Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Carnival

Privacy framework experience

Eirik Maus

Norsk Regnesentral

Geilo
12 mars 2005

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Personvern-varsko

- Flere og flere elektroniske spor og data
  - Forretningssystemer, registere
  - Banktransaksjoner
  - Overvåkningsvideoer
  - RFID-brikker på alle varer (snart)
- Stadig mer sammenkobling av systemer
- Veldig effektivt å ”bare slå opp”
- Integrasjon av forretningsprosesser

Politisk press for personvern

- Mange land har press på etater og bedrifter for å ha en klar "privacy policy"
- Store variasjoner, men de fleste land har personvernlover med liknende intensjoner

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER
www.nr.no

Personopplysningsloven

- § 8. *Vilkår for å behandle personopplysninger*
- Personopplysninger (jf. § 2 nr. 1) kan bare behandles dersom den registrerte har samtykket, eller det er fastsatt i lov at det er adgang til slik behandling, eller behandlingen er nødvendig for
  - a) å oppfylle en avtale med den registerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås, ...
  - f) at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.
- § 14. *Internkontroll*
- Den behandlingsansvarlige skal etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet.

http://www.lovdata.no/all/hl-20000414-031.html

Personopplysningsloven 2

- § 18. *Rett til innsyn*
  - Enhver som ber om det, skal få vite hva slags behandling av personopplysninger en behandlingsansvarlig foretar, og kan kreve å få følgende informasjon om en bestemt type behandling: (...)
- § 19. *Informasjonsplikt når det samles inn opplysninger..*
- Når det samles inn personopplysninger fra den registrerte selv, skal den behandlingsansvarlige av eget tiltak først informere den registrerte om
  - (...) b) formålet med behandlingen, (...)
- *§ 22. Rett til informasjon om automatiserte avgjørelser*
- Hvis en avgjørelse har rettslig eller annen vesentlig betydning for den registrerte og fullt ut er basert på automatisk behandling av personopplysninger, kan den registrerte som avgjørelsen retter seg mot, kreve at den behandlingsansvarlige gjør rede for regelinnholdet i datamaskinprogrammene som ligger til grunn for avgjørelsen.

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER
www.nr.no

Carnival

- Automatisert kontroll med personvern-håndheving i datasystemer
- Rammeverk for inkludering i enterprise-systemer
- Sjekker/håndheving av informasjons-bruk-regler
  - Tilgang, info-type, formål, bruker, tillatelse
- Regel-språk: EPAL (IBM / W3C)

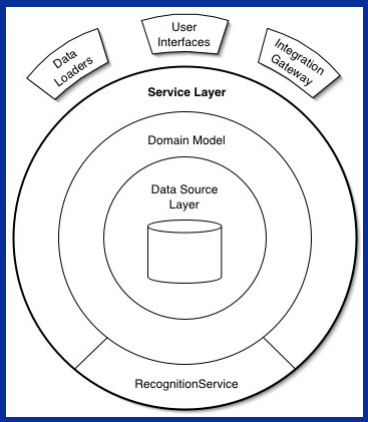
Mål for Carnival

- Ikke-invaderende rammeverk
- Mulig add-on i eksisterende systemer
  - Uten endring / minimal endring av systemet
- Full evaluering og håndheving av personvern-relaterte ikke-funksjonelle krav
- Applikasjonsuavhengige policies
- Mulig å bytte ut logikk for policies, obligations

Enterprise systemarkitektur

1. Bruker- / Integrasjons-gr.snitt (web-portal / web-services)
2. Tjeneste-/funksjonslag
3. Domenemodell
4. ~~Datakilde~~
5. Persistens: database

"systemet"



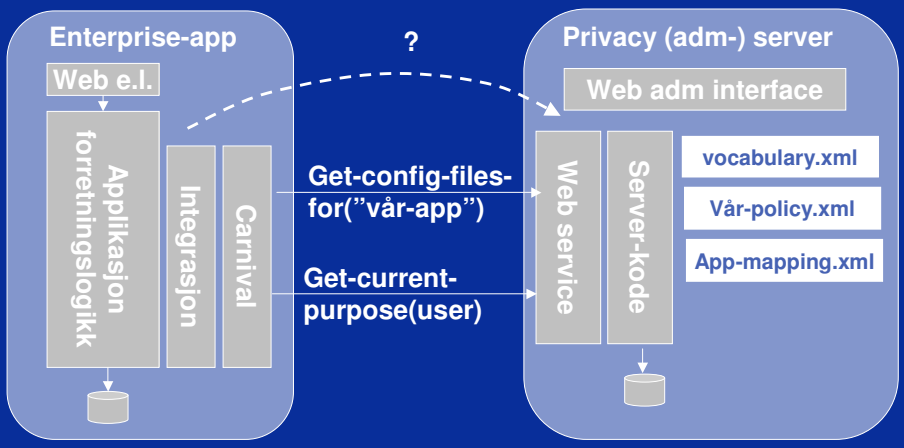
Kilde: Marting Fowler
http://martinfowler.com/eaaCatalog/serviceLayer.html

EPAL

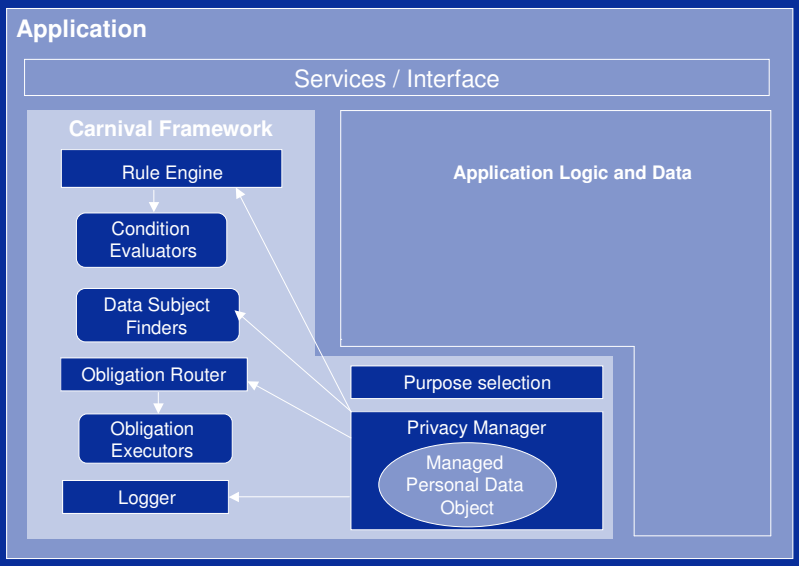
- IBM => W3C nov. 2003, impl. i Tivoli
- Vocabulary file definerer ”navnelapper” på
  - Data-typer, Bruker-roller, Data-handlinger, Formål
  - Obligations
    - x/ Må sende papirbrev til subjekt som er kredittsjekket
  - Conditions
    - x/ bruker må være datasubjektets fastlege
- Policy file : regler over vokabularet
  - Datatype, rolle, handling, formål ....
  - Ruling: allow / deny
  - (+ obligation, condition)
  - Prioritert rekkefølge, første regel gjelder

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER
www.nr.no

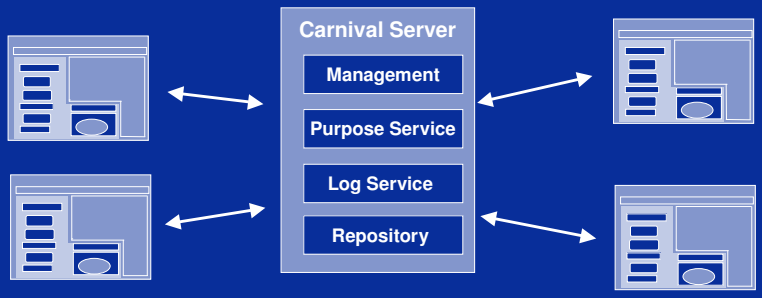
Carnival systemstruktur



Carnival Framework internals



Carnival deployment



- **Carnival-server koordinerer privacy på tvers av alle applikasjoner i konsernet**

integrasjonsutfordringer

- Hvordan integrere? Hvor?
- Hva er egentlig et ”Managed Personal Data Object” ?
- Hvordan garantere håndheving?
- Hvordan forbinde abstrakte policy-regler med konkret applikasjonskode?
- Hvordan finne brukers ”purpose”?
  - Vet HVA (action), men ikke HVORFOR

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER
www.nr.no

Første forsøk: AOP

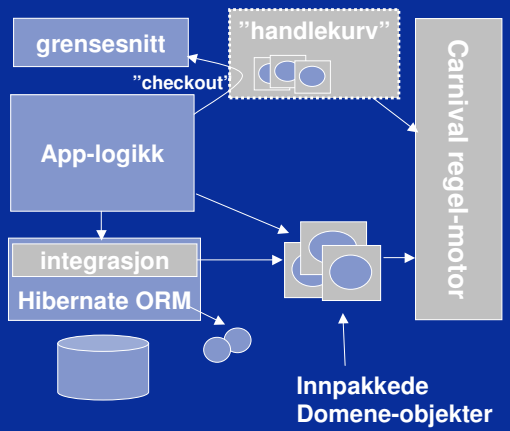
- Fokus: ikke-invadering, data aksesskontekst
- Sjekkpunkter ”veves” inn i applikasjonen
  - Context-punkt
  - Kontroll-punkt
- Purpose: regexp over context-stack

Erfaringer 1.a

- Tilfedige kontroll-punkter: ingen garanti
- Trace / context stack: dårlig ”purpose”, dødfødt
- Ingen returkanal!
  AOP kan ikke endre metodesignatur
- Hva med
  - Data som har blitt anonymisert
  - Data hvor tilgang er nektet til deler av data
  - Nekting av tilgang: grunn
  - Obligations
  - Data-subjekt neppe tilgjengelig på evalueringspunkt

Andre forsøk: dataaksess-nivå

- Fokus:
  - Garantert sjekk,
  - Tilbakemelding
- Dynamisk proxy rundt domene-objekter
- Sjekking på hver data-aksess
- ”Handlekurv” + sjekk-ut



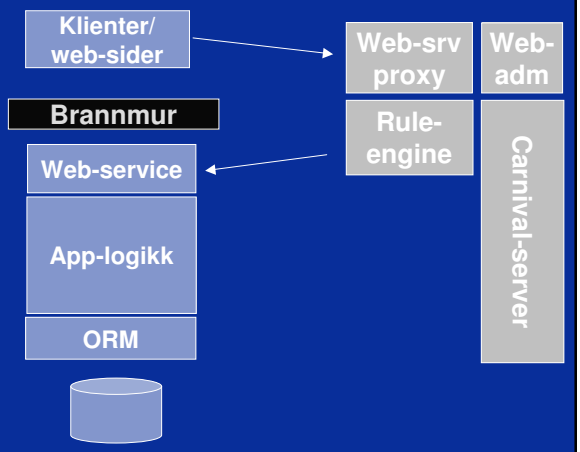
Erfaringer 2.a

- JA: Kan gi garanti på sjekking med feedback
  - Kan støtte Datasubjekt-betingelser
  - Kan inneholde evaluering-info
- MEN
  - Bruker må sette Purpose selv. Pålitelig?
  - Nytt GUI: purpose + tilbakemeldinger
  - Kan bare sjekke enkelt-attributter, ikke koblinger
  - Krever egen variant av Hibernate
  - Hva hvis getXYZ() ikke får lov? Kræsj?
  - Ikke-invaderende? Neppe...

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER
www.nr.no

Tredje forsøk: web service proxy

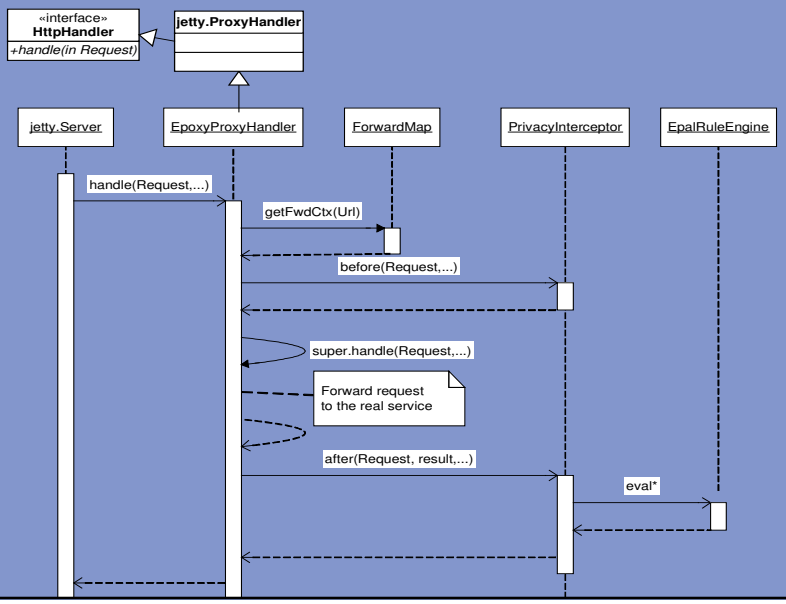
- Fokus:
  - Tilbakemelding
  - garanti
  - Brukbarhet
  - Sammenstilte data
- Personvern-proxy for Web services
- Adm: ”Montere” en webservice:
  - Ny proxy
  - Sjekker aksesser
- Map:
  wsdl => vocabulary type



Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Tredje forsøk 2



Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Erfaringer 3.a

- Fikk til allright demo: Beste så langt!
- Kan ikke lenger støtte datasubject: neppe tilgjengelig
- MEN: kan kombineres med forsøk 2

Konklusjoner 1: teknologisk

- Ikke-invaderende urealistisk: endrer jo funksjonaliteten i systemet
- Ofte: obfuskering / stryking av informasjonselementer: hva skjer?
- Krever tilbakemeldinger til brukeren: må signallere på nye måter, f.eks. vha. Farger
- Kan ikke lett legge til ”metadata” på primitive datatyper
- Må endre programkode: ikke lenger ”rammeverk”

Konklusjoner 2: konseptuelt

- Purpose: intensjoner inni hodet til brukeren
  - Kan ikke oppdages automatisk
  - Kan ikke sjekkes automatisk
- Ikke alle ikke-funksjonelle krav som kan formelt beskrives kan ha automatisk ikkeinvaderende evaluering
  - Condition: krever evaluering over domeneobjektene og deres attributter: må spesiallage programkode
- Er personvernhåndtering *egentlig* ikke-funksjonelt? Svarer vi på feil spørsmål?
- MEN: Kan benyttes til logging/overvåkning, ikke håndhevelse, av policy