Identity management throughout life – solutions, trends, side effects

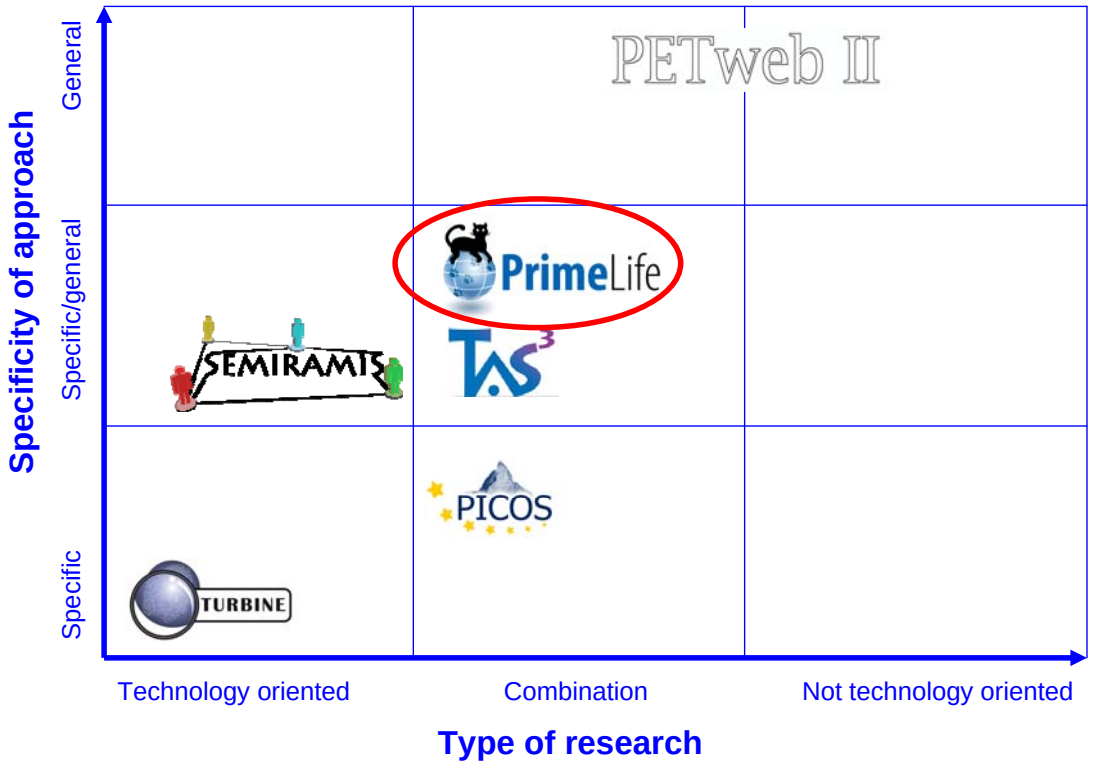
29th September 2010. Brussels.
ICT 2010: Digitally Driven. Networking session Day 3.
Marit Hansen – ULD (Data Protection Authority Schleswig-Holstein), Germany

Our networking session

Agenda

- Introduction: project overview
- 8 min slots per project
- … sums up to 45 minutes = 1st half
- 2nd half:
  - Discussion
  - Collaboration
  - Networking

Project overview



Identity management throughout life – solutions, trends, side effects

PrimeLife

Privacy and Identity Management in Europe for Life

29th September 2010. Brussels.
ICT 2010: Digitally Driven. Networking session Day 3.
Dieter M. Sommer – IBM Research, Zurich, Switzerland

PrimeLife PICOS TURBINE PETweb II SEMIRAMIS

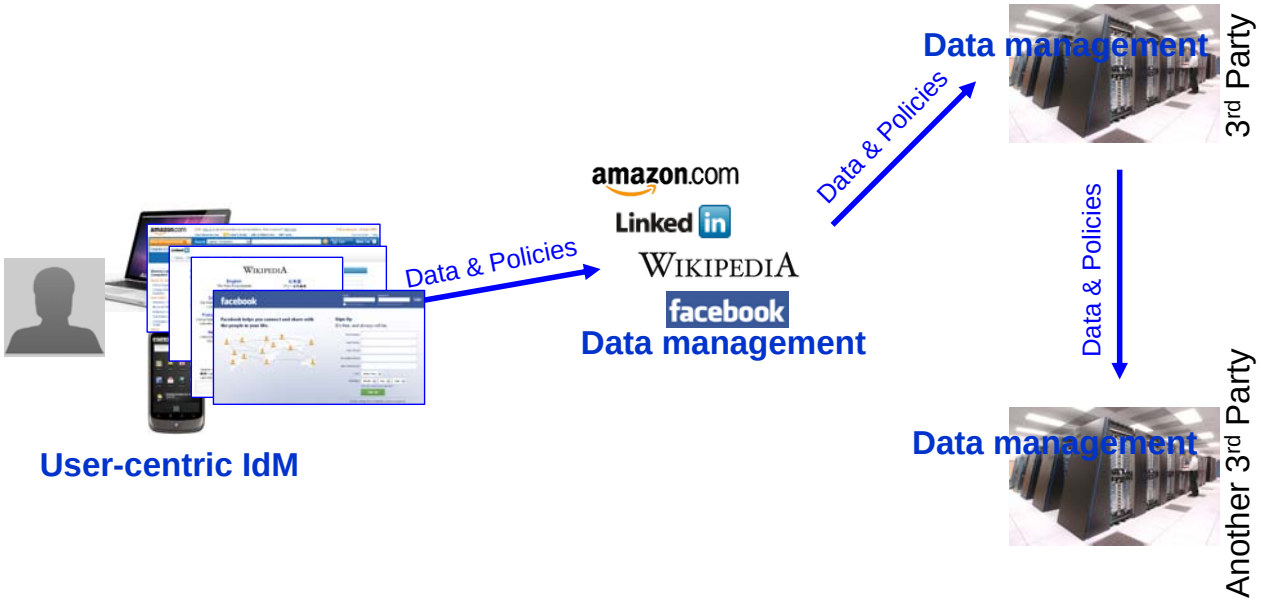
Why PrimeLife?

A person's digital footprint grows massively over time

Storage is getting ever cheaper, data mining more powerful

Challenge: User Information Management

A User And Her Electronic Interactions



PrimeLife PICOS TURBINE PETweb II SEMIRAMIS

PrimeLife's Vision

In the Information Society, users can act and interact in a safe and secure way while retaining control of their private sphere.

PrimeLife's History

PRIME Privacy and Identity Management for Europe — 2004-2008

PrimeLife — 2008-2011

2004-2008

Privacy in user-centric IdM
Data minimization
Privacy-enhanced policies
Basic research

2008-2011

Privacy in life
Web 2.0 use cases
E.g., Social networks
Privacy live: Dissemination
Continuing basic research

- **Budget**
  around €15 Million
- **Duration**
  March 2008 to Feb 2011
- **15 Partners**
  from Enterprise, Academia and Government

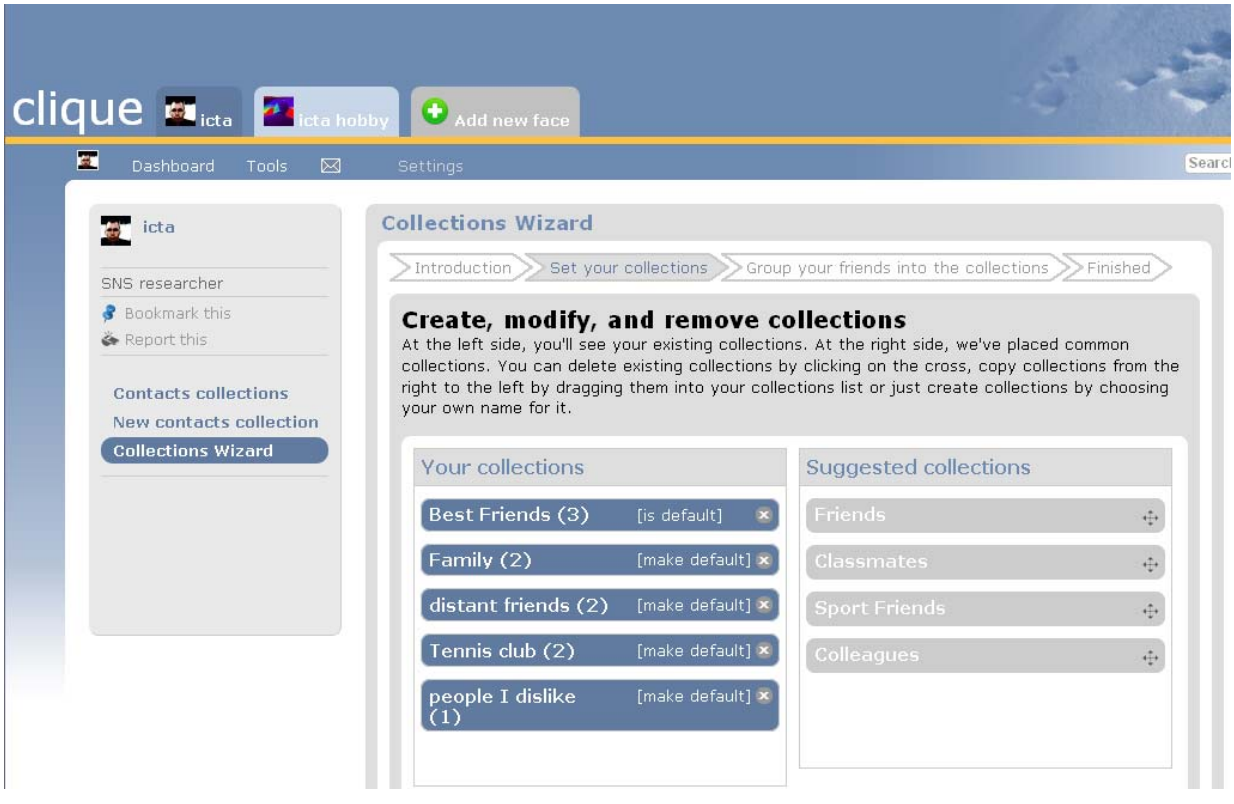
What PrimeLife is doing

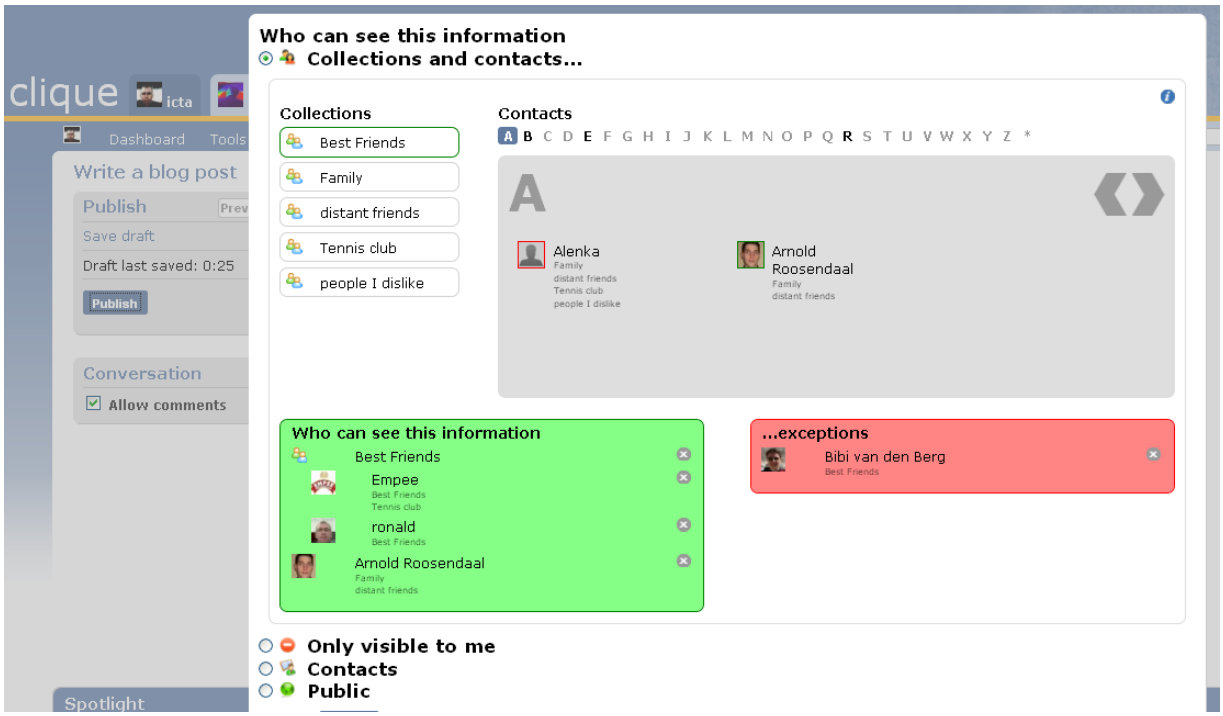
Examples

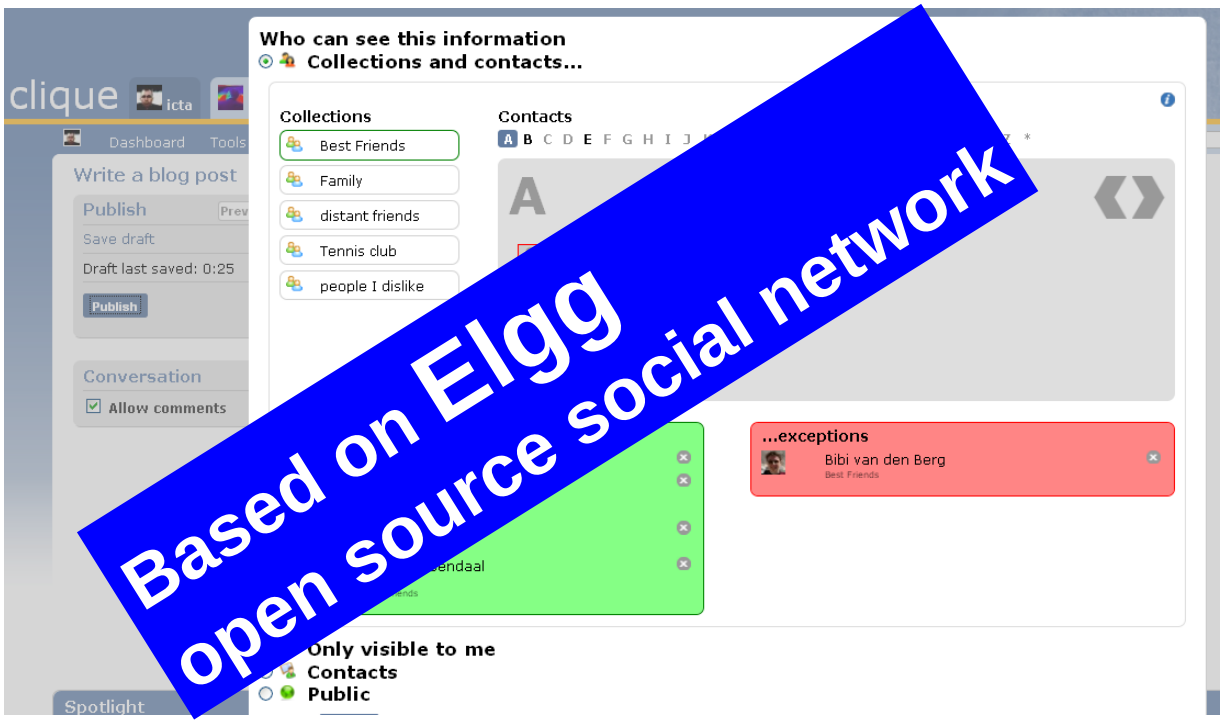
Social Networks

Clique

[Motivation: see www.facebook.com for page with compromising content]

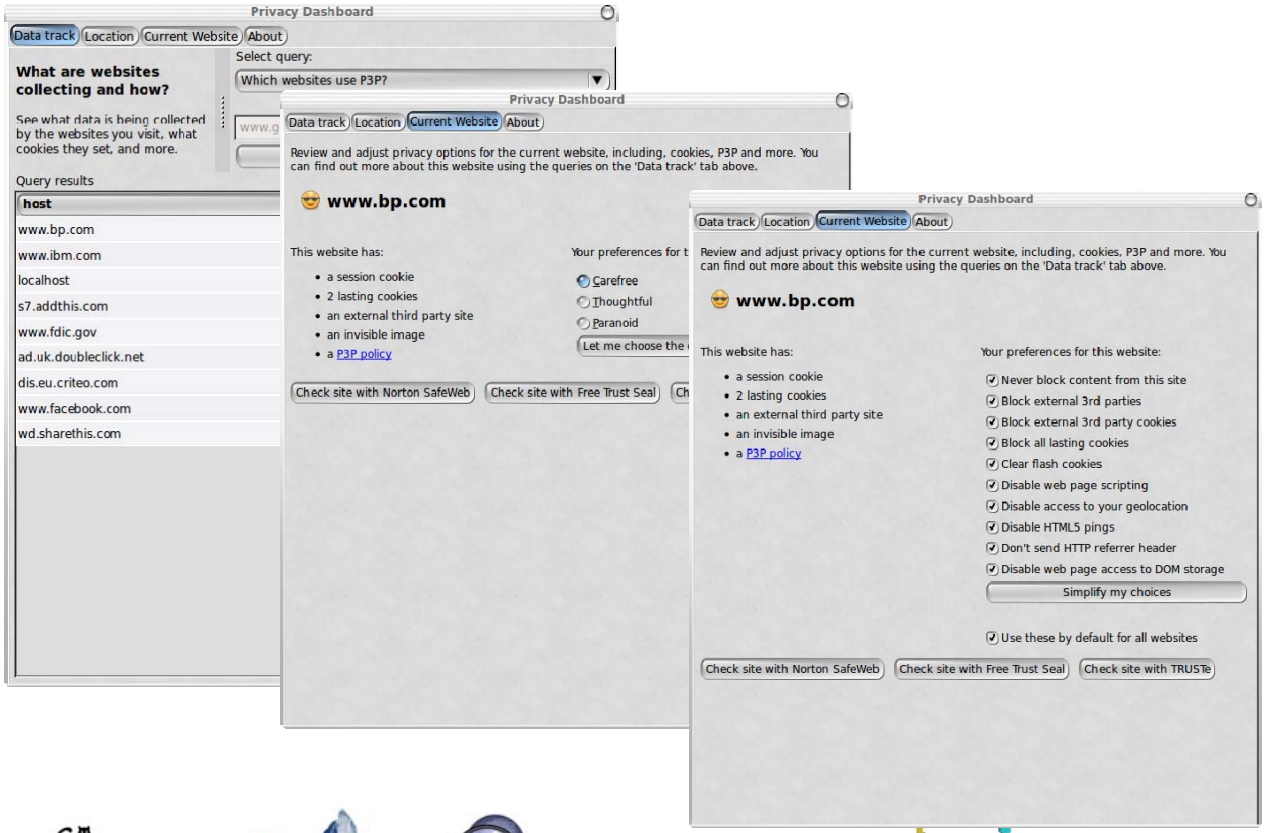



clique
icta
Dashboard
Tools
Write a blog post
Publish
Save draft
Draft last saved: 0:25
Publish
Conversation
Allow comments
Spotlight
Who can see this information
Collections and contacts...
Collections
Best Friends
Family
distant friends
Tennis club
people I dislike
Contacts
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z *
A
Alenka
Family
distant friends
Tennis club
people I dislike
Arnold Roosendaal
Family
distant friends
Who can see this information
Best Friends
Empee
Best Friends
Tennis club
ronald
Best Friends
Arnold Roosendaal
Family
distant friends
...exceptions
Bibi van den Berg
Best Friends
Only visible to me
Contacts
Public


clique
icta
Dashboard
Tools
Write a blog post
Publish
Save draft
Draft last saved: 0:25
Publish
Conversation
Allow comments
Spotlight
Who can see this information
Collections and contacts...
Collections
Best Friends
Family
distant friends
Tennis club
people I dislike
Contacts
...exceptions
Bibi van den Berg
Best Friends
Only visible to me
Contacts
Public
Based on Elgg
open source social network

Web Browsing
Privacy Dashboard

ICT 2010 Identity management throughout life – solutions, trends, side effects

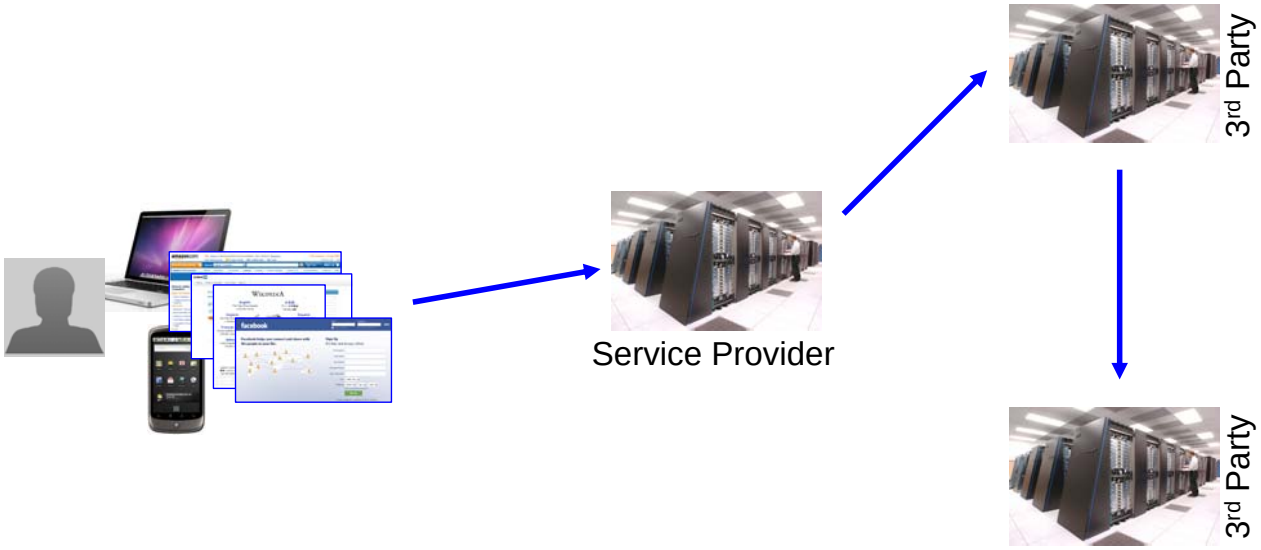


http://www.primelife.eu/results/opensource/76-dashboard

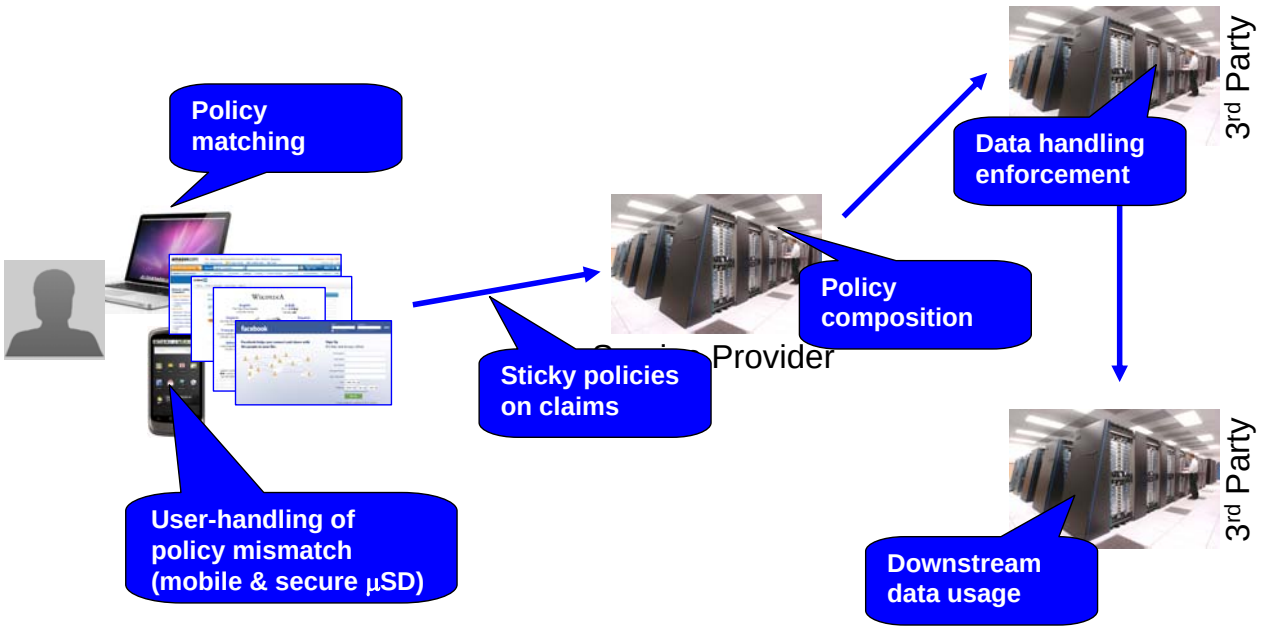
Try it now!
[on Firefox 3.6 or greater]

Service Composition & Policies

Service Composition & Policies



Service Composition & Policies



Open Source

www.primelife.eu/

PrimeLife exhibition stand

Hall 7, “Safety and Security” area
Stand id 2928, “PrimeLife”

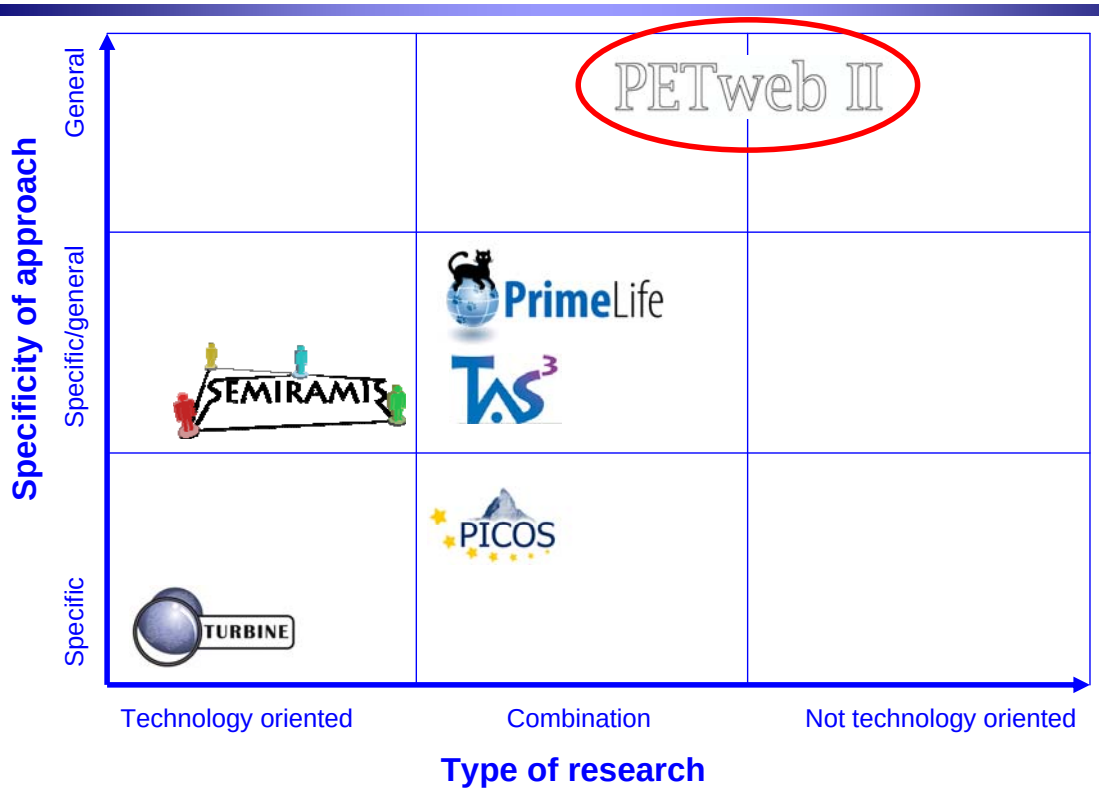
Come and see our (open source) products and talk to PrimeLife!

Dieter M. Sommer, IBM Research
dso@zurich.ibm.com

on behalf of the PrimeLife Consortium

www.primelife.eu

Project overview



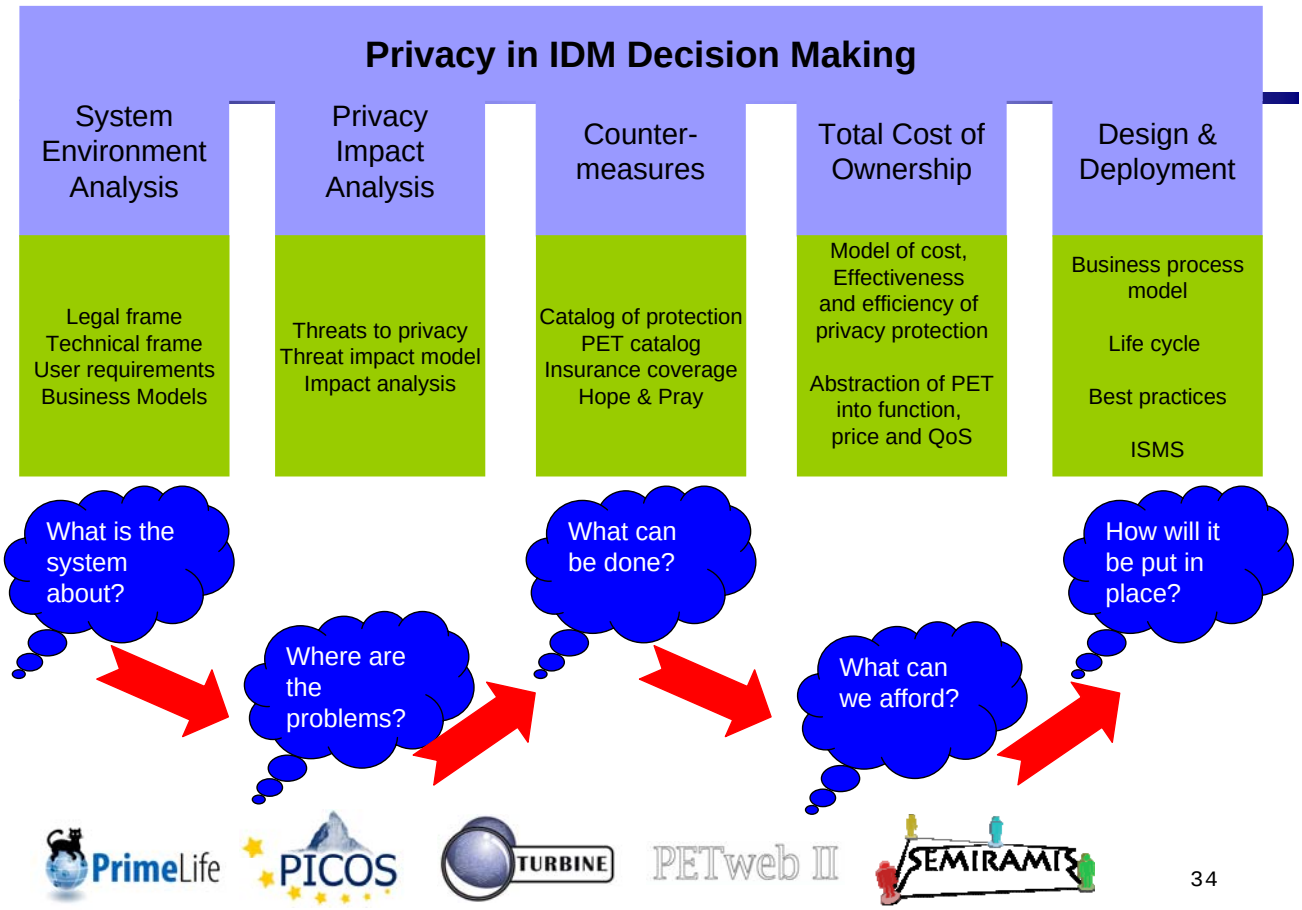
Identity management throughout life – solutions, trends, side effects

PETweb II – Privacy in Identity Management

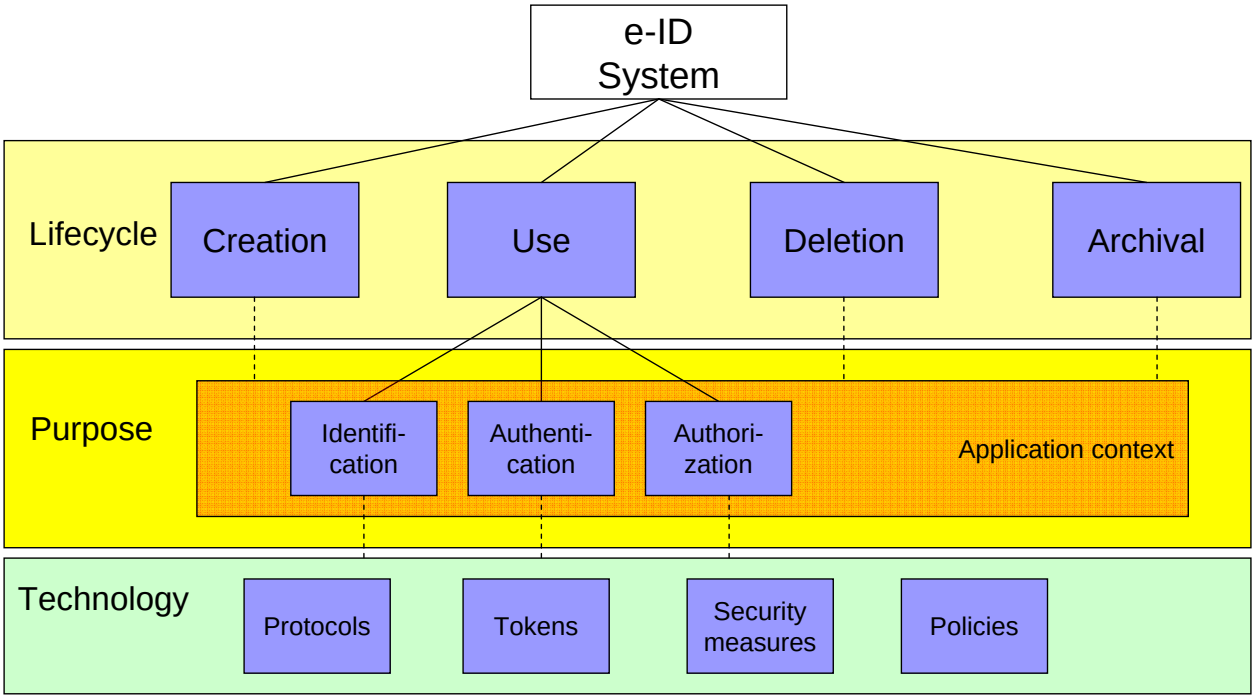
29th September 2010. Brussels.
ICT 2010: Digitally Driven. Networking session Day 3.
Lothar Fritsch – Norwegian Computing Center, Oslo, Norway - http://www.nr.no/

PETweb II: Privacy respecting IDM for Norway

- Vision:
  - Help system owners chose the right IDM systems with good privacy properties
  - Provide metrics & analysis methods
  - Case studies and best practice examples
- Project outline:
  - Develop understanding of risk factors
  - Develop simulation/analysis tool for privacy analysis
  - Educate and graduate 2 PhD students
  - Network with Norwegian stakeholders



Analysis of risk & side effects created by e-ID



Risk factors in IDM & e-ID

- We're working with qualification and quantification of risk-relevant properties.
- Particular focus: What happens when IDMS get new applications attached? What are risks originating from function creep?

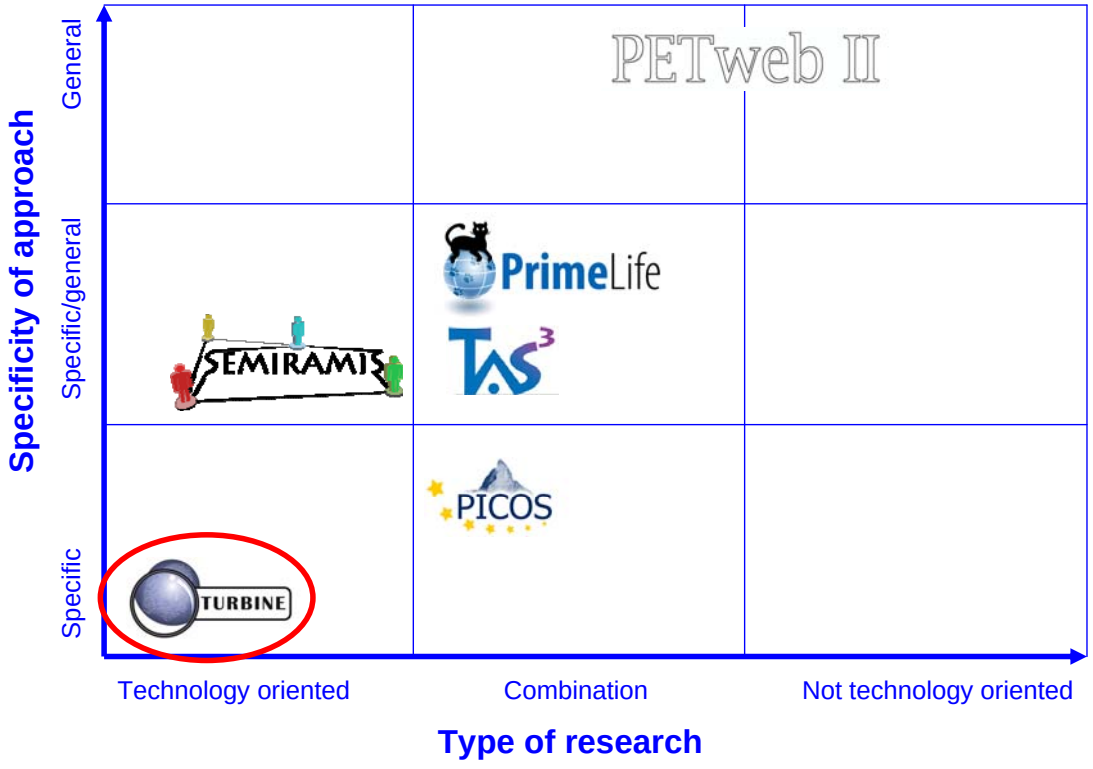
Risk contributing factors	*Parameters*
Secrecy of Authentication tools	Publicly known, inferrable, secret
Mobility of Authentication Tool	Copyable, remotely usable, concurrently usable, immobile
Claim type	single, multiple
Risks to IDM	loss, misuse, disclosure, disruption, theft, replacement value
Provisioning	creation, edit, deletion
Frequency and duration	Uses per year, total life time of identifier/transaction
Use/Purpose	Authentication, Authorization, Identification
Personal attributes	Forced, chosen, role, pseudonymity
Obligations & policies	Relationship to ID, Relationship to PI

EU collaboration interests

- Call 7
  - Privacy design and IDM concepts in e-Health
  - Privacy and e-ID challenges in the Internet of Things
  - Usability, User interfaces, and e-inclusion issues
- Call 8
  - Further development of trustworthy components with known privacy and risk properties
  - Tools and methods
- … and any other issue is welcome
  - Privacy economics, Usability testing, Lifelong e-ID,…

PrimeLife PICOS TURBINE PETweb II SEMIRAMIS

Project overview



Identity management throughout life – solutions, trends, side effects

TURBINE

Authentication: trusted individuals preserving personal data

29th September 2010. Brussels.
ICT 2010: Digitally Driven. Networking session Day 3.
Nicolas Delvaux – Morpho

Authentication

- How user can authenticate?
  - Login/password
  - Token (smart card, mobile, …)
  - Personal data (Face, voice, Fp)

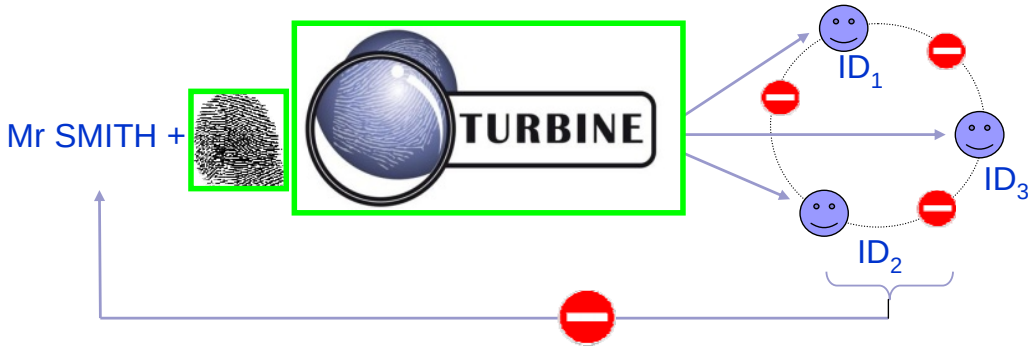

"On the Internet, nobody knows you're a dog."

- Service providers
  - Legal approach "click for consent"

Biometrics: a solution for authentication?

- YES !
  - Biometrics characteristics to guarantee excellent authentication level
    - Universality, Uniqueness, Permanence, Collectability.
- NO !
  - Biometrics characteristics authenticate **FOREVER**!
    - No way for a citizen to repudiate his personal biometrics data
- Solution through state-of-the-art protection
  - Crypto-graphic with symmetric or asymmetric keys, smart cards
  - Ready to be unbreakable for a full live?

Crypto –Biometrics techniques for identity

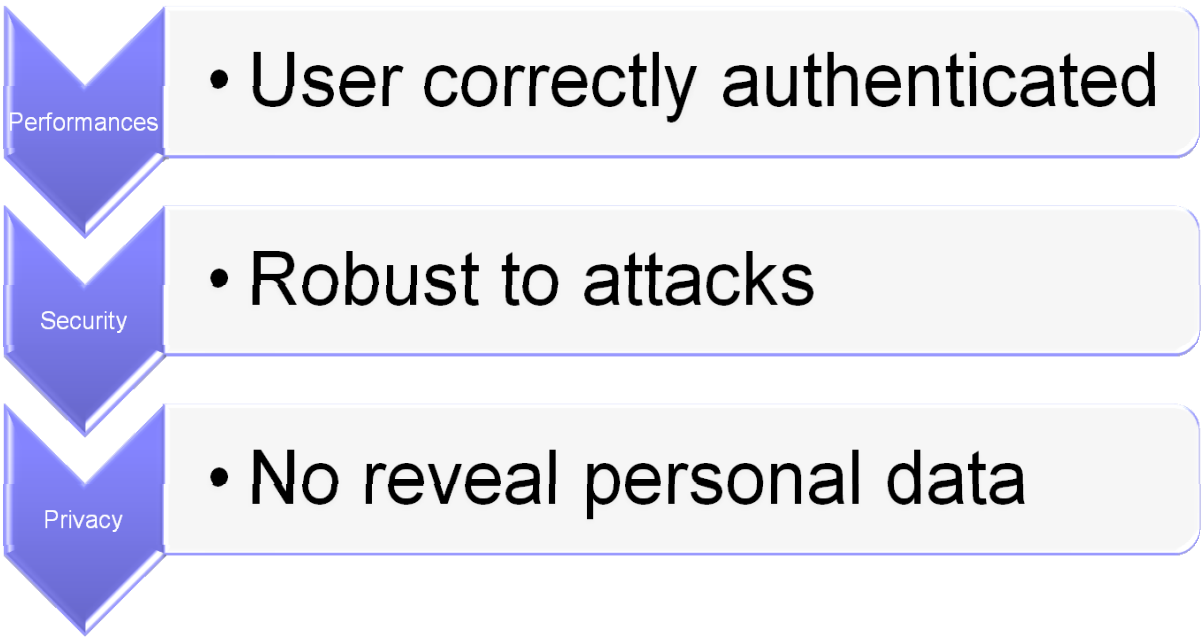


To transform fingerprint

1. into “pseudo-identity”
   - Parameters create independent identities:ID_1, ID_2, … ID_n
   - No possibility to link different “pseudo-identities”
2. without reverse-engineering capability

➔ **Revocation** of pseudo-identities is possible!

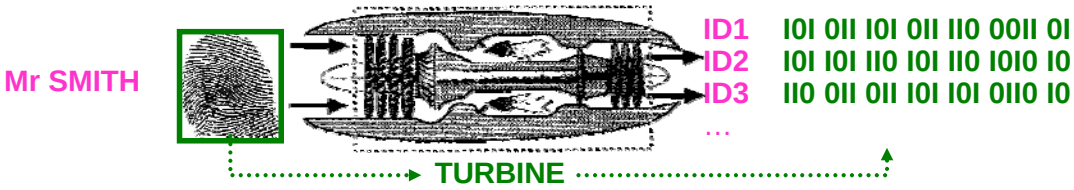
Challenges addressed



Performance challenge

- Fingerprint systems are accurate
  - As example, FVC 2002:
    - FRR (FAR 1%) = 0.11%
    - FRR (FAR 0.1%) = 0.14%
    - EER = 0.14%
- TURBINE target operational accuracy
  - Verification for access control
  - To deliver identity trust

Security Challenge



- Different identities (pseudo, voter, tax payer, …)
  - **But non link between identities**?
- Fingerprint is transformed & substituted instead of encrypted
  - **But non way to reverse**?

Attacks on crypto-biometrics:

- FAR attack; Inverting the hash; Hill Climbing attack; Nearest Impostors attack; Attacks on the Error Correcting Code; Non-randomness attack; Re-usability attack; Blended substitution; Linkage attack

Privacy framework challenge

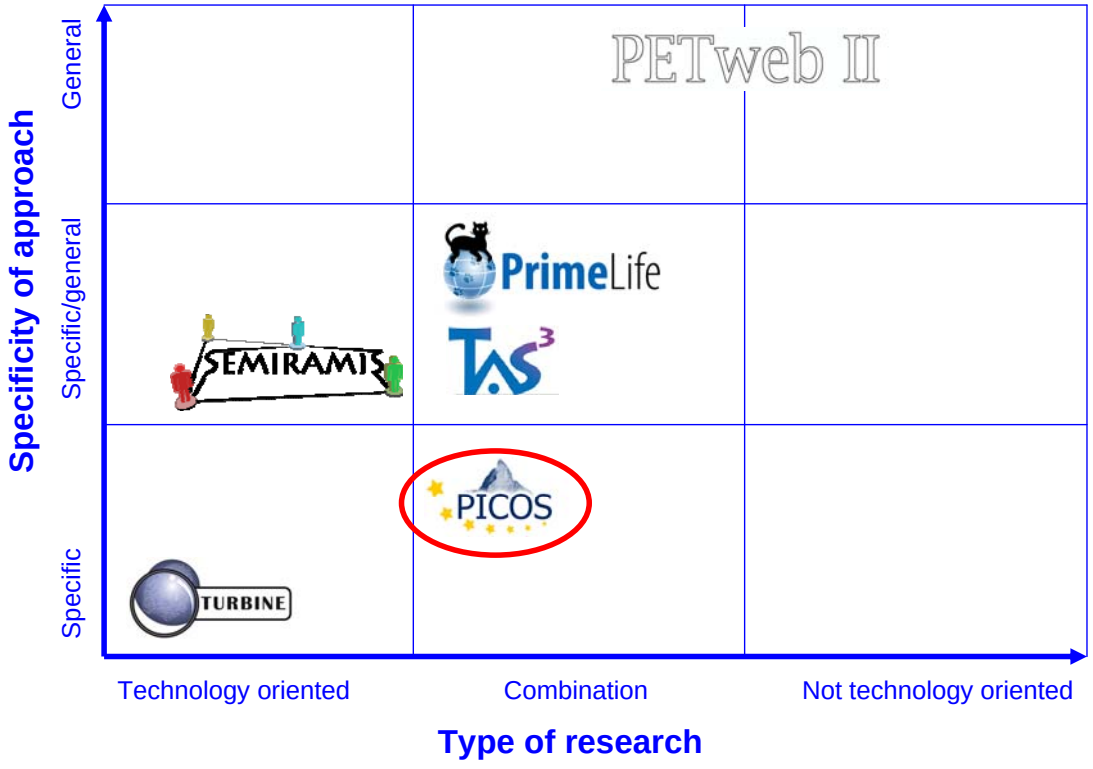
- Identity management must be in accordance with EC 95/46 Directive on Data Protection

- TURBINE
  - Assessment of security Identity management Scheme
  - Secure element to store some information
  - EDPS opinion on the overall scheme

TURBINE

- TURBINE:
  - A PETs IDM technology
  - A tool in a more secure network
  - A biometric authentication for specific services (e-Gov, health, …)
- Technology contribution related to trusted identity authentication

Project overview



Identity management throughout life – solutions, trends, side effects

Privacy and Identity Management for Community Services (PICOS)

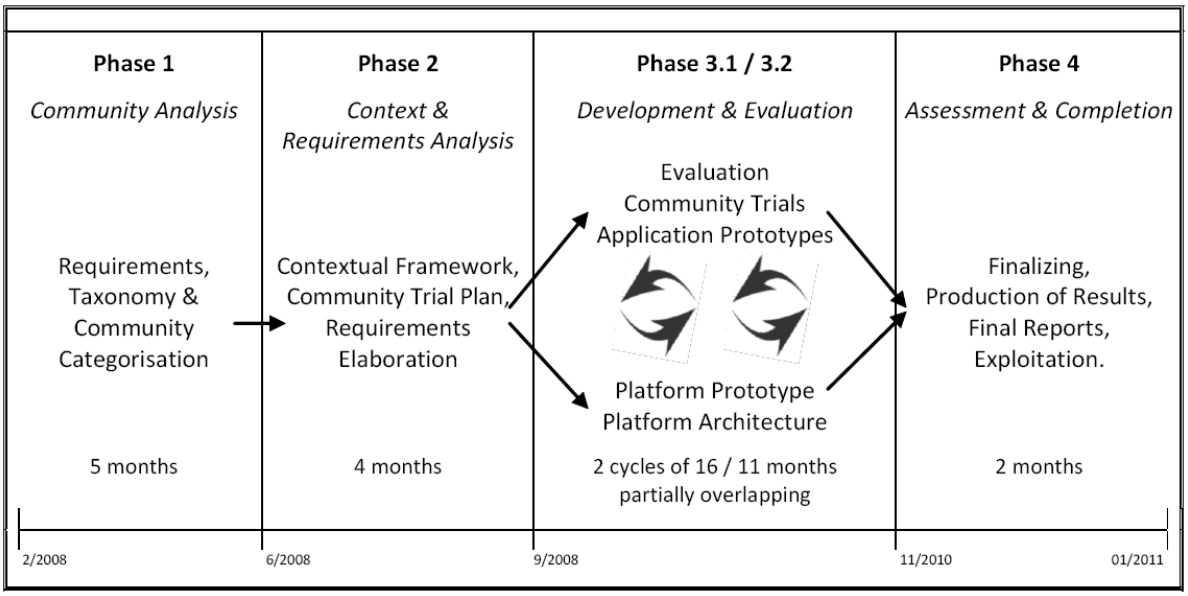
29th September 2010. Brussels.
ICT 2010: Digitally Driven. Networking session Day 3.
Markus Tschersich – Goethe University Frankfurt

PrimeLife PICOS TURBINE PETweb II SEMIRAMIS

Scope

- Focus:
  - Privacy in mobile communities
    - How to improve **trust** and **privacy** in service provision to these communities?
    - What supporting services and infrastructure?
- Challenges:
  - Client mobility & locatability
  - Small devices/UIs
  - Independence from phone types/OSs
  - Independence from comms service providers

Project approach

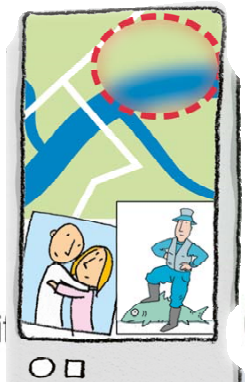


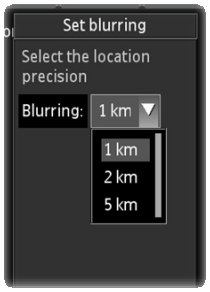
PICOS prototype “AnglerApp”

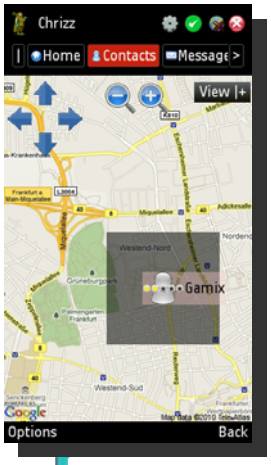
- Prototypical implementation for field trials
- Advanced privacy and identity management features optimized for mobile communities
  - Sub-Community
  - Location Blurring
  - Private Rooms
  - Partial Identities
  - Privacy Advisor

Location Blurring

- A user's location is obfuscated on a map to
  - hide its (exact) position
  - allow only selected people to view the exact position
- Different levels of blurring
  - to control the degree of obfuscation





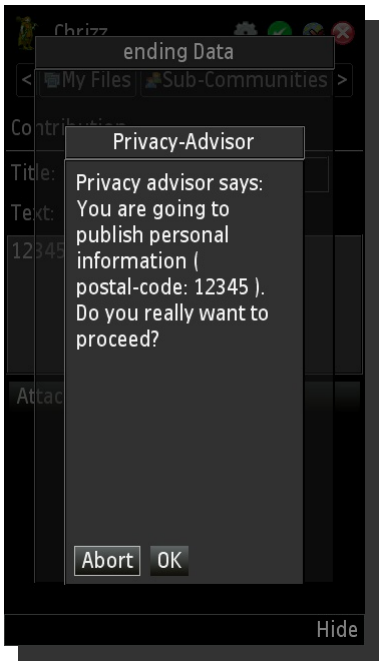


Partial Identities

- Different Partial Identities for different usage contexts
  - e.g., for usage in different sub-communities to reflect various roles of users
- A limited set of personal information is disclosed for each Partial Identity

Privacy Advisor

- Provides privacy-related guidance to users (e.g., regarding disclosure/sharing of location info, street address)
- Based on the user's current behaviour and context

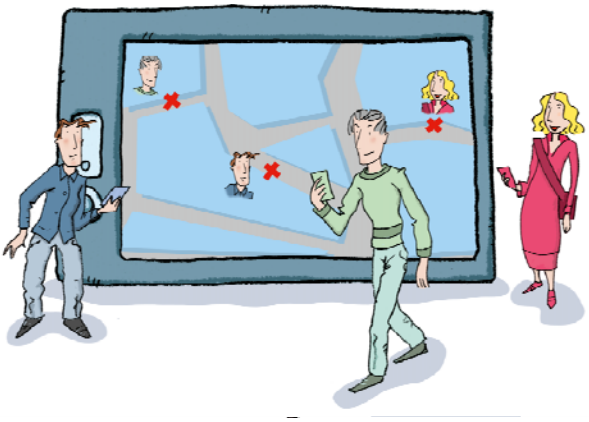


PICOS prototype "GamerApp"

- Prototypical implementation for field trials
- Interaction between players outside of the game
  - Via mobile devices and fixed web clients
  - Enhancement of trust and privacy features in AnglerApp
  - Consideration of marketing/advertising aspects in order to exploit emerging marketing opportunities

Open topics and further work

- Mobile Communities with Location-Based Services
- Trust and Privacy towards service provider
- New Cases: Business, Healthcare,…

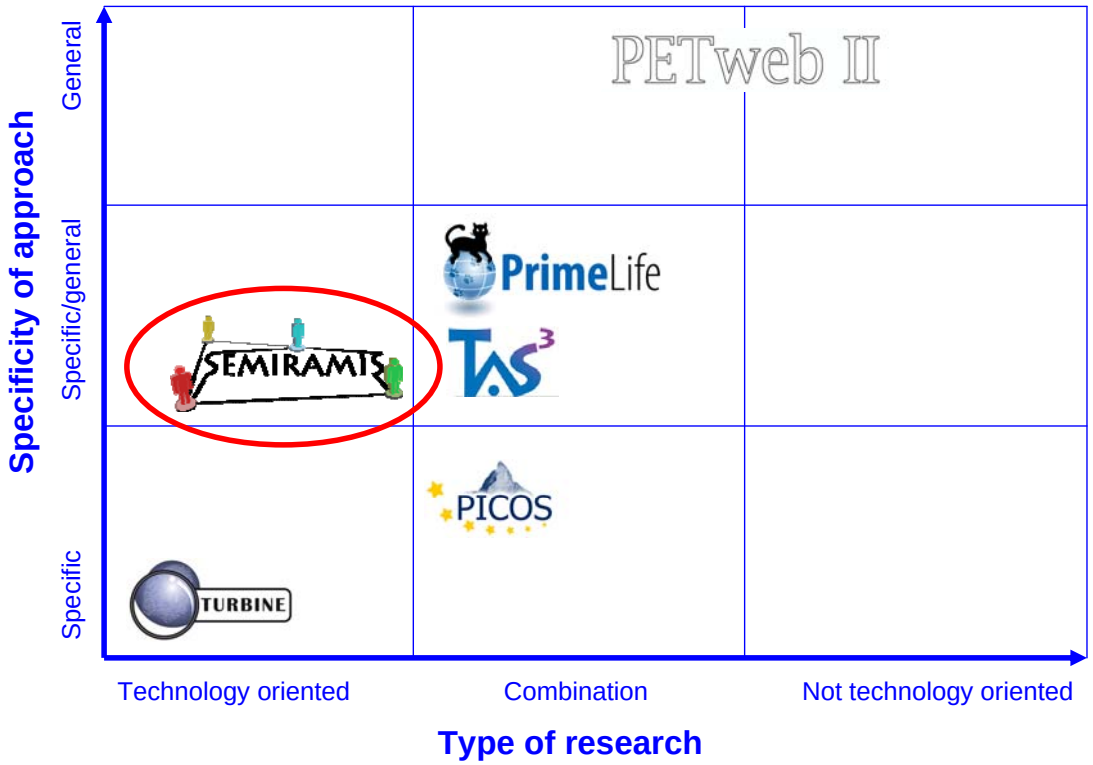


More information

Visit our stand:
R7.09
or
www.picos-project.eu

contact@picos-project.eu
twitter.com/picos_project
www.facebook.com/picos.project

Project overview



Identity management throughout life – solutions, trends, side effects

SEMIRAMIS

Secure Management of Information across multiple Stakeholders

29th September 2010. Brussels.
ICT 2010: Digitally Driven. Networking session Day 3.
Charles Bastos Rodriguez – Atos Origin

SEMIRAMIS - Overview

Secure Management of Information across multiple Stakeholders

- CIP-ICT-PSP.2009.7.1: A European infrastructure for secure information management
- Duration: 30 months
  Start date: March 2010
  End date: August 2012
- Cost: 4,034,498.00 € Funding: 2,017,247.00 €
- Consortium: 9 partners from 6 countries.
- Project coordinator: Atos Origin (Spain)

SEMIRAMIS

- The actual context:
  - The efficient implementation of “cross border“ processes will become a critical issue in Europe
  - Such processes comprise public institutions, citizens and private institutions
  - The demand will increase continuously and brings up the following challenges
    - Interoperability which would result in unproductive delay and further burdens
    - User friendliness which allocate too much “resources“
    - Efficiency , which introduce cost higher than needed

SEMIRAMIS

The aim of SEMIRAMIS

- **The main aim of SEMIRAMIS is to provide an infrastructure for e-services, which minimizes the administrative burdens of such processes with a special focus on**
  - **Scalability (in a European context)**
  - **Interoperability (in an European context)**
  - **Security respecting individual national policies**
  - **Trust in a heterogeneous Europe**
- ***The key qualities of the infrastructure include***
  - Ensuring data privacy, confidentiality and trust according to the applicable regulations
  - Managing access to the data, strictly on a *need-to-know* basis for the user and the e-services being accessed
  - Providing open interfaces to allow different organizations, whether private or public
  - Defining a modular and customizable architecture, whose components can be deployed at different locations

SEMIRAMIS

Means of validation

- **SEMIRAMIS has three generic scenarios validating the concept which are:**
  - **eDoc for citizens**
  - **Roaming Students**
  - **Tax Inspector**

Which have a similar scope in terms of diversity and are generic enough for a generalized solution

SEMIRAMIS

- **Scenario "e-DOC Services for Citizens"** A European Citizen decides to move for a short period of time to another country. As a consequence of a job offer, he will try to stay in the country more time than initially planned.
- Several needs may arise, which can be solved by SEMIRAMIS:
  - The foreign company asks for the Citizen's previous experience which involves the communication of personal data.
  - He will require a temporary housing and healthcare facility so he may need a certificate of residence.
  - If he is travelling with kids, they would also need access to public education facilities. Family membership and previous scholar information is required.
  - To stay in contact with the family in the country of origin, he needs access to local TELCO services.
- The Citizen's consent is needed before releasing personal information.
- Several ways of citizen authentication are considered such as eID authentication.

SEMIRAMIS

- **Scenario "Roaming Student"** A European student moves to another country to continue his studies in another European university.
- Several aspects of the roaming student life are considered:
  - During the matriculation process the foreign university may require academic information about the student from his home university.
  - The student may request some TELCO services in the foreign country. The new contracted services should have the same profile or equivalent to the services at HT.
  - The student may receive economic aid from the government. The student should prove that he is enrolled at the university.
- Policies are defined by the student to control personal information releasing.
- Interoperability issues for the academic information format are addressed.
- eduGAIN/eduroam are considered in this scenario for interaction between universities.

SEMIRAMIS

Thank you!

For more information please visit:
http://www.semiramis-cip.eu/

Contact us:
Project Coordinator – Charles Bastos Rodriguez:
charles.bastos@atosorigin.com
Dissemination manager – Véronique Pevtschin:
veronique.pevtschin@eng.it

Where do we go from here?

- This is a networking session!
- So: who else in the room is active in related projects?
- What are future research challenges? (Think of FP8 …)