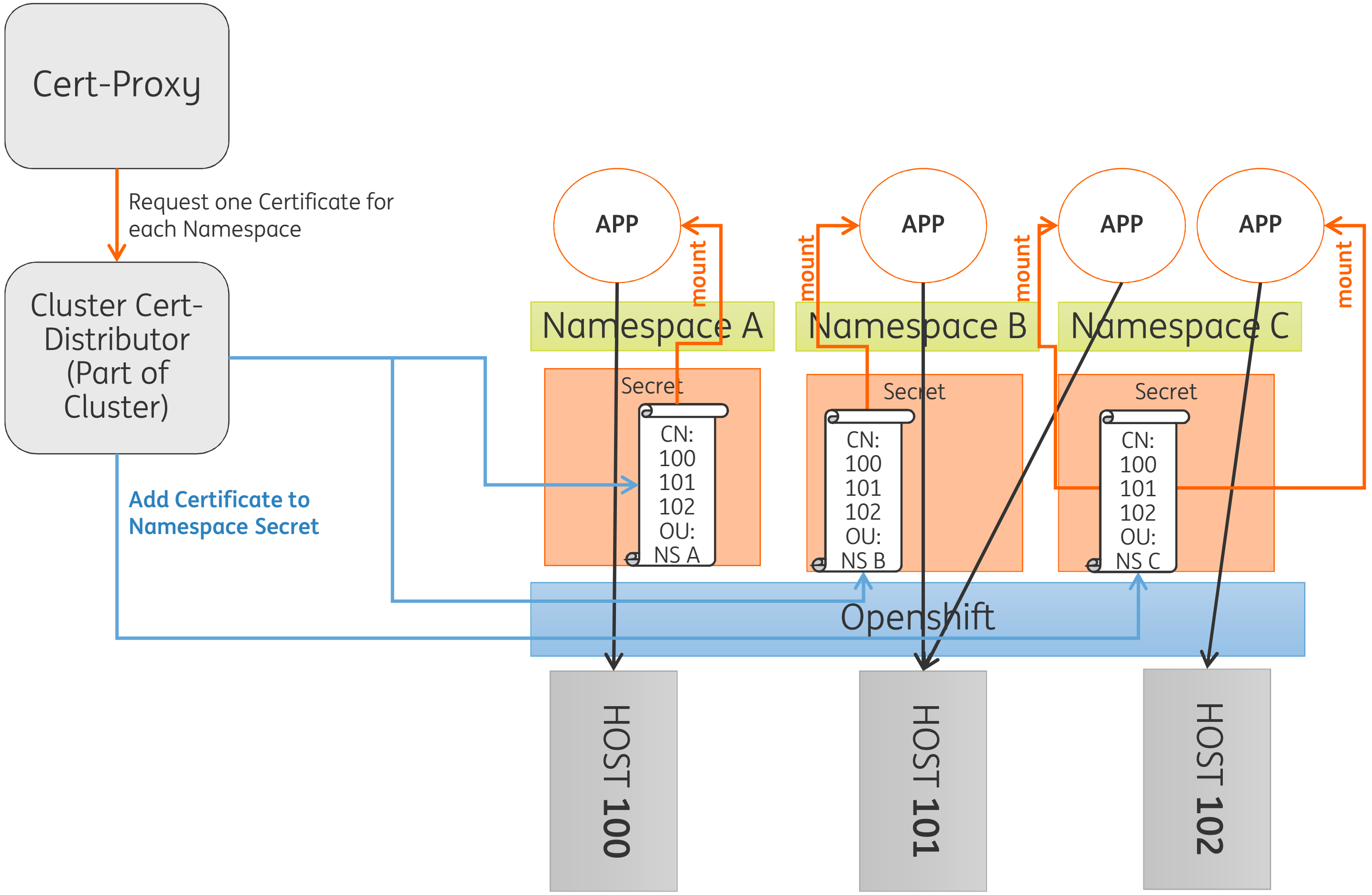
Additional Value

Result

👤 → ☺ 📖 → ☺

#encryptionLove

Work in Progress: OpenShift



Namespace Certificates for outgoing connections

Only the Cert-Distributor requests a Certificate per Namespace. This Certificate has all Hosts in alternative-names and Namespace as OU.

The Cert-Distributor puts the Certificate in the right Namespace.

Certificate is mounted as file in the Container.

Ideas on our Roadmap

Community

- Building a ING-wide community for further development

ACME

- Offering ACME protocol
- Clients can use any ACME client they like
- Checking of all security constraints in the backend
- Could be used e. g. for incoming connections on OpenShift (OpenShift-ACME [1])

Enhanced KPIs

- Put metrics into an Elastic Stack
- Have a nice Kibana dashboard
- Make success mesurable

More Usecases

- Offer Certificates for service specific DNS names (e. g. Loadbalancer Services)
- Therefor: Add more different security constraints

Official CAs

- Add external (official) CA's

[1] OpenShift-ACME: https://github.com/tnozicka/openshift-acme

Thank you!

Bernd Strößenreuther
Platform Architect / CoE IT

ING Deutschland
Südwestpark 97
90449 Nürnberg

bernd.stroessenreuther@ing.de

www.ing.de

Facebook.com/ING.Deutschland

@ING_Deutschland

Instagram.com/ING.Deutschland

YouTube.com/ingdiba

Obligatory last slide

You want to join our **#encryptionLove** experience ?

Get your dream job !

www.ing.de/karriere