X.509:
From #encryptionHate to #encryptionLove

Christian Gebhardt, Bernd Strößenreuther / ING Germany

Rotterdam, 2018-11-22

ING

Who are we?

Christian Gebhardt
Lead Java Platforms
CoE IT

Christian.Gebhardt@ing.de

ING-DiBa AG
Südwestpark 97, 90449 Nürnberg

Bernd Strößenreuther
Platform Architect
CoE IT

Bernd.Stroessenreuther@ing.de

ING-DiBa AG
Südwestpark 97, 90449 Nürnberg

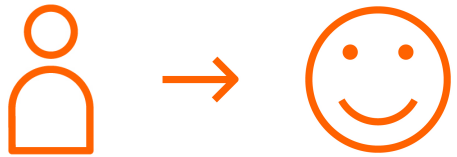
Encryption is good for you!

Encrypting network communication reduces the attack surface.

→ Engineers love encryption!

We 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 our 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 UniCert Web Interface takes a few weeks
  ≠ agil!

This would lead us to

#encryptionHate

ING

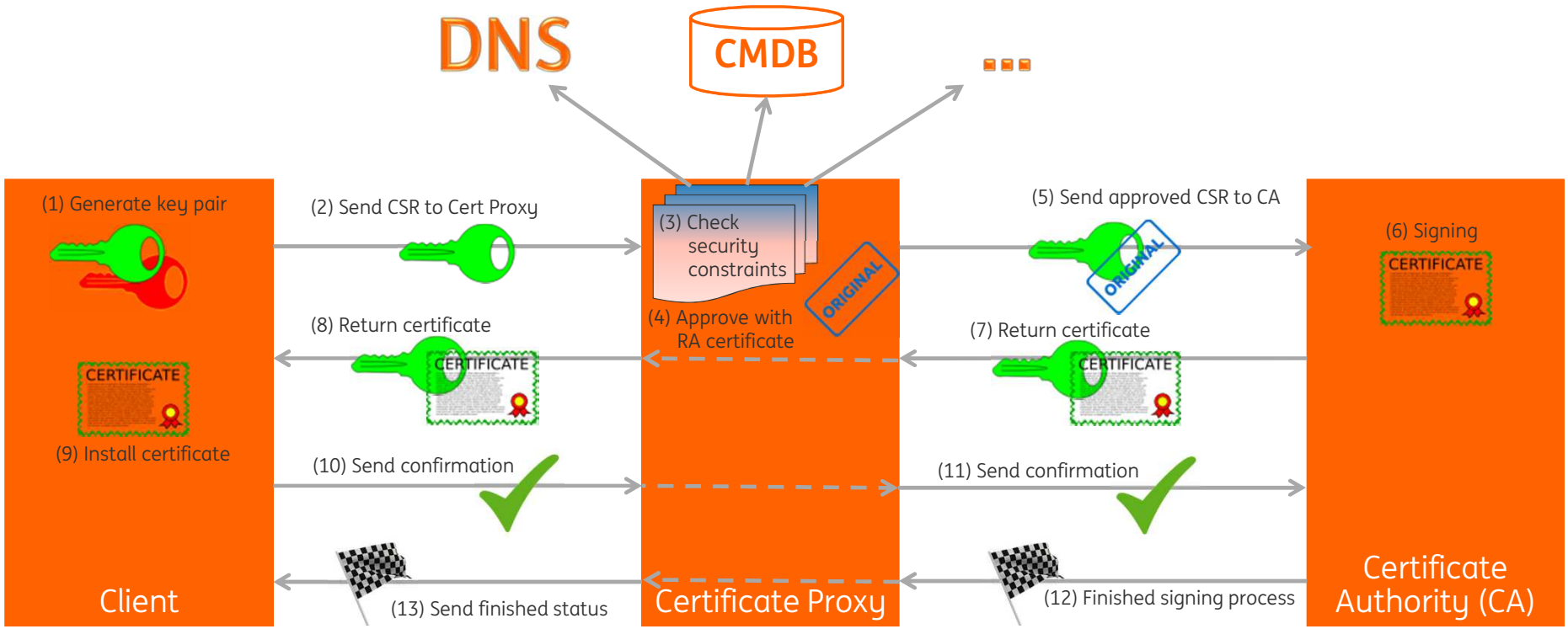
Automation required

We wanted something with the convenience of

but even stronger verification.

ING

Replace PKI Trusted Bone by a Bot



CertProxy: Technology

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

Client:

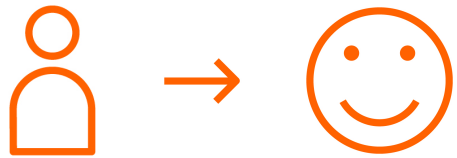
- Shell-Script
- Cronjob for renewal of certificates

20 sec until having a valid certificate from ING PKI

Our Experience

- Improvment of data quality in CMDB
- Rolled out 5000+ certificates from productive PKI
- First renewals have been done without interaction
- Additional benefit: We can use short certificate livetimes
  (currently: 90 days)
- Meanwhile also used by one other team in germany
  and one team in Belgium is testing within our test environment right now.

Result



#encryptionLove

ING

Ideas for our Roadmap

- Make CertProxy an international offering
- Building a community for further development
- Multiple (configurable) certificate policies (replacing profiles)
- Add more different security constraints
- Add external (official) CA‘s

If you want to join our

#encryptionLove

experience, please do not hesitate to contact us:

Bernd.Stroessenreuther@ing.de
Christian.Gebhardt@ing.de

ING