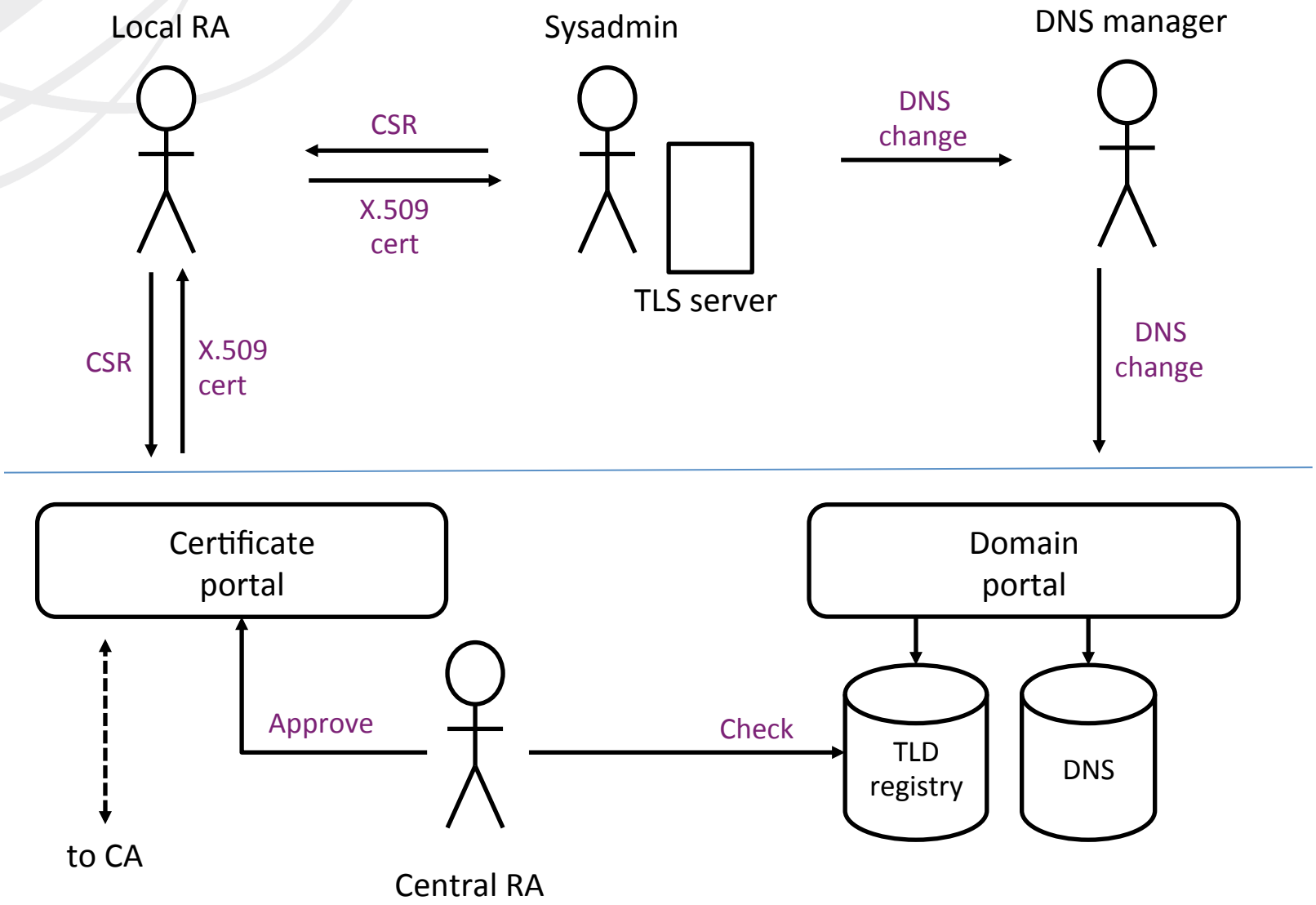
DANE Pilot: integrating certificate and domain services

Joost van Dijk, Roland van Rijswijk
SURFnet

Roles and Services



Certificate Workflow

- Sysadmin generates key pair
- Local RA approves CSR
- Local RA sends in the CSR, downloads X.509 certificate from the portal, distribute to sysadmins
- DANE: Notify Domain portal to generate TLSA record

DEMO

DANE pilot

Problems with DANE

- DANE complicates an already hard problem
  - Certificates for TLS is difficult
    - workflow / roles at the institution
  - (DNS management is difficult too)
- DANE adds problems:
  - Synchronization of cert during key rollover
  - Certificate is bound to specific port number

More problems

- What about expired certificate?
  - Compliant clients will check “valid to”
  - Certificate portal notifies Local RA (prior to expiry)
- What about compromised certificate?
  - Revoke certificate (CRL, OCSP)
  - Certificate portal notifies Local RA (immediately)
- With DANE:
  - On notification, change cert, but DNS takes time to propagate
  - Expired certificates can be auto-removed
  - Revoked certificates will have to be removed