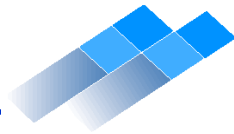


Hierarchy and organisational Structures as understood by

Oliver Welter - welter@tum.de

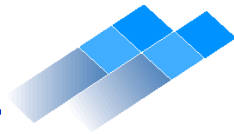


Root of Trust / Hierarchy

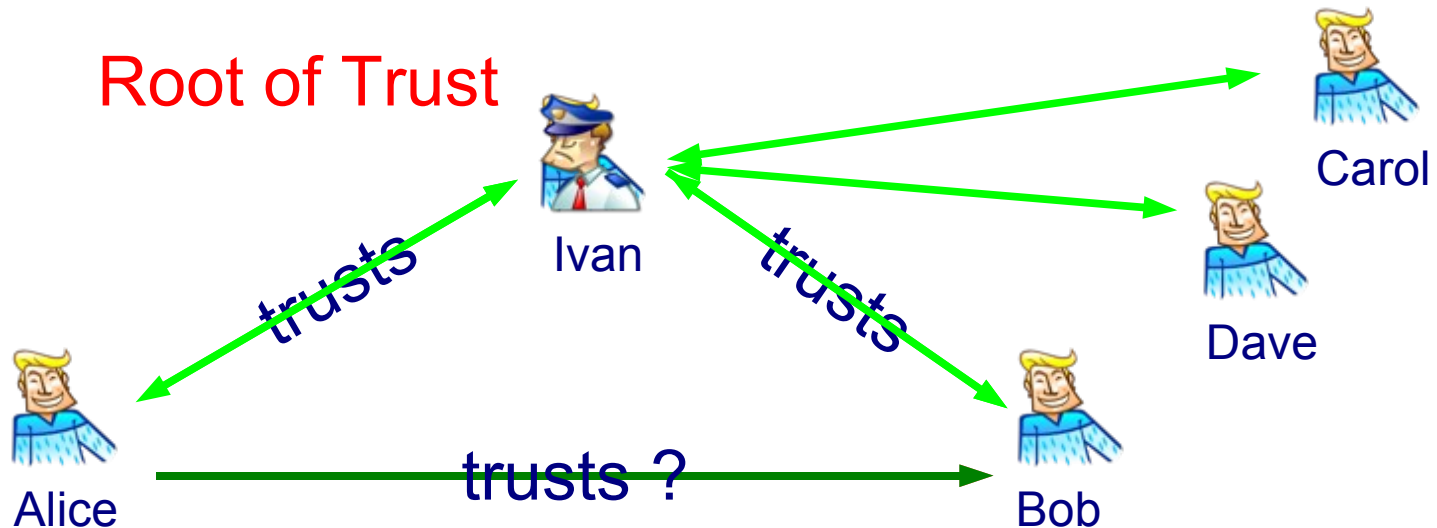
Certificate Issuance Workflow in OpenCA

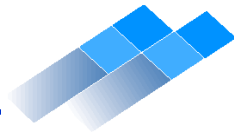
actual Implementation

Outlook

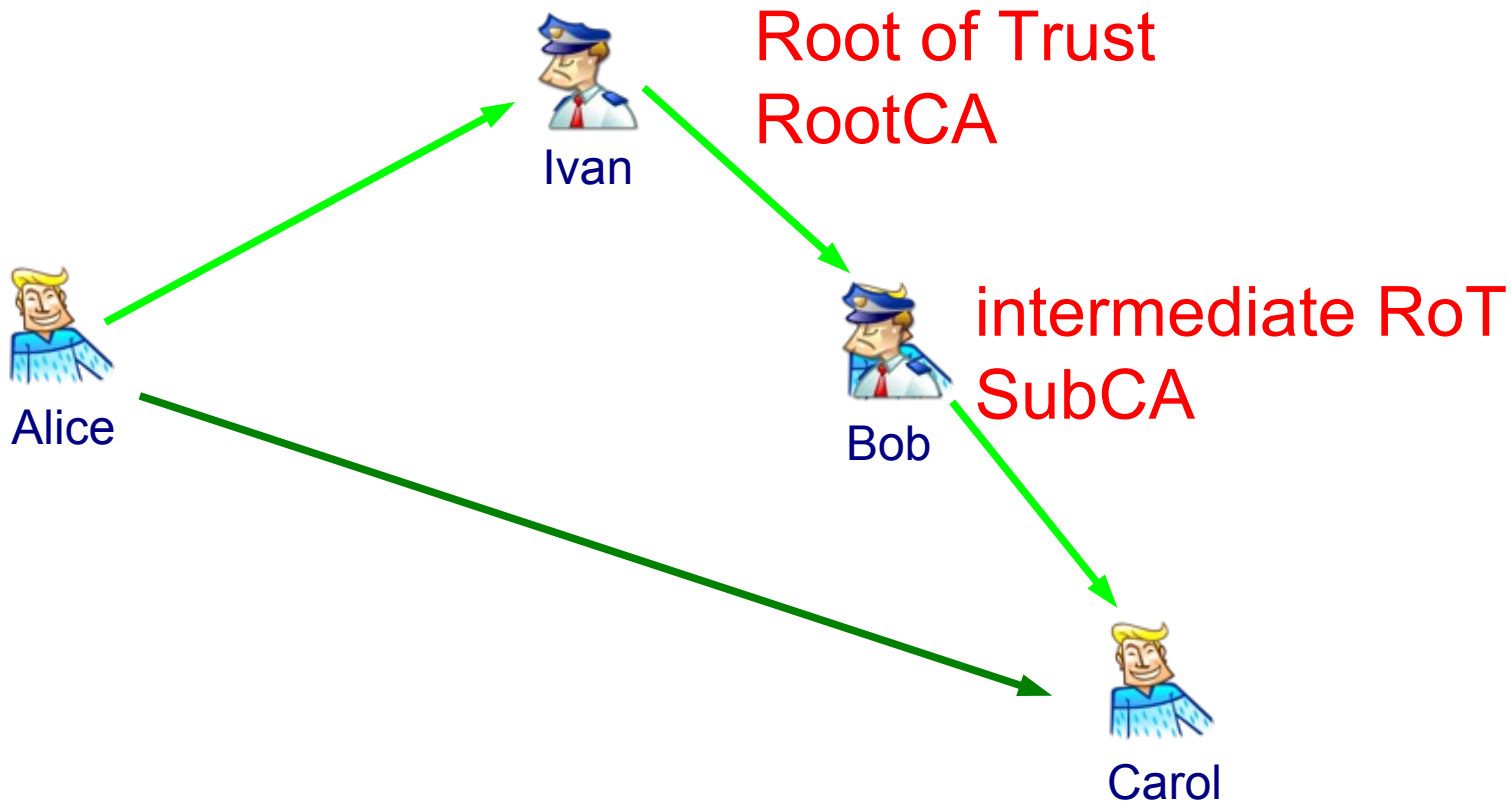


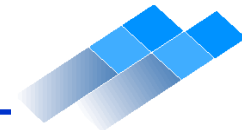
- ★ Trust: assume that an entity behaves like expected
- ★ transitive Trust-Relation:



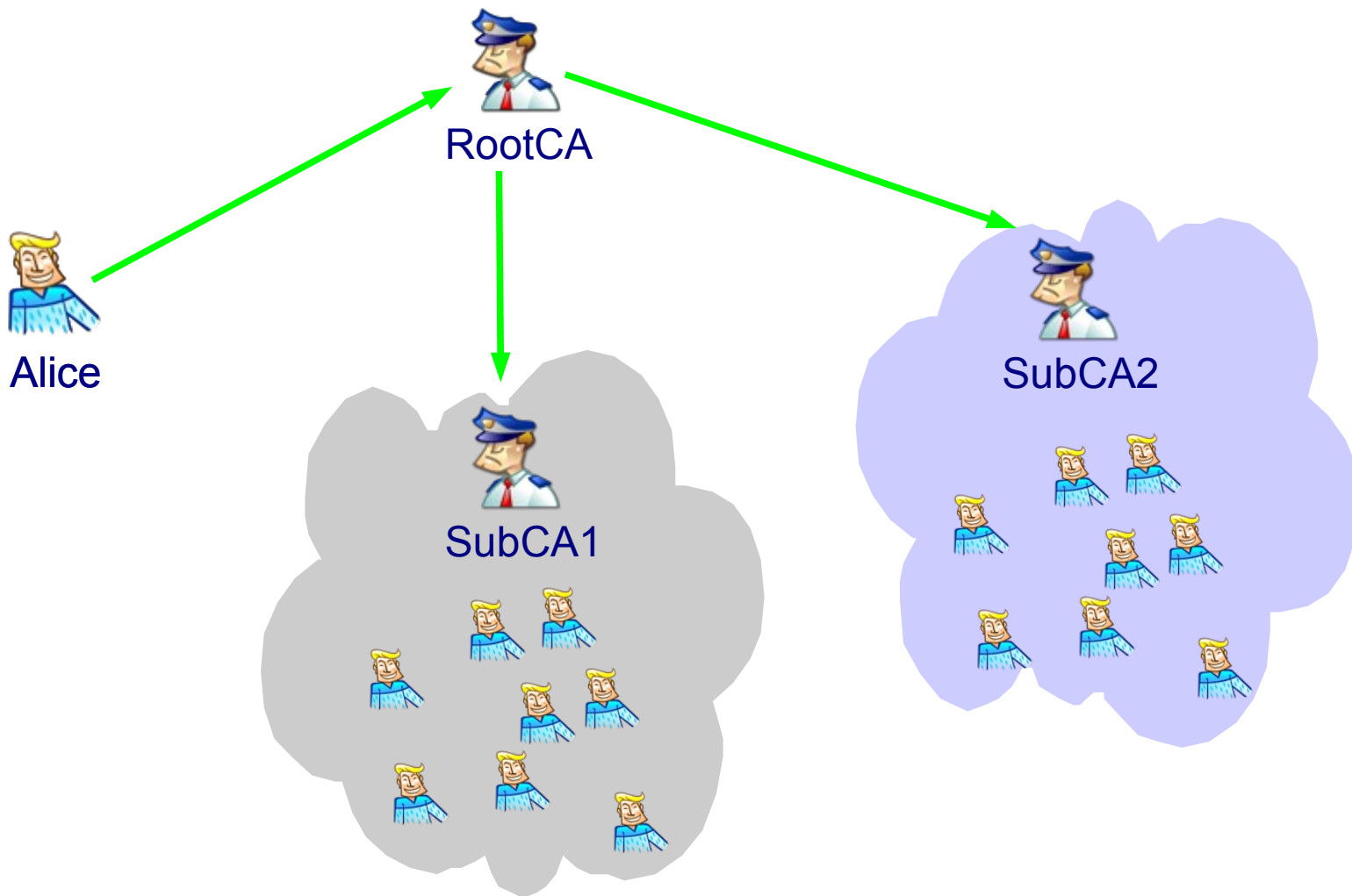


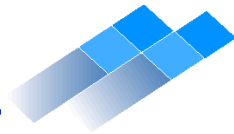
★ Chain of Trust





★ Chain of Trust



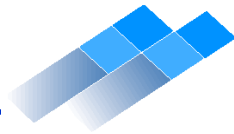


Root of Trust / Hierarchy

Certificate Issuance Workflow in OpenCA

actual Implementation

Outlook



- ★ user creates his keypair
- ★ public key e + identity = certificate request (CSR)
- ★ „Registration Authority“ checks identity
- ★ „Registration Authority“ approves CSR
 - ★ an operator signs the request
- ★ „Certification Authority“ creates certificate from CSR
- ★ certificate is published



request



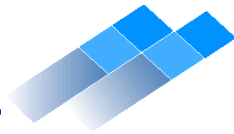
identification



certification



publishing



Request



Identification



Certification



Publishing

User

creates

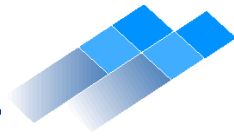
wird
benachrichtigt

Registration
Officer

identified ?
authorized ?
=> approve
request !

Certification
Operator

create
certificate

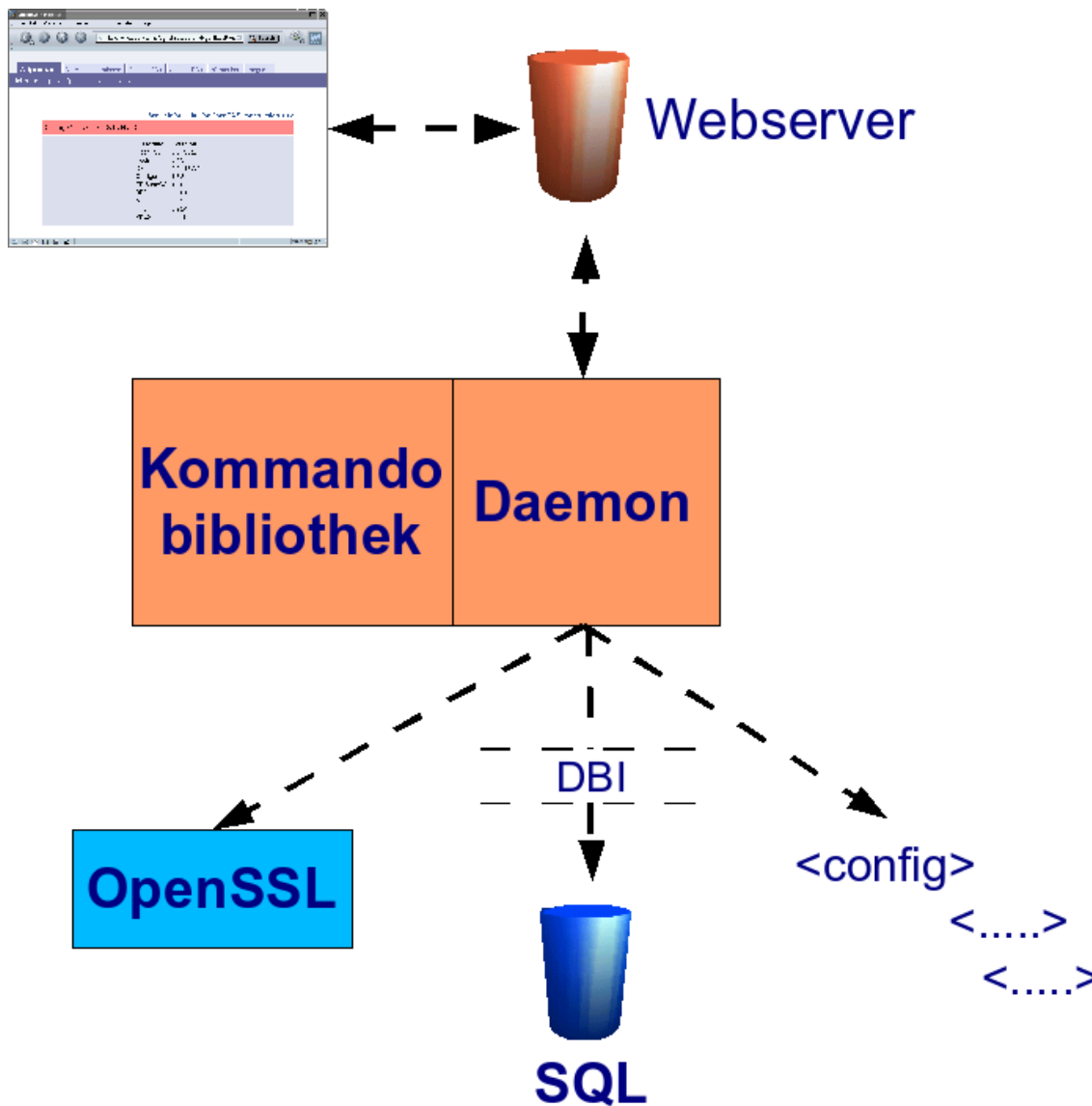
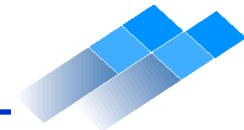


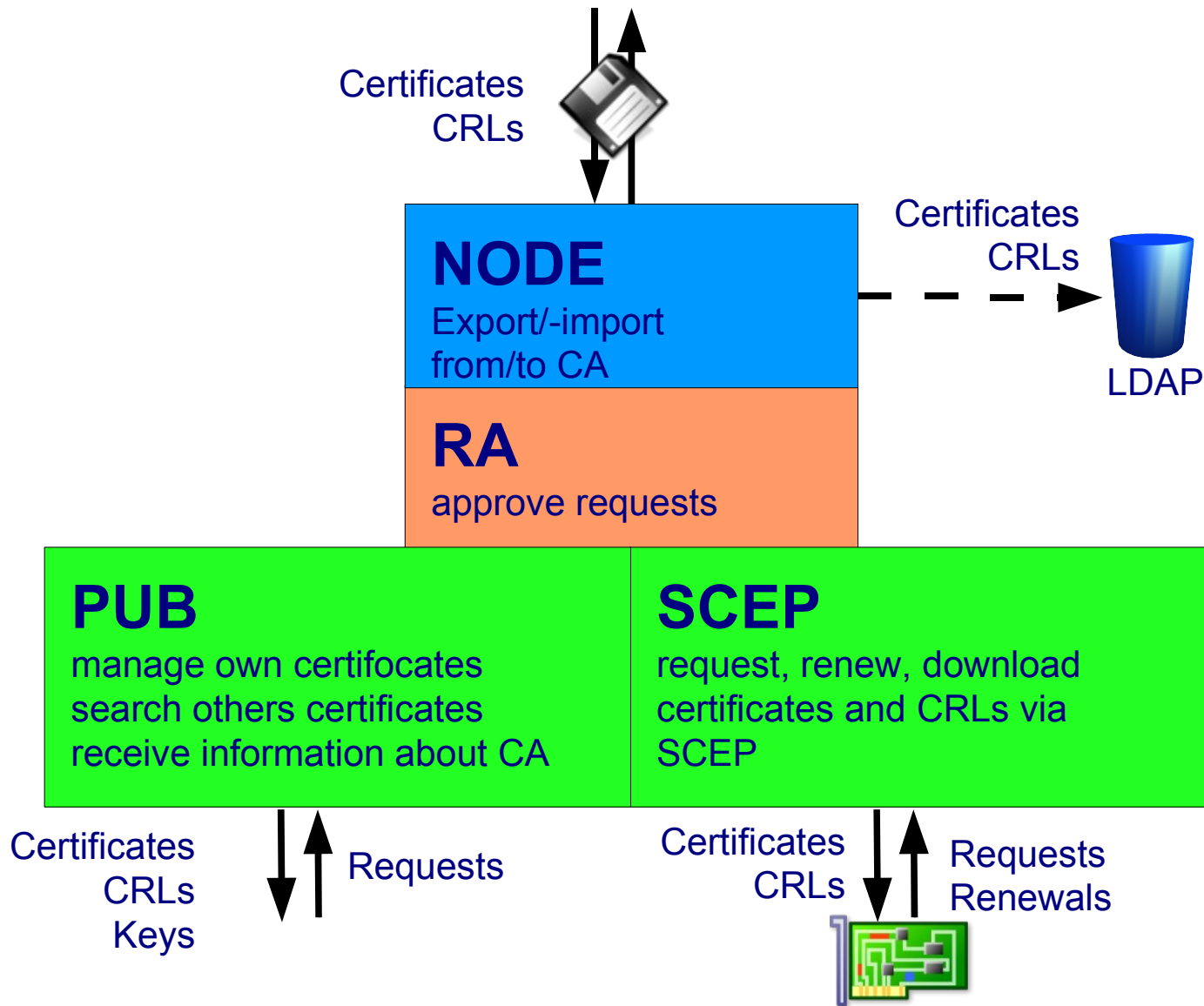
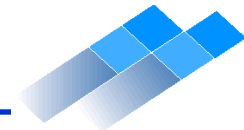
Root of Trust / Hierarchy

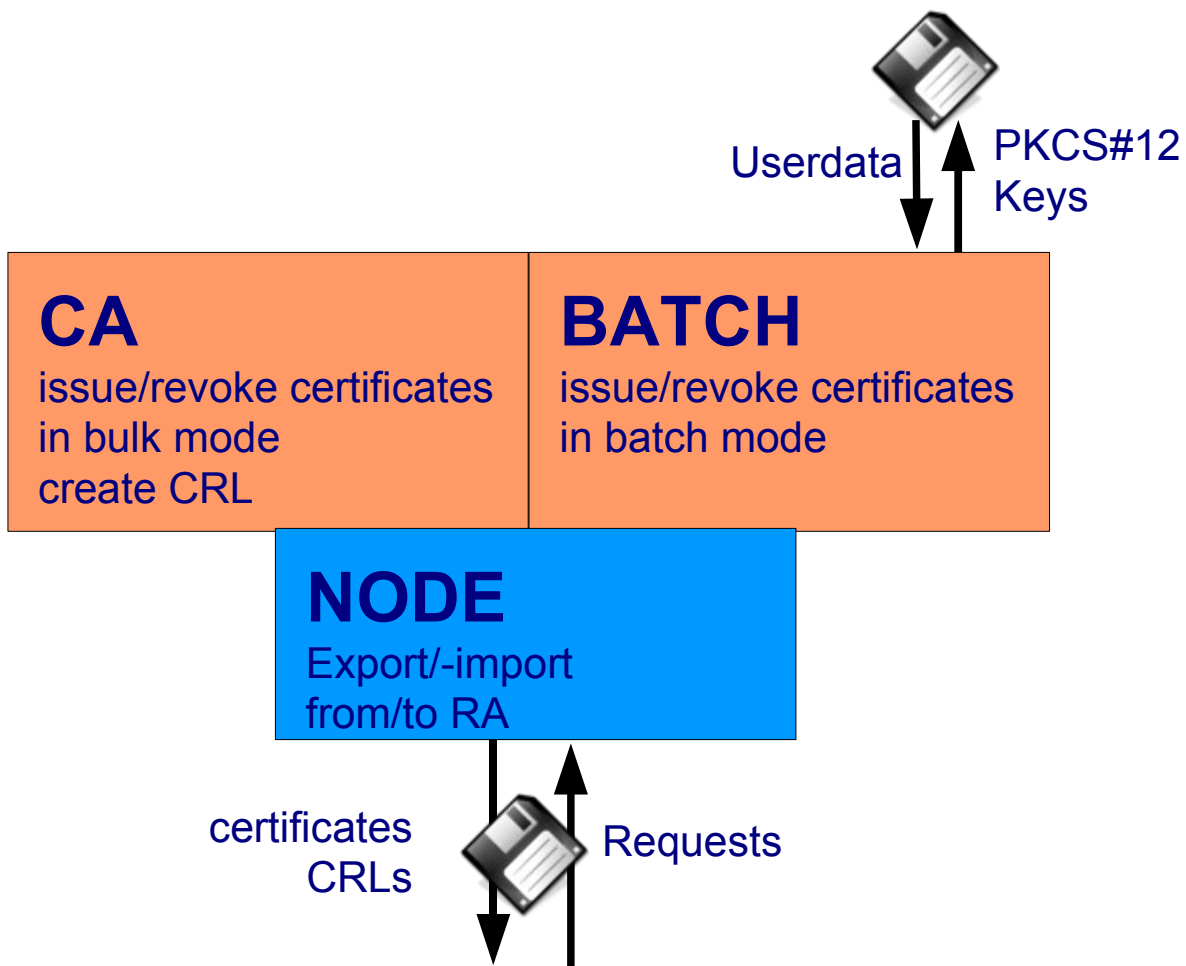
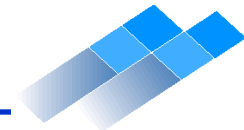
Certificate Issuance Workflow in OpenCA

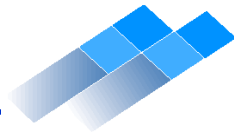
actual Implementation

Outlook







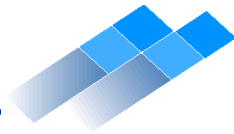


Root of Trust / Hierarchy

Certificate Issuance Workflow in OpenCA

actual Implementation

Outlook



- ★ Interface-Logic
 - ★ logical groups of commands
 - ★ separate menu-structure
 - ★ separate access control

- ★ Integration
 - ★ Batch/SCEP allow integration with many third party systems
 - ★ starting with upcoming release:
powerful shell interface to all components

protect the environment !

