Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

e - urząd a prywatność
E-government and Privacy

Dr. Wolfgang Leister
Chief Research Scientist
Norsk Regnesentral

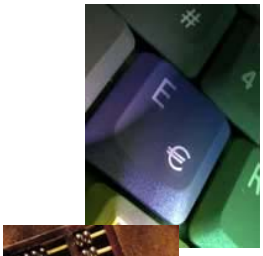
E-government Conference
Warszawa, 26. october 2005

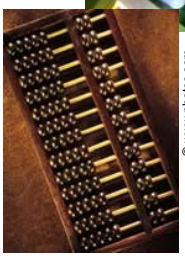
Contents overview

- The Norwegian Computing Center
- E-Government – selected topics
  - Multi-channeling
  - Privacy
- Focus: Privacy
  - Privacy Regulations and their implications
    - Example: PACSflow in hospitals
    - Experiences: Privacy Framework Carnival
  - E-Traces Report for the Norwegian Data Inspectorate

Facts about NR

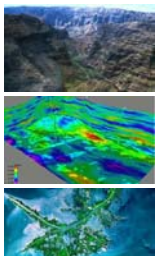
- Applied research
- Financed by
  - domestic private companies
  - public sector
  - The Research Council of Norway
  - EU
  - international companies
- ***Established in 1952***
- ***50 research scientists***
- ***Turnover 45 MNOK***
- ***Two main research areas:***
  - Information and communication technology (ICT)
  - Statistical-mathematical analysis and modeling

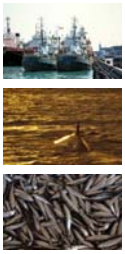


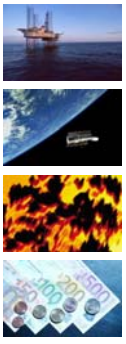


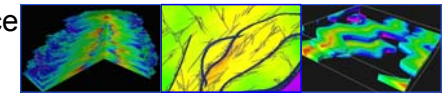
Statistical-mathematical analysis and modeling

- Natural resources
- Environment
- Petroleum
- Remote sensing
- Image analysis
- Finance and insurance









ICT Research at NR

- Security
  - Privacy
  - Digital forensics
  - Risk management
  - Public Key Infrastructure (PKI)
  - Digital Rights Management (DRM)
  - Mandatory Access Control

- Multimedia multichannel
  - Video/Audio Streaming
  - Multimedia Metadata & Databases
  - Mobility
  - Games
  - Digital TV
  - Multimedia e-learning tools

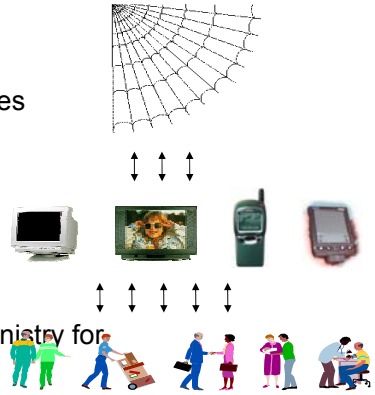
Privacy protection

- Strategic institute program 2002-2005
- 8 MNOK
  - Main topics
    - enabling organizations to protect the privacy of their customers
    - using personal information legally
    - development of a framework for enforcement of privacy policies
- Academic collaboration
    - AFIN, Faculty of Law, Univ. of Oslo

Norges forskningsråd

Service channeling (channel S)

- Strategic institute program 2000-2004
- 9 MNOK
  - Five main topics
  - Service and information architectures
  - Mobile solutions
  - User interface
  - Interoperability
  - Electronic commerce
- Multi-client R&D
  - Demonstrator for the Norwegian Ministry for Taxes

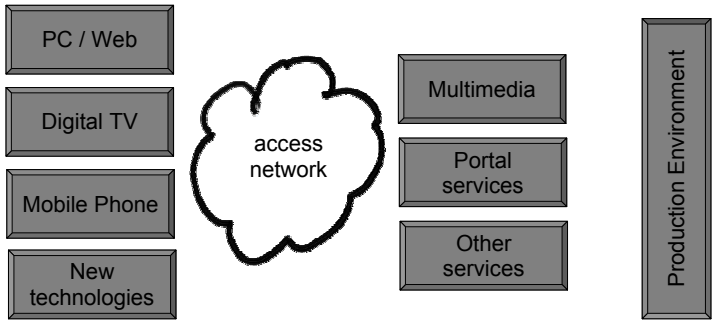


Skatteetaten

E-Government

- Principal goals in E-Government
  - Information-flow in/between departments/authorities
  - Information infrastructure for authorities and the citizen
  - Privacy and Security requirements must be fulfilled
- Service Channeling – M³Ci
  - Provide information flow through many channels
    - e.g., paper, Web, mobile phones, digital TV, new technologies
    - Public Office ↔ Citizen
    - Many services will be automated (e.g., citizen applies and has the right to receive a service when all preliminaries are in place)
    - Create Information Market Places by connecting several stand-alone services across country borders (SPACE project).

The M³Ci platform



M³Ci = MultiMedia – MultiChannel infrastructure

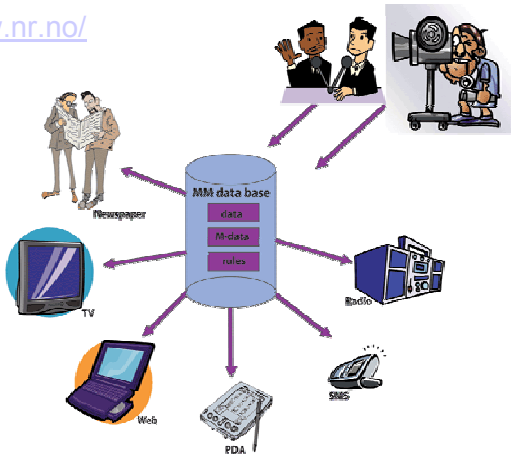
M³Ci focus

- ***Production of services and content***
- ***Unified production environment for all channels***
- ***Development of basis components, operating system support, drivers and hardware-support for M³Ci.***
- ***Scaling and use in large and varying networks***

- ***Development of components for the Norwegian Taxes Ministry / prototypes and early versions***
- ***New M³Ci services for the Norwegian Taxes Ministry, EU, health care, and other authorities.***

The ChannelS Report

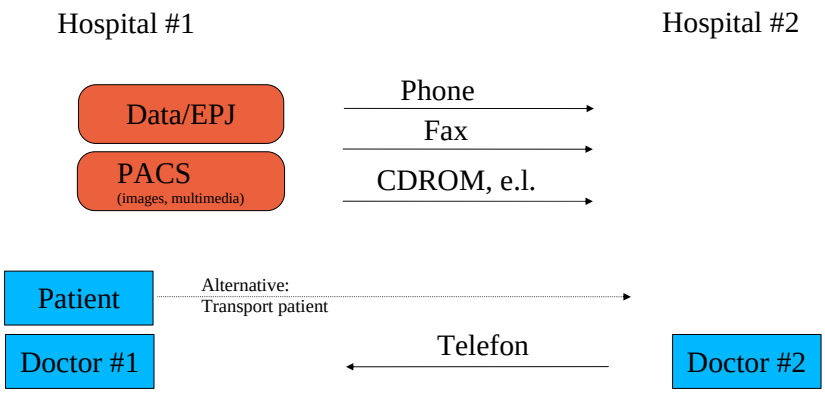
- Download from http://www.nr.no/
  - Media Transformations
  - Metadata
  - Digital TV
  - Open Source
  - Image Encoding
  - Mobile Technologies
  - Streaming
  - ...



PACSflow – Challenges in Health Care

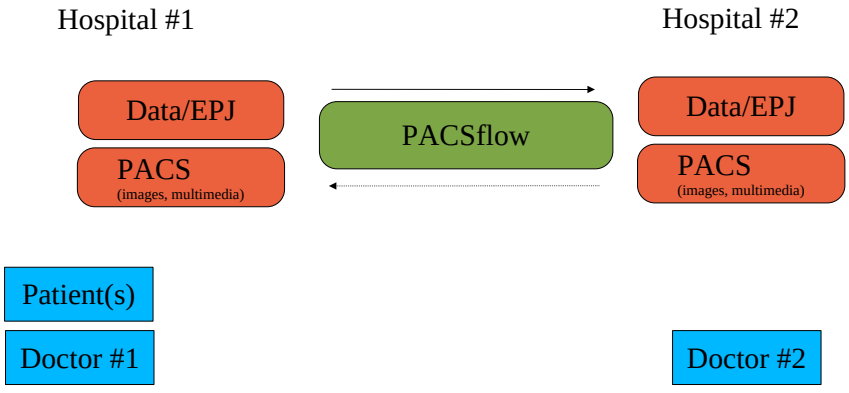
- Can high volume ultrasound images, patient reports, and messages be transferred between hospitals using the Internet?
  - Security!
  - Privacy!

Routines in health care today

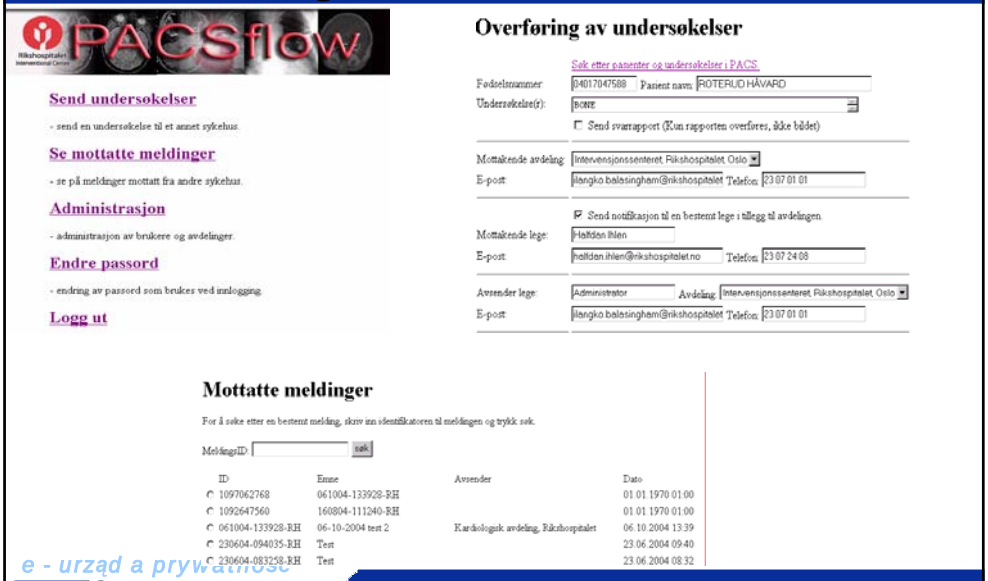


PACSflow – Høykom-project

(national norwegian project)



PACSflow – Project in Høykom-program of the Norwegian Research Council

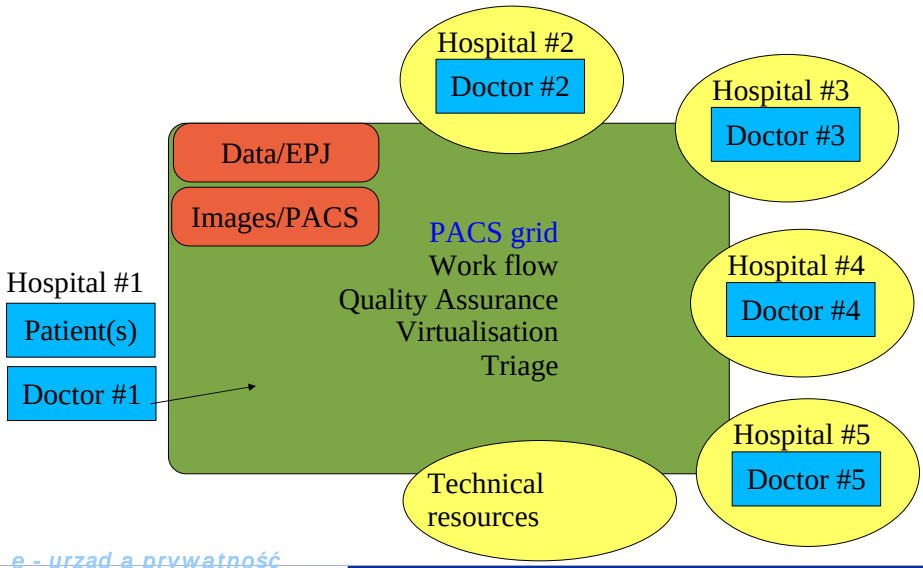


e - urząd a prywatność

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Vision – PACS Grid

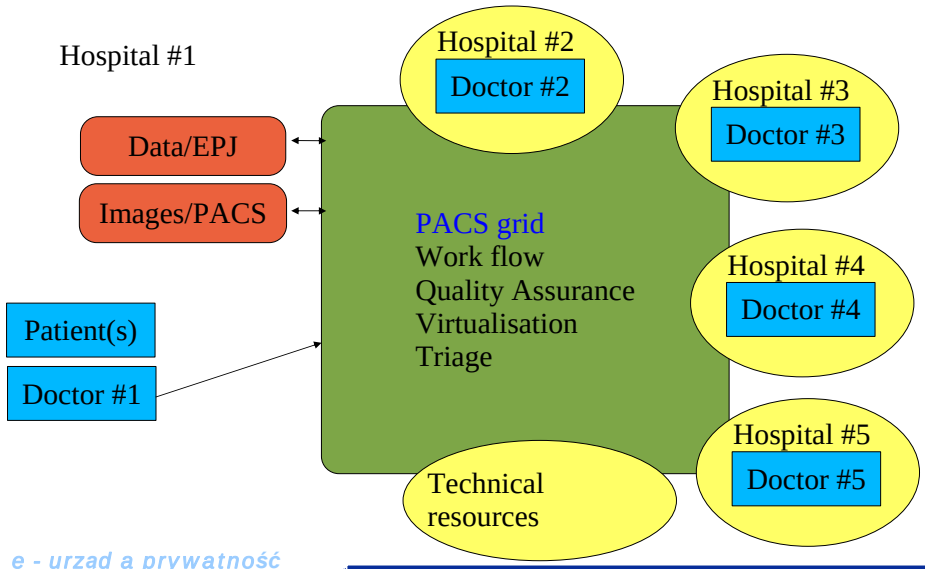


e - urząd a prywatność

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

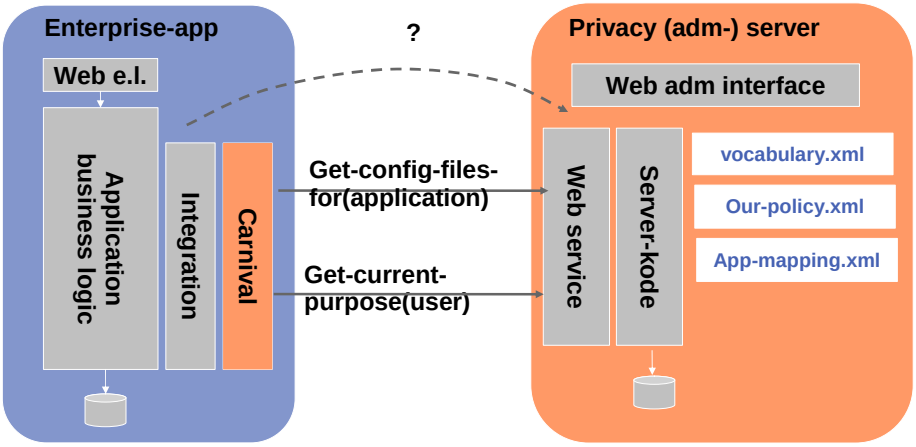
Do Privacy Requirements Disturb?



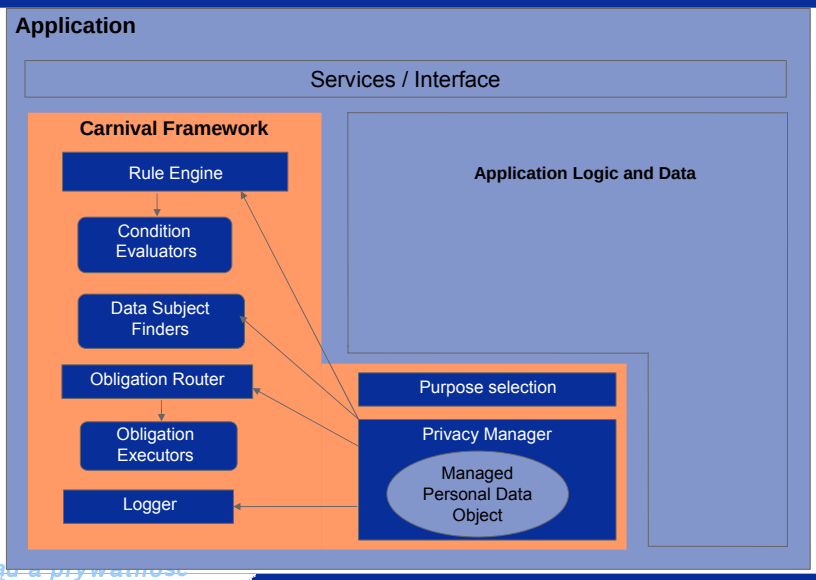
Carnival – Framework for privacy enforcement

- Automatically checks and enforces policies for information use / privacy
  - Access, information type, purpose, user, grants
  - Enterprise-wide systems
  - Rule-language: EPAL (developed by IBM / W3C)
  - Non-invasive framework
  - Add-on to existing systems / only minor changes in existing system necessary
  - Application-independent policies
  - Policies and obligations can be changed

Carnival system structure



Carnival Framework internals



Conclusions from Carnival

- Non-intrusive framework is not realistic:
  - Carnival changes the functionality in the system
  - The user must be informed when policies fail
  - Application code must be changed
  - «Metadata» cannot be attached to primitive data types ...
- Conceptually
  - «Purpose» is in user's head, intentions cannot be detected / checked
  - Not all policies have a non-intrusive evaluation. Conditions need program code that is special purpose.
- What can we learn from Carnival?
  - Carnival can be used well for logging of privacy and surveillance
  - Carnival cannot yet be used for enforcement of policies
  - But we are working on it :-)

Electronic Traces

- ***Report to the Norwegian Data Inspectorate and the Norwegian Ministry of Justice.***
- ***Describe how technologies generate electronic traces***
- ***Describe how electronic traces are generated, used and stored.***
- ***Describe sources and how information is used normally***
- ***Examples: telephone, computer networks, services on the Web, biometry, ...***
- ***"To be in cyberspace is to be recorded. … Where a vast number of activities in traditional space are inherently non-traceable, cyberspace actions are the traces themselves." (Int. Journal of Communications Law and Policy, nr.3 1999)***
- ***Copies of digital documents are identical, and can be distributed swiftly and effectively.***

Privacy and communication theory

- Axioms from Communication Theory (Watzlawick)
  - Axiom 1: One cannot not communicate
  - Axiom 2: Human beings communicate both digitally and analogically
  - Axiom 3: Communication = Content + Relationship
  - Axiom 4: Punctuation of the communication sequence
  - Axiom 5: All communication is either complementary or symmetrically
- As a consequence: One cannot avoid electronic traces!
- Electronic traces must be controlled!
  - → Research in Privacy Control

Which traces are generated – where – when – how much – how

Traces are generated and collected in all situations. These traces are of different types and stored in different places.

- Types of (personal) information
  - Identifying, localisation, health care, customer, membership, biometry, access and admission, payment, participation in public room
- Situations that create electronic traces
  - Authentication (something you know, have, are)
  - Payment (how much, where, when)
  - Admission and access control (what, when, where)
  - Trace people and equipment (RFID, GPS)
  - Use of sensors (health care, cars, alarms)

Technologies generating traces (I)

- We have investigated 12 ICT systems
- We found ca. 30 sources of electronic traces.

- Telephony — Bills – telephone log
  - PSTN — (A-nr, B.nr, time)
  - Mobile / cellular — (+ location)
- Data communication / networks — Bills – subscription
  - Access technology (analog, ISDN, xDSL)
  - Telecommunication / Internet (nasjonal – global networks)
  - LAN / WLAN
  - Personal Data Networks (bluetooth)
  - Other wireless communication (sms, wap)

Technologies generating traces (II)

- www technologies
  - **cookies**
  - **web proxies / filters**
  - **Firewalls**
- www services
  - **Search engines**
  - **Home banking**
  - **Chat-rooms**
  - **Gaming**
  - **web archives**
  - **web mail / Gmail**
- E-mail
- Payment over the Internet
  - **Kreditt, Debet**
  - **e-purse, e-cash**
- Catalogues and searching
- Video distribution – IP streaming
- IP telefony (VoIP)
- Misc
  - **Immediate Messaging**
  - **P2P networks**
- Digital Identities
  - **PKI, Digital Signatures**
  - **Delegated Identities**
- Electronic forms
- Authentication
- Admission- and access control
  - **Buildings**
  - **IT systems**
  - **DRM**
  - **Electronic tickets**

Technologies generating traces (III)

- Tracing technologies
  - RFID (passive, very tiny)
  - GPS (active, get smaller)
- Identifying technologies
  - One-to-many search, find identity of given person
  - biometry (finger prints, face geometry, iris, voice, …)
- Collection technologies (active and possibly hostile)
  - web-bugs
  - Spyware
  - keyboard loggers
  - Location tracing
  - trojan horses
    - search engines
    - packet sniffers
    - video
- Video surveillance
  - At work
  - Public (traffic, public places)

Selected Subject (I): WLAN

- Vulnerability
  - Increasing number of households install WLAN
  - Wireless (radio) networks are …. OPEN and accessible
  - Security must be switched on actively
- Reasons
  - Missing competencies (especially mass marked), including bad user manuals
  - Ignorance
- Estimates
  - ca. 50% of WLAN routers in Oslo area are without encryption.
  - Half of them have original passwords for admin user!
- Bad security → Bad privacy

DANGEROUS

Selected Subject (II): Gmail

- ***FREE***
- ***Large capacity per (2 GB)***
- ***Stores all information***
- ***Used for advertising and direct marketing***
- ***Based on content and words in each email***
  An email about bike-trip last weekend can result in advertisement on terrain bikes ...
- ***Do we understand the privacy policy?***
- ***Is it so bad?***
- ***What can the user control?***

Selected Subject (III): Web archives

- Scans «all» web pages and stores its content
- Content is seakable «forever»
  - Even if original content is removed!
- Stores «history log» of web pages over years
- Examples: http://www.archive.org
- The end user cannot control this
- BEWARE: The Web has no «regret»-button

Where are traces stored?

- Company databases
  - Customer register, Unions, Payment information
- Public accessible data bases
  - Tax lists, car registrations, «Brønnøysund-register»
- Personal equipment
  - PC – Mobile phone – PDA
  - GPS equipment, answering machine, memory sticks, CDs, DVD, ...
- Threats
  - File not completely erased («Delete» does not immediately remove content)
  - Swap-space (temporary memory of copy on hard drive)
  - Temporary files
  - Data burglery (active data collection by hostile programmes)

Technologies for Privacy

In most of the operative solutions there is an opening for storing more informations than the laws allow. Therefore, policies and work routines must be introduced to take care of privacy.

- Technical Privacy vs Policy Privacy
  - Proofs for technical privacy solutions
  - Technologies give full privacy → No need for introducing work routines
- Work routines and policies have disadvantages:
  - Can be changed without notice
  - Proof difficult whether these lead to the necessary results
- Anonymous alternatives for billing, telephony, communication are available, but are not in use – Why?

Conclusions

- For e-government applications we need both
  - Privacy
  - Multi-channeling and multimedia

  to implement good applications
- Both areas interact with each other:
  - Multi-channeling and multimedia set special requirements to privacy
- When forming policies for privacy:
  - Policies should be mostly technology-independent
  - Else strange requirements to technical solutions
    - (e.g., prohibit use of smtp protocol for certain data)

Thank You