Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

KIS - Ekspertseminar om BankID

Dr. Ing. Åsmund Skomedal

Forsknings sjef, DART, Norsk Regnesentral

asmund.skomedal@nr.no

18. mars 2009

Tema til diskusjon

Agenda punkter

- Kritisk analyse av digitale signaturer i BankID og graden av ikke-benekting ("non-repudiation")
- Drøfting av behovet for en uavhengig tredjepart ("trusted third party")
- Drøfting av behovet for en uavhengig analyse av BankID før systemet eventuelt blir tatt i bruk som et nasjonalt ID-system

Bakgrunn

Noen momenter / observasjoner som har fremkommet …

- **Hole et. al. …**
  - **a) bruk av fødselsnummer muliggjør effektive DDos angrep (velg mulige F. nr. – gjett engangspassord og passord => blokkerer nesten alle IDer)**
  - **b) variabel (lav) autentiseringsstyrke ~ to faktor (inkl svake passord)**
  - **c) Man in the Middle (MitM) angrep er enkelt / mulig grunnet ubeskyttet adresse informasjon**
  - **d) non-Rep tjeneste bruker ikke en TTP**
  - **e) sluttbrukere har ikke tilgang til teknisk info om nRep**

Tolkning av observasjoner

Aspekt	a) F nr	b) 2 fa	c) MitM	d) Ikke TTP	e) Doc
Teknologi / design	x	x	x		
Sikkerhet		x	?		
Organisasjon	x			?	
Documentation					x
Ressurser (pers, utstyr)					

a) gjelder for alle som bruker F. nr som identifikator

b) spesifikk for BankID (!)

c) design / implementasjon (et spesielt BankID problem?)

d) spesiell relasjon BankID – Bank (men ikke BankID – kommune)

e) gjelder alle CAer under selvdeklareringsregime (intil videre)

Tema til diskusjon

Generell litteratur / bakgrunn

- e-signatur lov og forskrift
- QC doc, oversikt følger
- noe offentlig fra BankID (White Paper)

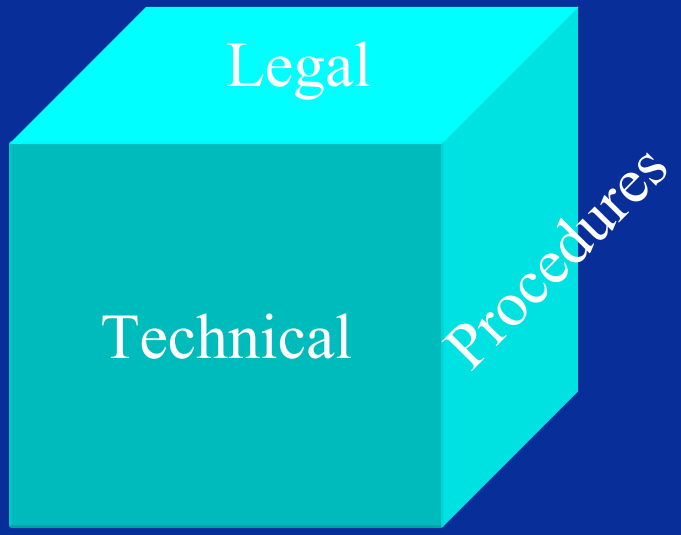
Utfordringer:

- relasjonen til andre land og nasjonale utstedere
- lik behandling av ID utstedere i det Norske markedet
- behov for analyse eller sertifisering (politisk vilje ?)

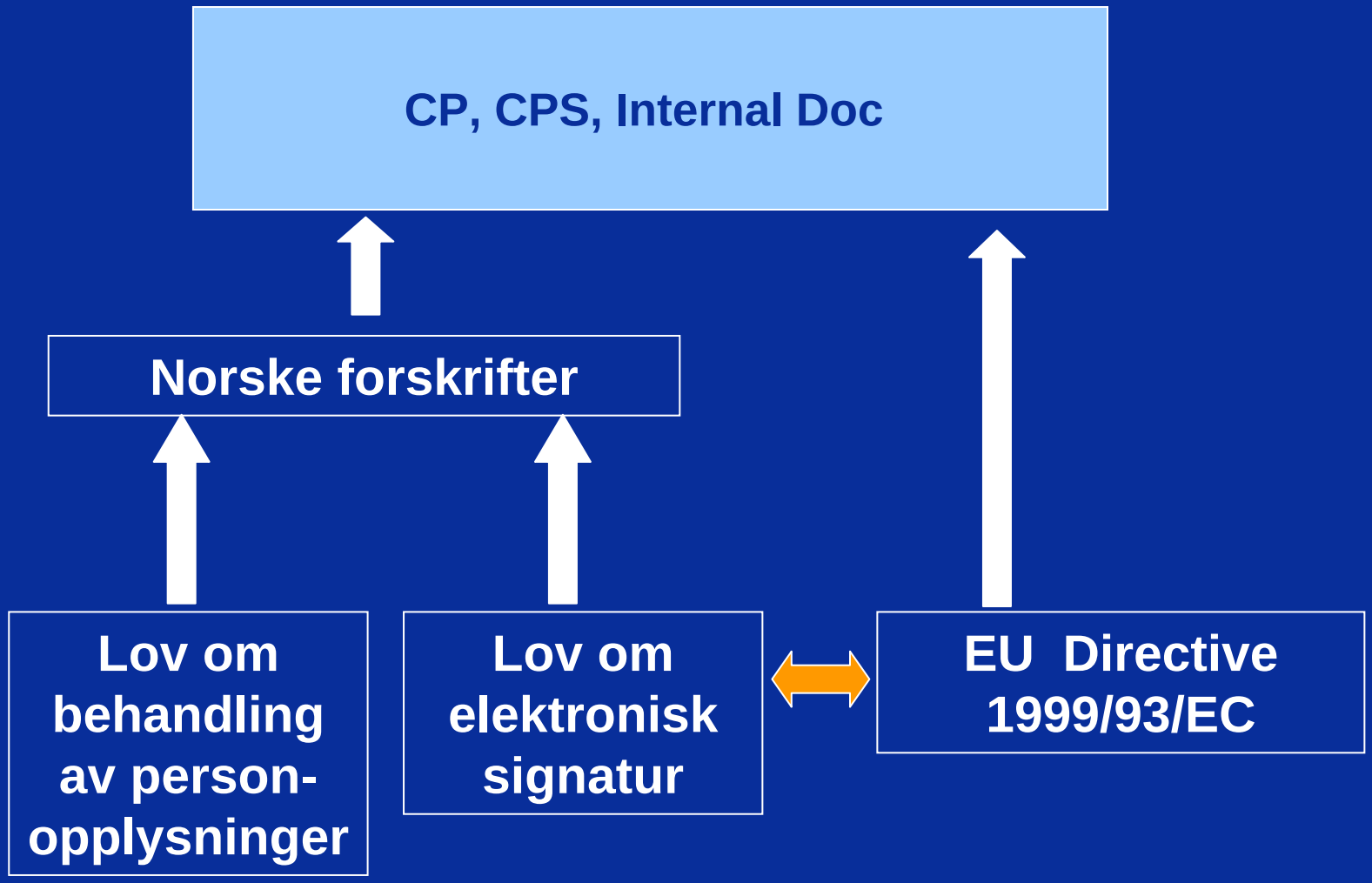
Standards and dimensions of eID

- Legal aspects (responsibility, liability, …)
- Procedural aspects (routines, procedures, doc, …)
- Technical aspects (security, crypto, cert content, ...)

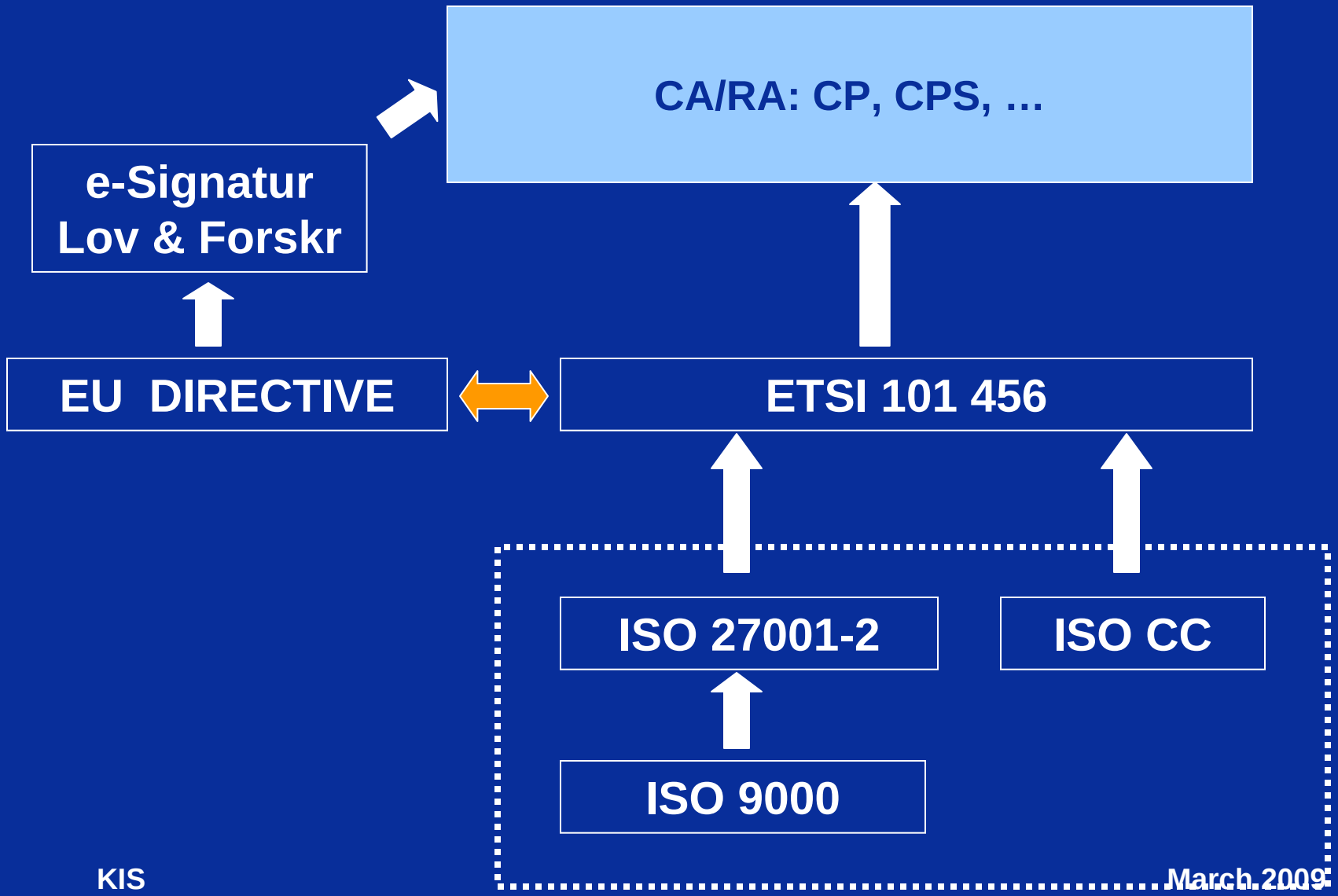
In the following the scope is issuing Certificates / e-ID in general, i.e. it is not specific to BankID and it is not about digital signatures



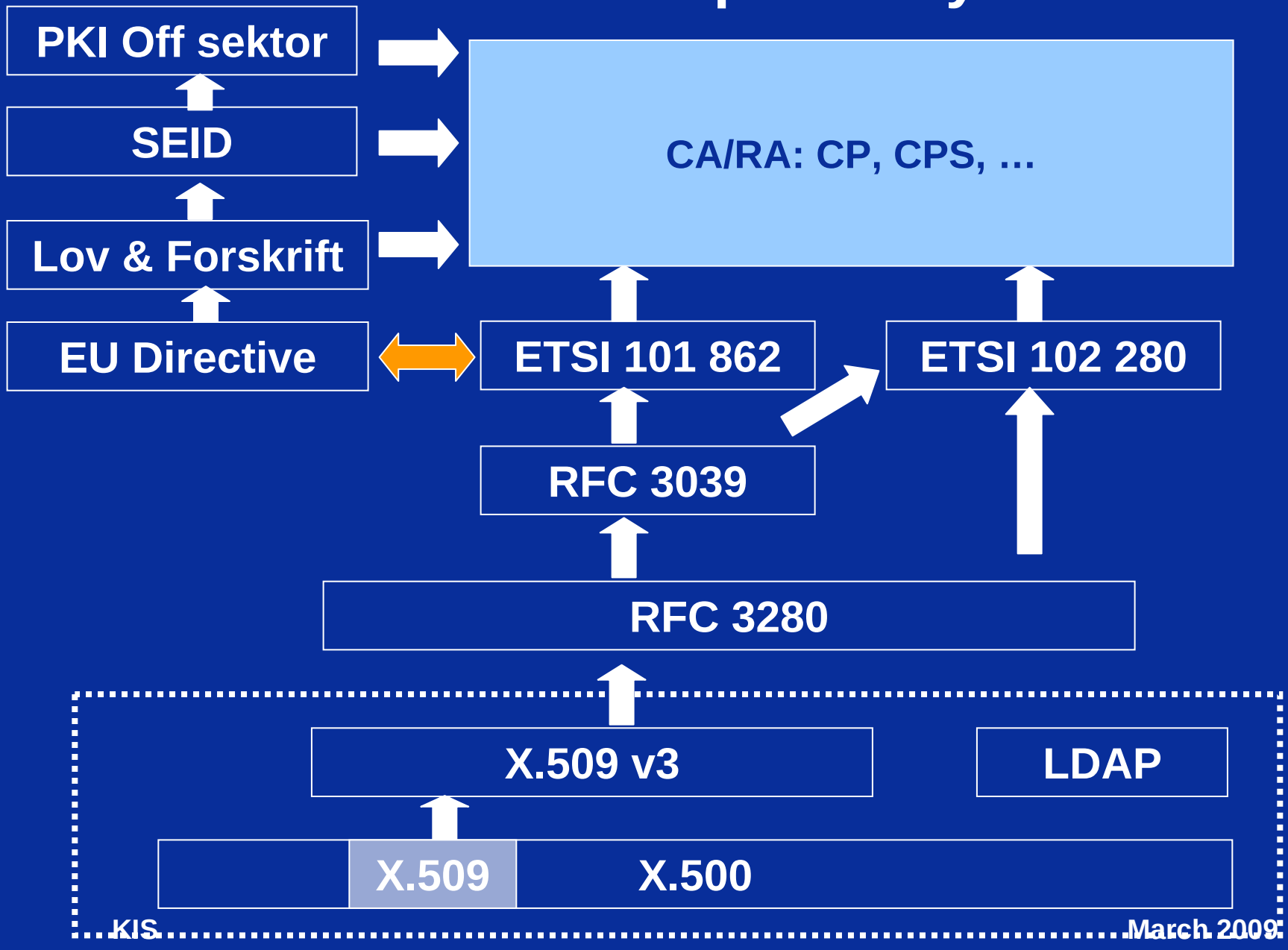
Legal Regulation



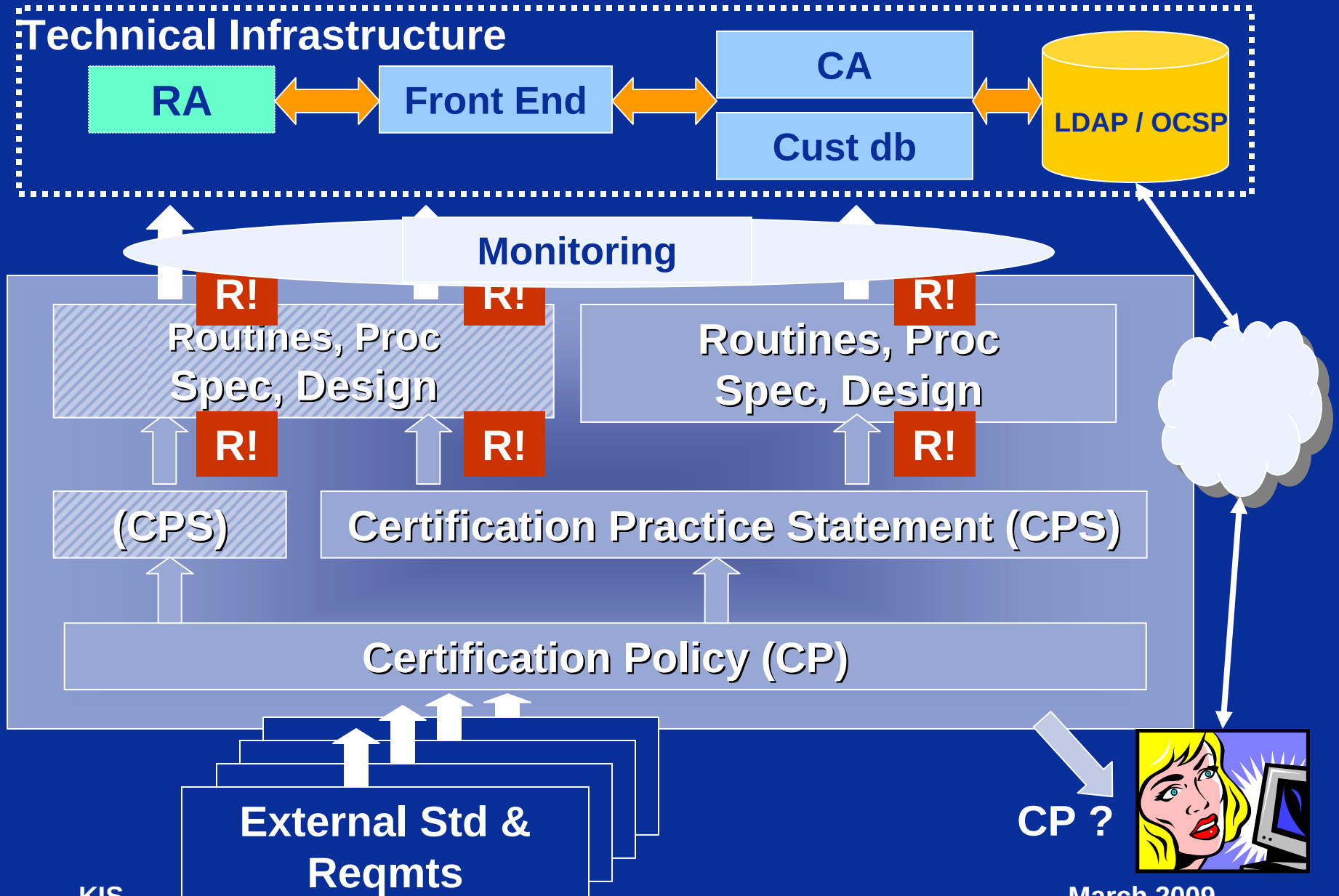
Procedures: Quality and Security Assurance



Technical: Interoperability and Security



CA; example internal Structure



Requirements, review / audit

- INPUT: all of the above => high COMPLEXITY !!
  - ITU, ETSI, IETF
  - SEID, PKI i offentlig sektor; Person Std. / Høy
  - Norsk Lov (E-signatur, Personopplysningsloven, …)

- Match against
  - CP (often only external document)
  - CPS
  - Technical Specifications, Design documents
  - Installation doc, Routines and Procedures
  - Operational doc (log, audit, training, …)

Analysis of
Business model
"Requirements"
Security Analysis
Security Review
Security Audit

- Purpose: Consistency check of all documents and operations relative to the external and internal requirements
- Questions
  - is it necessary with third part review ? (not mandatory, but very useful!)
  - if yes;
    - under what regime ? (similar to CC certification ?)
    - at what level of detail ? (all, but some by internal QA)
    - by who (?)

PROs & CONs

- Argumenter FOR ekstern revisjon / sertifisering av QC, SEID, P. Høy
  - Grunnleggende sikkerhetstekniske mekanismer i samfunnskritisk infrastruktur er uten reelt teknisk innsyn / tilsyn med dagens ordning (selvdeklarering)
  - kompleksiteten i systemene er MEGET STOR
    - systematisk og detaljert gjennomgang hever sikkerheten
  - ulike tekniske løsninger under samme regulativ skal gi (tilnærmet) samme sikkerhetsnivå
  - mer enhetlig håndtering av alle ID / Signatur leverandører
  - enhetlig kostnadsnivå for leverandørene

- Argumenter MOT
  - kostnadsdrivende
  - leverandørene har allerede gode (nok) QA regimer
  - … mer ?

- Det offentliges rolle
  - Etablere mandat til å opprette sertifiseringsordning
  - Kompetanse for å opprette og drive (?) organisasjonen
  - Finansiering (i begynnelsen)