



Multi-CA and CA Rollover Capability

Planning for truly continuous CA operation

2005-10-18 – Martin Bartosch

What's this all about?

- [Multi-CA support

- support of multiple **different** CA "realms"

- [CA Rollover support

- service **continuity** regardless of CA certificate validity

- prevent need for absurd CA certificate lifetimes

Multi-CA Support

- [Why use multiple CAs?

- different “name spaces” (e. g. customers)

- organizational separation

- different CP/CPS

- [OpenCA currently supports **one single CA** per instance

- [Multiple installations on one system require

- separate web frontends

- separate databases

Multi-CA Support

— [Next release will provide Multi-CA support

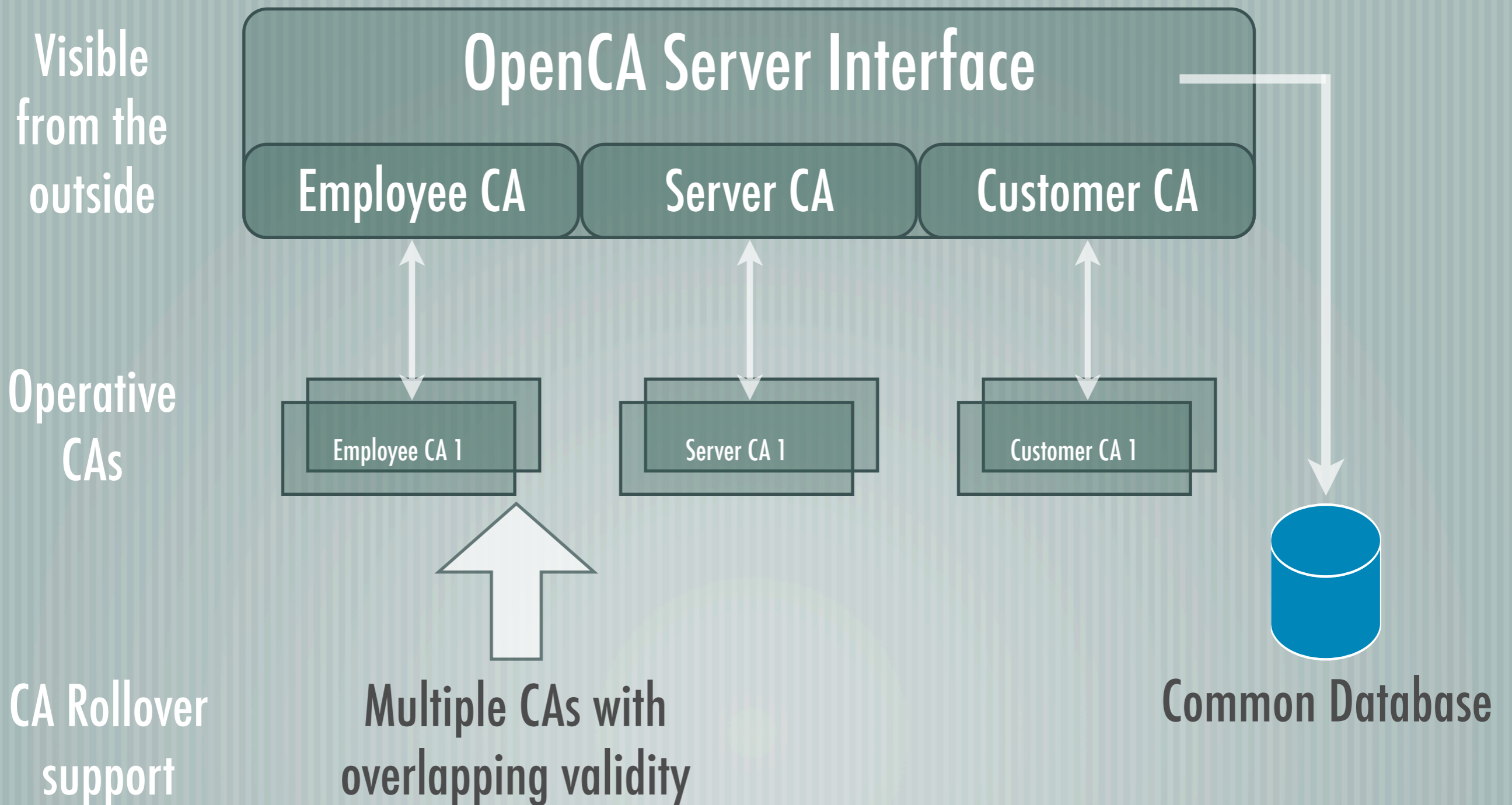
— more than one CA can be configured

— users will be able to choose CA on the login page

— alternative: select the desired CA by URL

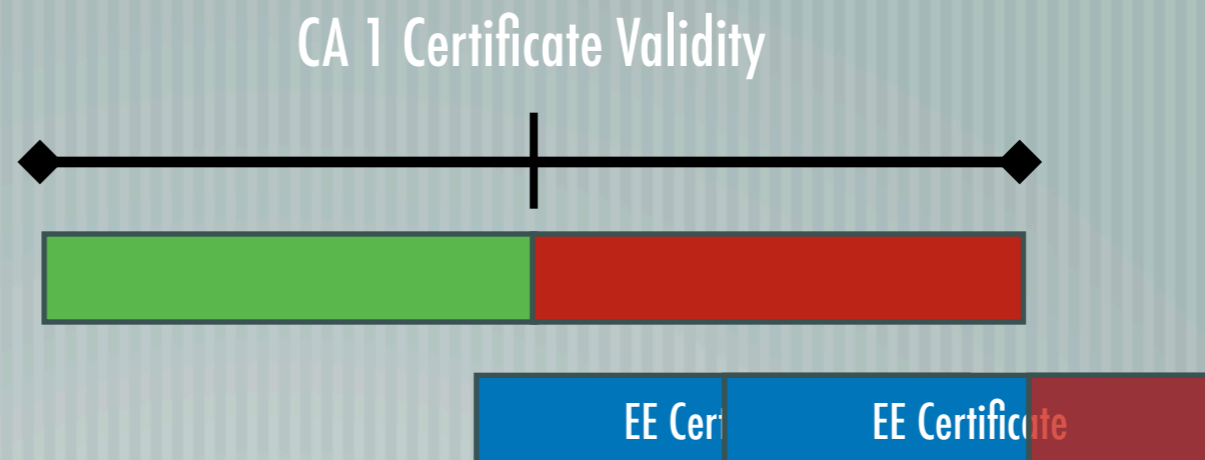
— completely separated name space for certificates, requests, CRLs etc.

Overview



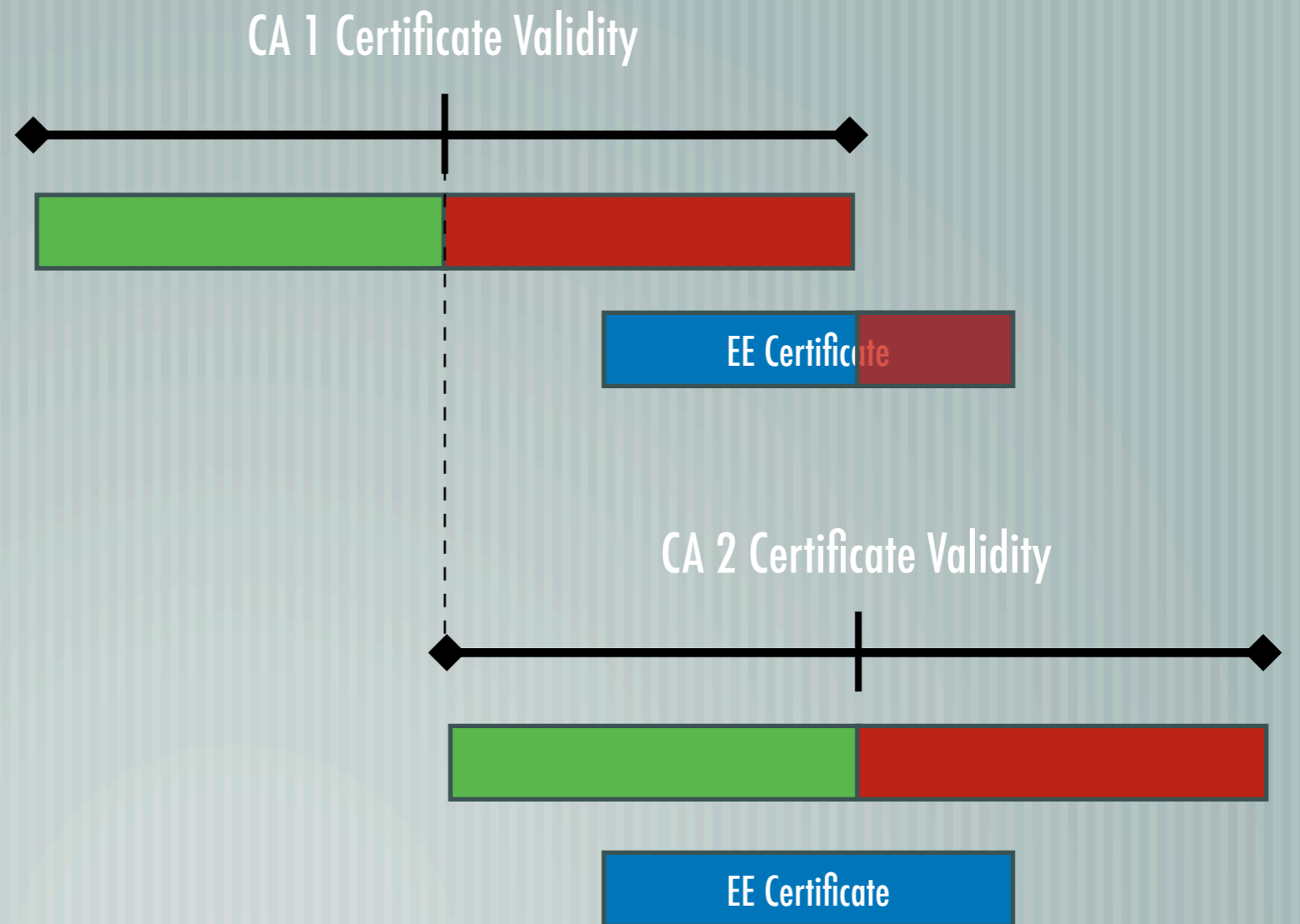
CA Rollover Support

For any CA there is one point after which no new certificate with the full desired lifetime can be issued



CA Rollover Support

Provide a CA certificate with overlapping validity that takes over after this point



CA Rollover Support

- [One externally visible CA may consist of one or more internal operative CAs
- [User requests to a CA are automatically dispatched to the responsible operative CA
- [Decision based on CA certificate validity

CA Rollover Support

- [Rollover handling for CA operations

- Certificate issuance

- Certificate renewal

- Certificate revocation

- CRL issuance

Dispatching Certificate Issuance

- [Determine valid operative CA candidates

- CA enabled in configuration

- CA is valid now

- requested certificate fully fits into CA lifetime

- [From remaining CAs pick the one with highest NotBefore date

- [Process certificate request in this CA

Dispatching Certificate Renewal

— [Identify original certificate to renew

— Reject request if not found or two valid certificates already exist

— [Determine certificate validity for renewed certificate

— [Dispatch Certificate Request to issuing CA (may roll over)

Dispatching Certificate Revocation

- [Determine CA that issued the certificate in the first place
- [Revoke certificate in this CA

Dispatching CRL Issuance

— [Determine valid operative CA candidates

— CA enabled in configuration

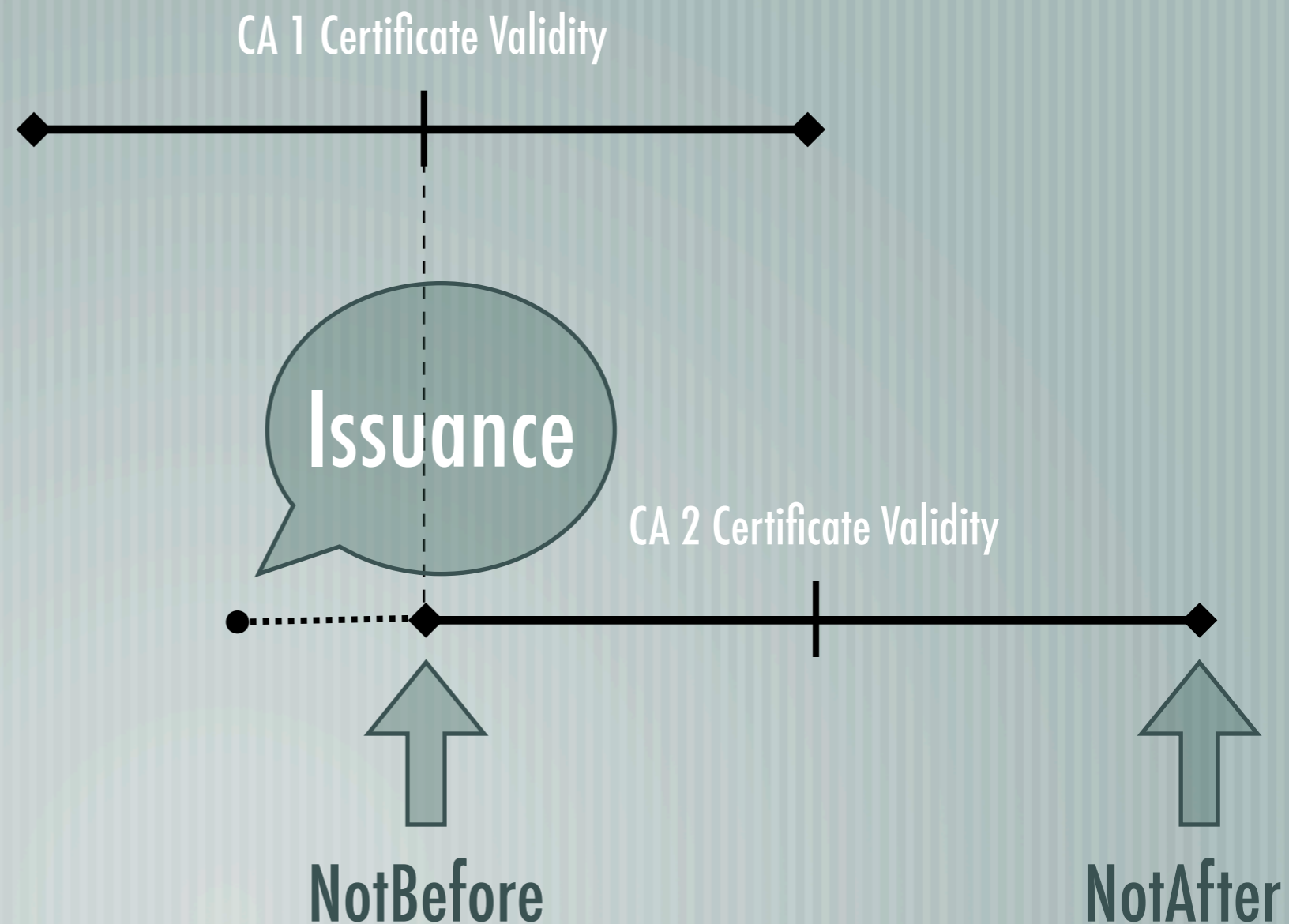
— CA is valid now

— [Create CRLs for **all** identified CAs

Operational Issues: Administration

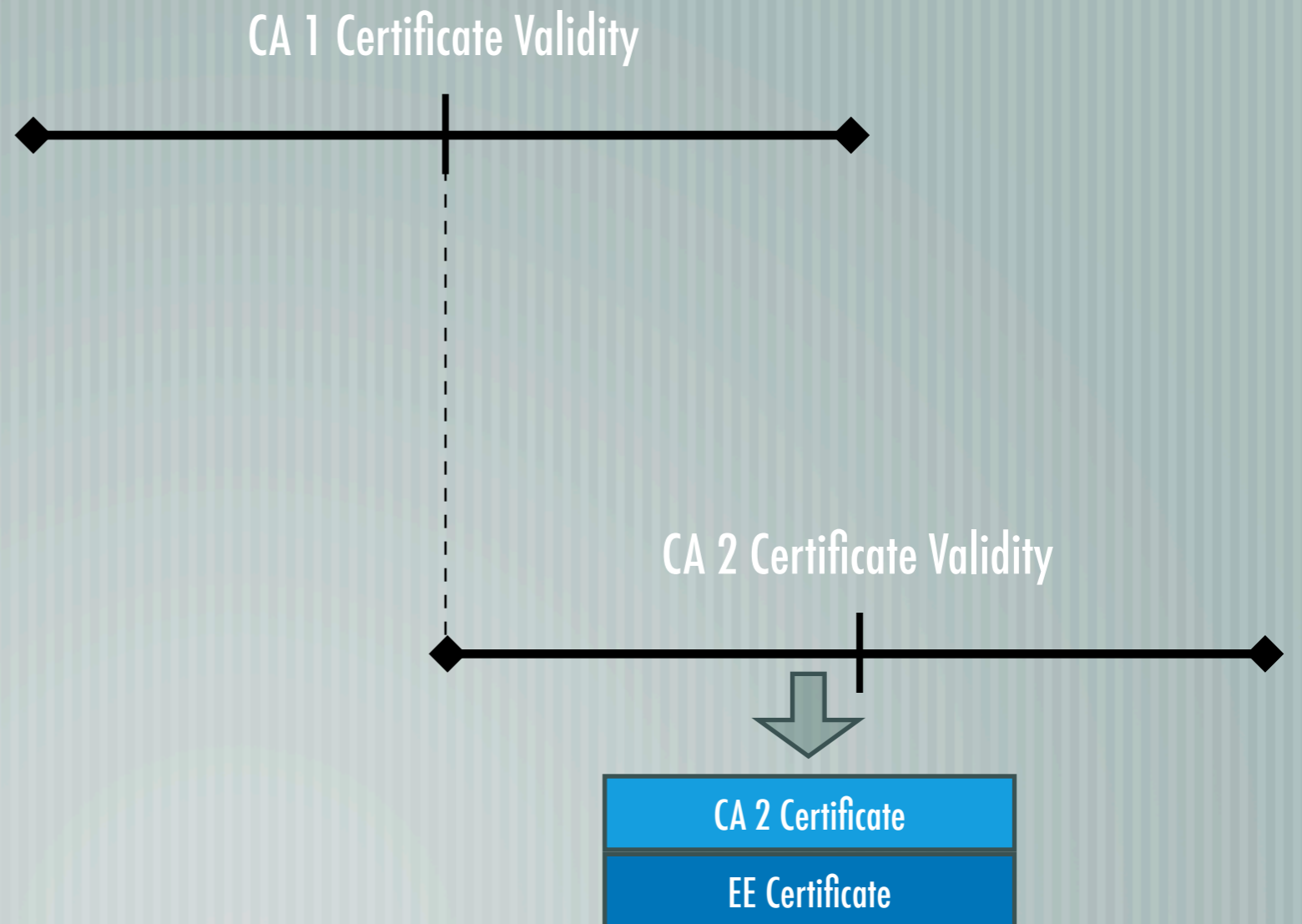
Issuing CA certificates **can** be created in advance

No real technical or operational need for this



Operational Issues: Distribution

CA certificate distribution happens implicitly for **subordinate** CAs

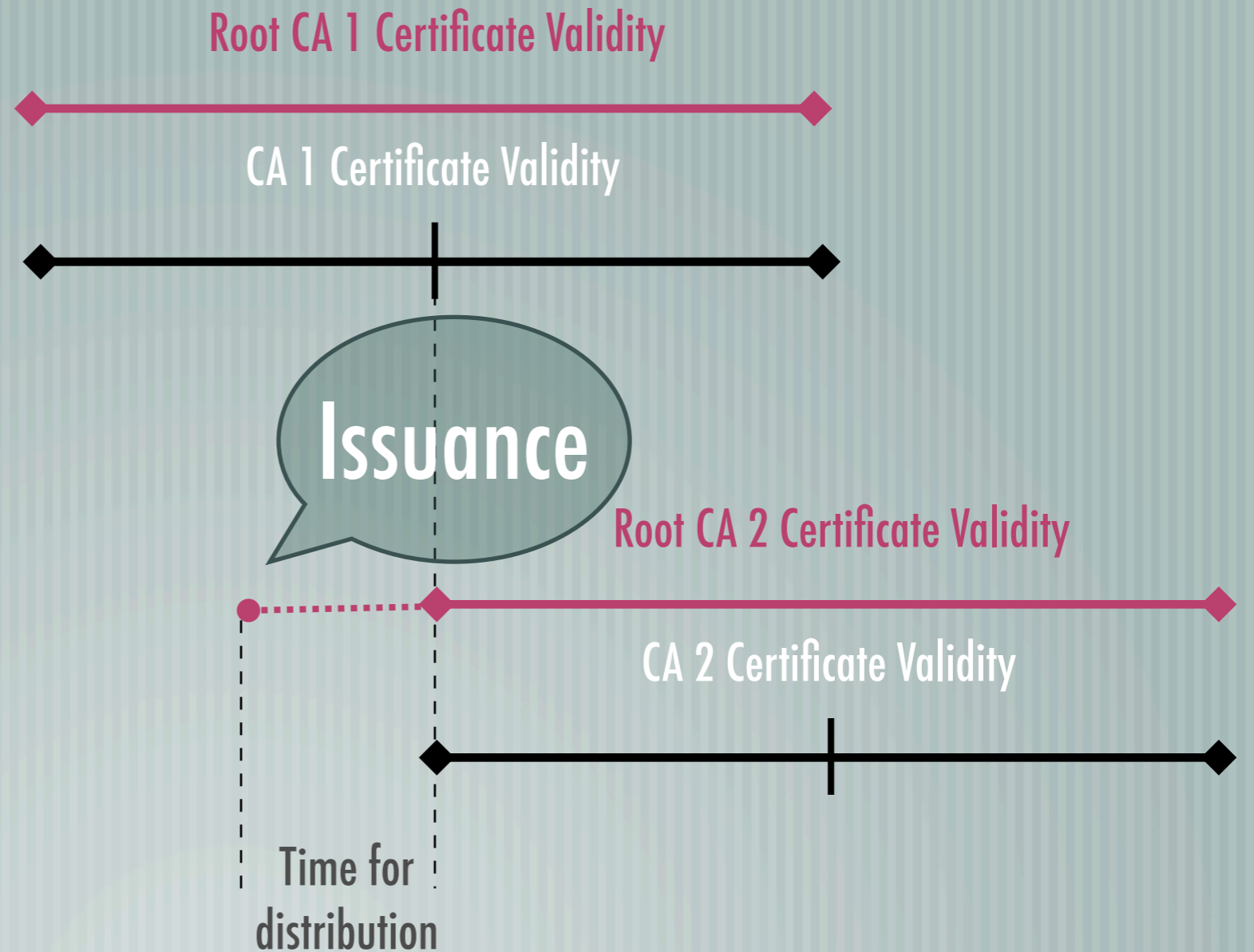


Operational Issues: Root Certificate Distribution is critical

Must be carefully planned and prepared

Root Certificates **must** be created in advance

Provide ample time for distribution



Operational Issues: Root Certificate Distribution - Security Considerations

— [Root Certificate distribution should ideally happen manually

— [Automated processes are possibly a security problem

— Rogue certificates might be injected

Operational Issues: Root Certificate Distribution

— [Ideas for automatic Root Certificate deployment

- Let clients poll Root Certs from directory/web server
- Once a new Root Cert is found, copy it into quarantine area
- Accept Root Cert if the same certificate is still present after e. g. 10 days
- Requires security monitoring of directory/web server

Thanks for your
attention!

Martin Bartosch



Cynops GmbH

info@cynops.de

Kirchgasse 10c

61449 Steinbach (Taunus)

T (+49) 0 61 71.6 98 18 03

F (+49) 0 61 71.6 98 18 09

<http://www.cynops.de/>