PrimeLife

Reference Group Meeting

March 23 – 24, 2009

Trusted content &
privacy throughout life

SEVENTH FRAMEWORK PROGRAMME

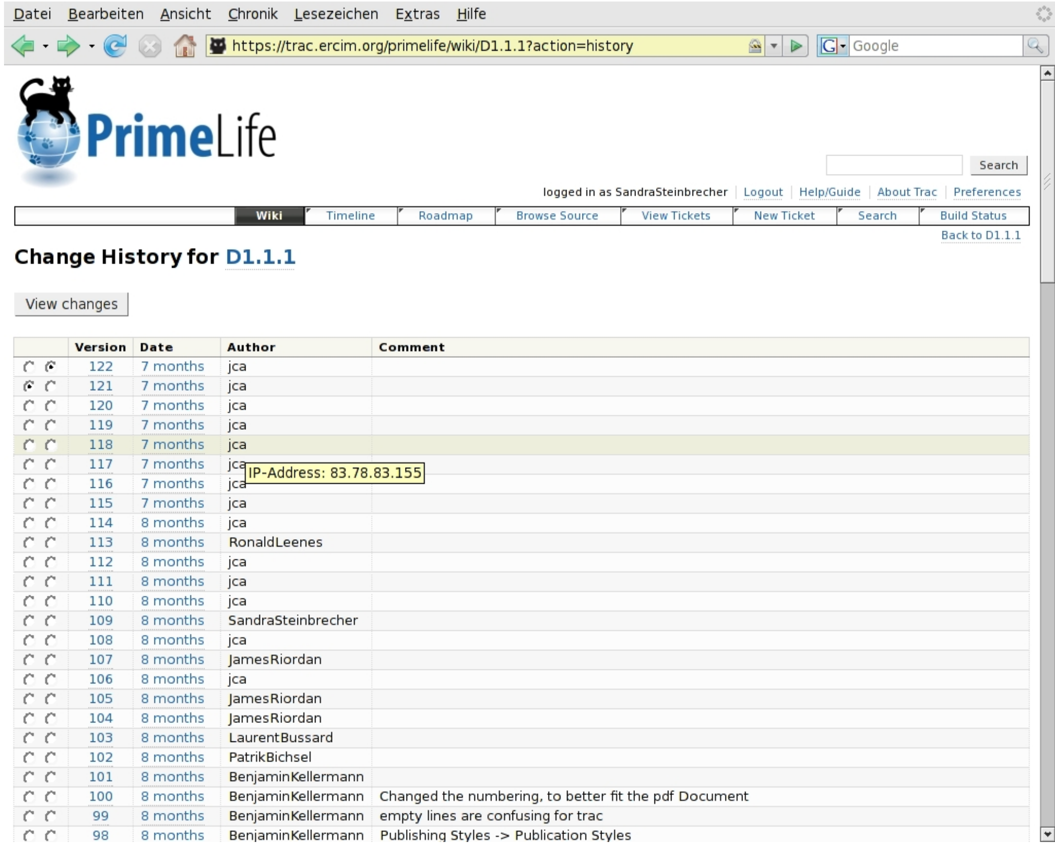
A research project funded by the
European Commission’s
7th Framework Programme

KATHOLIEKE UNIVERSITEIT LEUVEN · GOETHE UNIVERSITÄT FRANKFURT AM MAIN · cureCED · Microsoft Innovation Center Europe · W3C® · IBM · SAP®

How to trust in digital content

- changing quickly
- many authors
- large amount of information

What computational support is realistic/feasible for helping humans to assess trustworthiness?


Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
https://trac.ercim.org/primelife/wiki/D1.1.1?action=history
Google
PrimeLife
Search
logged in as SandraSteinbrecher | Logout | Help/Guide | About Trac | Preferences
Wiki | Timeline | Roadmap | Browse Source | View Tickets | New Ticket | Search | Build Status
Back to D1.1.1
View changes

Change History for D1.1.1

	Version	Date	Author	Comment
○ ●	122	7 months	jca	
● ○	121	7 months	jca	
○ ○	120	7 months	jca	
○ ○	119	7 months	jca	
○ ○	118	7 months	jca	
○ ○	117	7 months	jca	
○ ○	116	7 months	jca	
○ ○	115	7 months	jca	
○ ○	114	8 months	jca	
○ ○	113	8 months	RonaldLeenes	
○ ○	112	8 months	jca	
○ ○	111	8 months	jca	
○ ○	110	8 months	jca	
○ ○	109	8 months	SandraSteinbrecher	
○ ○	108	8 months	jca	
○ ○	107	8 months	JamesRiordan	
○ ○	106	8 months	jca	
○ ○	105	8 months	JamesRiordan	
○ ○	104	8 months	JamesRiordan	
○ ○	103	8 months	LaurentBussard	
○ ○	102	8 months	PatrikBichsel	
○ ○	101	8 months	BenjaminKellermann	
○ ○	100	8 months	BenjaminKellermann	Changed the numbering, to better fit the pdf Document
○ ○	99	8 months	BenjaminKellermann	empty lines are confusing for trac
○ ○	98	8 months	BenjaminKellermann	Publishing Styles -> Publication Styles

IP-Address: 83.78.83.155

resulting scope: trustworthiness as a multilayered concern (integrity, binding, context, accuracy)

only some of these layers allow automation

Solutions to problems

Humans typically assess

- secondary information about the (primary) information
- who has provided this information

resulting goal:
software tool with concise/relevant/reliable metadata

- certification of authors with knowledge in a certain field by designated authorities (e.g. academic degrees by universities)
- giving readers the possibility to rate authors and content
- calculating reputation of authors and content

hierarchic

grassroot

Reputation systems

+ can collect estimation of content by certain raters at a certain point in time (that hopefully will predict future estimation).

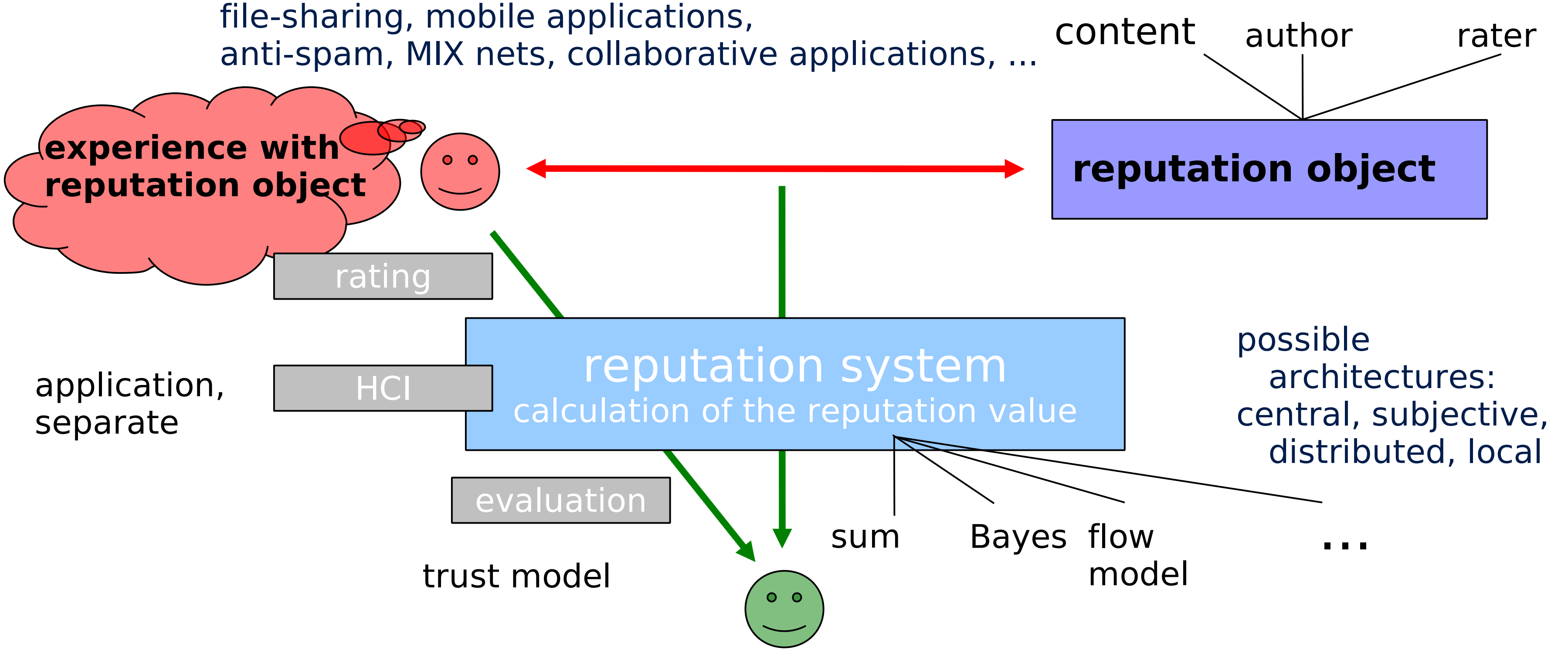
+ can reach effects of social networks: control (by raters) and learning (by future readers).

- do not prevent any reader from making bad experiences.

- do not make technical measures that help to reach accountability (certification and PKI) obsolete.

Design options

application fields: electronic marketplaces,
file-sharing, mobile applications,
anti-spam, MIX nets, collaborative applications, ...



content author rater

reputation object

experience with reputation object

rating

application, separate

HCI

reputation system

calculation of the reputation value

possible architectures:
central, subjective,
distributed, local

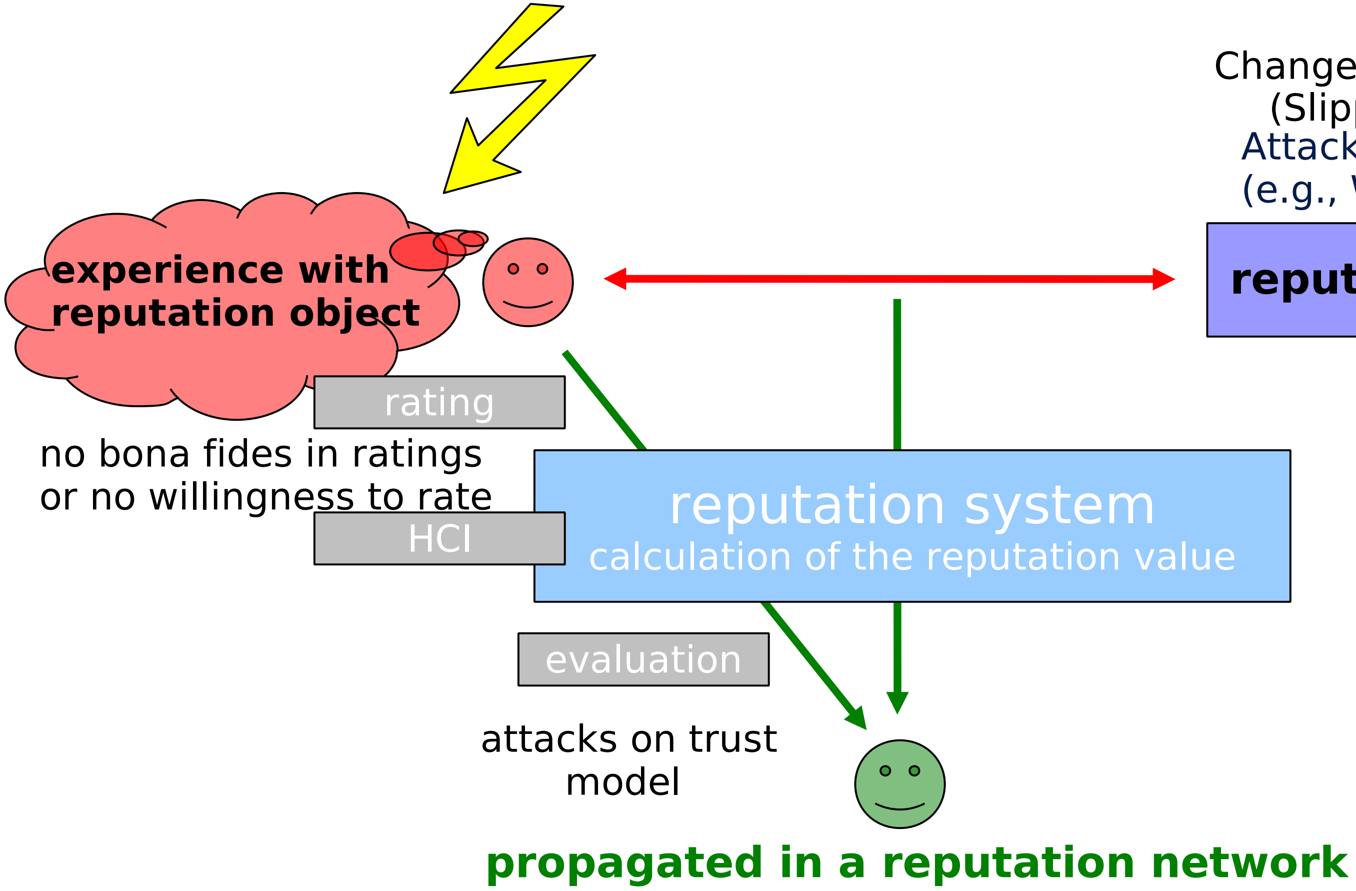
evaluation

trust model

sum Bayes flow model ...

propagated in a reputation network

Threats to consider


experience with reputation object
rating
HCI
reputation system
calculation of the reputation value
evaluation
reputation object
propagated in a reputation network

Changes of the reputation object (Slipping, Milking)

Attacks on identity (e.g., Whitewashing, Sybil)

no bona fides in ratings or no willingness to rate

Attacks on calculation of reputation value

attacks on trust model

Privacy problems (for raters and reputation objects)

What helps: instead of trial and error requirements analysis before system design

Design requirements and options

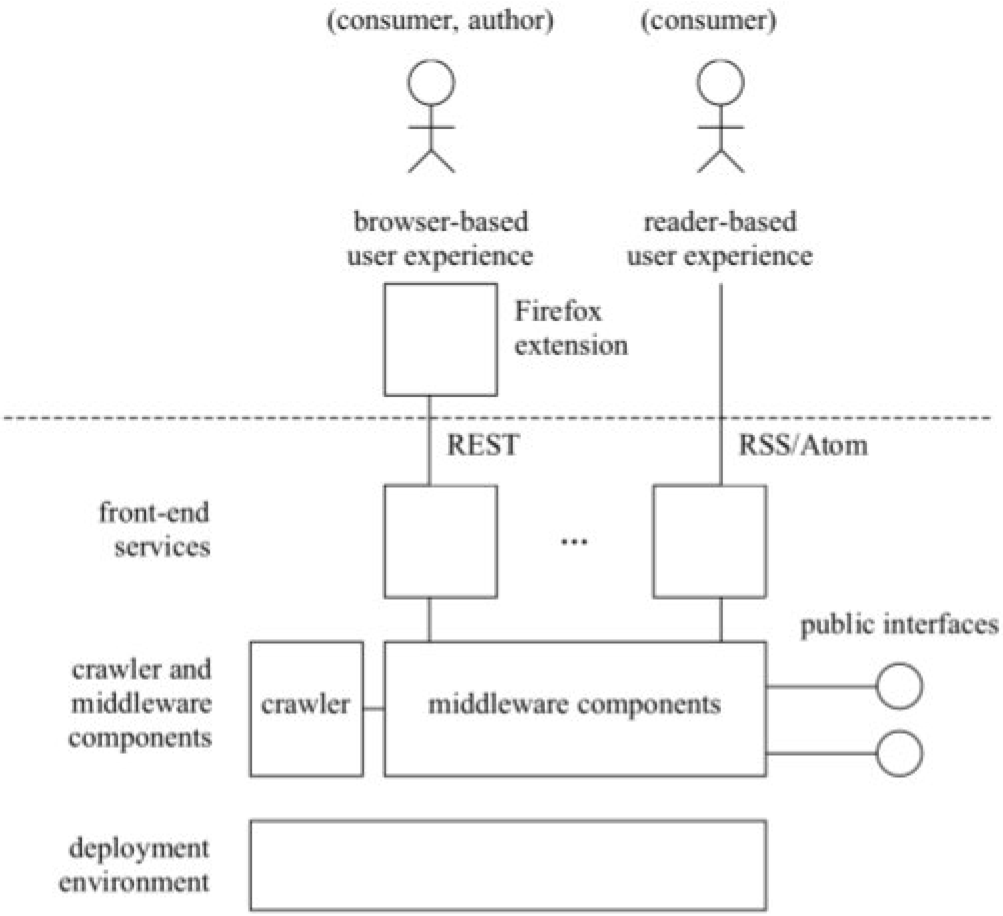
Initially:

- how to calculate the reputation of content
- how to calculate the reputation of authors
- how to calculate the reputation of raters

Dynamic aspects:

- changing content
- changing authors
- changing reputation

1st Focal Prototype: Blog - High-level architecture

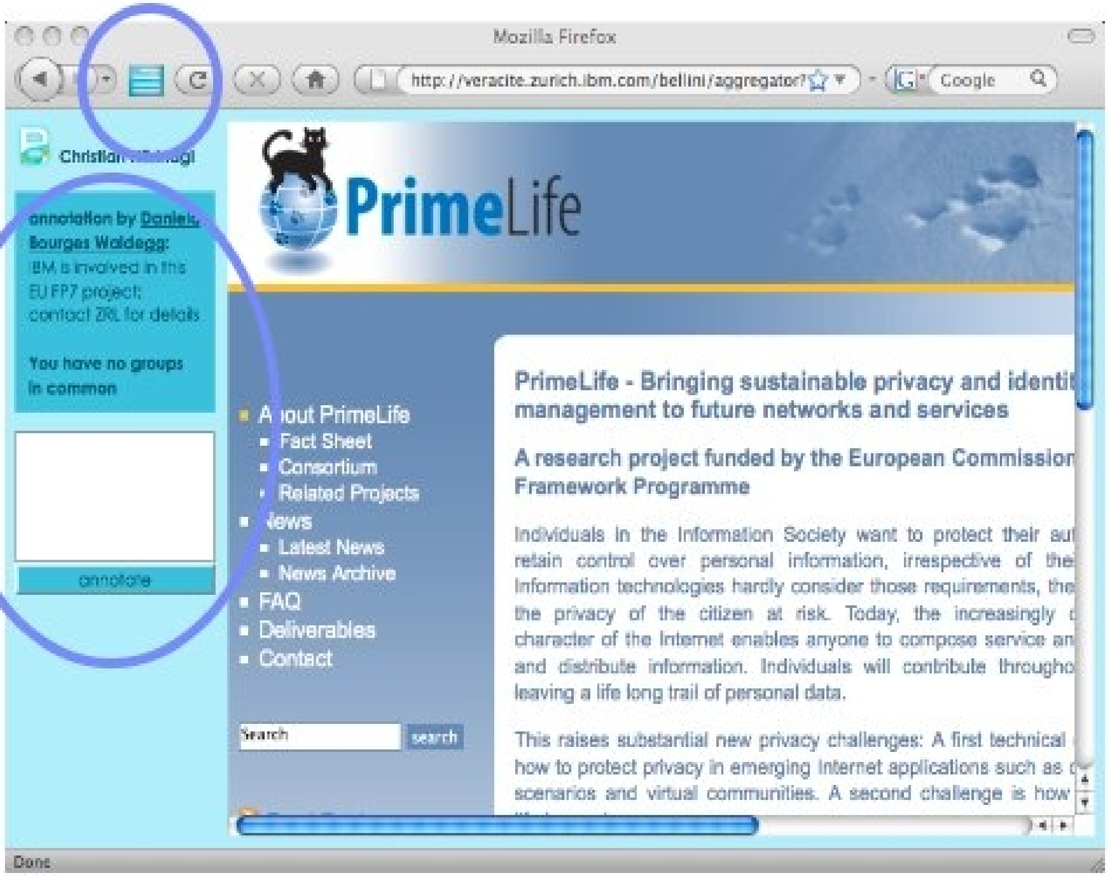


includes interfaces for alternative integrations:
identity
reputation
ontologies
secure binding
repository
trust valuation

(more details in D1.1.2 report)

1st Focal Prototype: Blog - User experience

- browser-based user experience (with Firefox extension)
  - specific new button indicates presence of annotations
  - provides access to further/summary information about them
- feed-reader-based user experience available as well



annotation by Daniela Bourges Waldegg: IBM is involved in this EU FP7 project: contact ZRL for details

You have no groups in common

PrimeLife - Bringing sustainable privacy and identit management to future networks and services

A research project funded by the European Commission Framework Programme

Individuals in the Information Society want to protect their au retain control over personal information, irrespective of the Information technologies hardly consider those requirements, the the privacy of the citizen at risk. Today, the increasingly character of the Internet enables anyone to compose service an and distribute information. Individuals will contribute througho leaving a life long trail of personal data.

This raises substantial new privacy challenges: A first technical how to protect privacy in emerging Internet applications such as scenarios and virtual communities. A second challenge is how

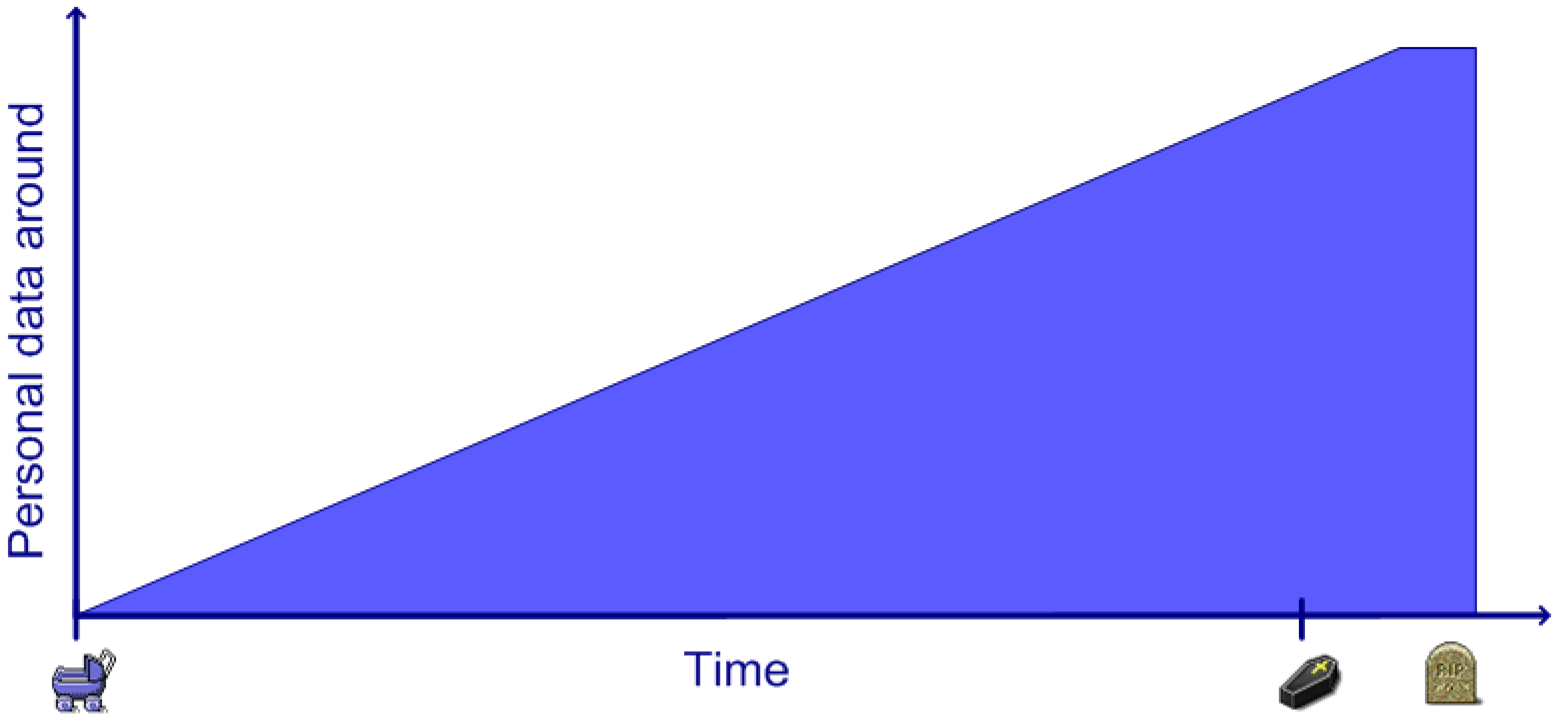
1st Focal Prototype: Blog - Some technical contributions

- BURLs (bound URLs)
  - versioning mechanism for referring to specific instance of URL-addressable content (URL including content digest and more)
- normalization
  - heuristic means e.g. to make sure that signers see exactly what they commit to (no hidden content)
- semantic signatures
  - digital signatures combined with ontology-based terms that tell their scope, resulting obligations, etc.
- privacy-friendly protocol designs
  - e.g. multiple inquiries to meta-data repository reveal no information about a user’s browse path/history to server

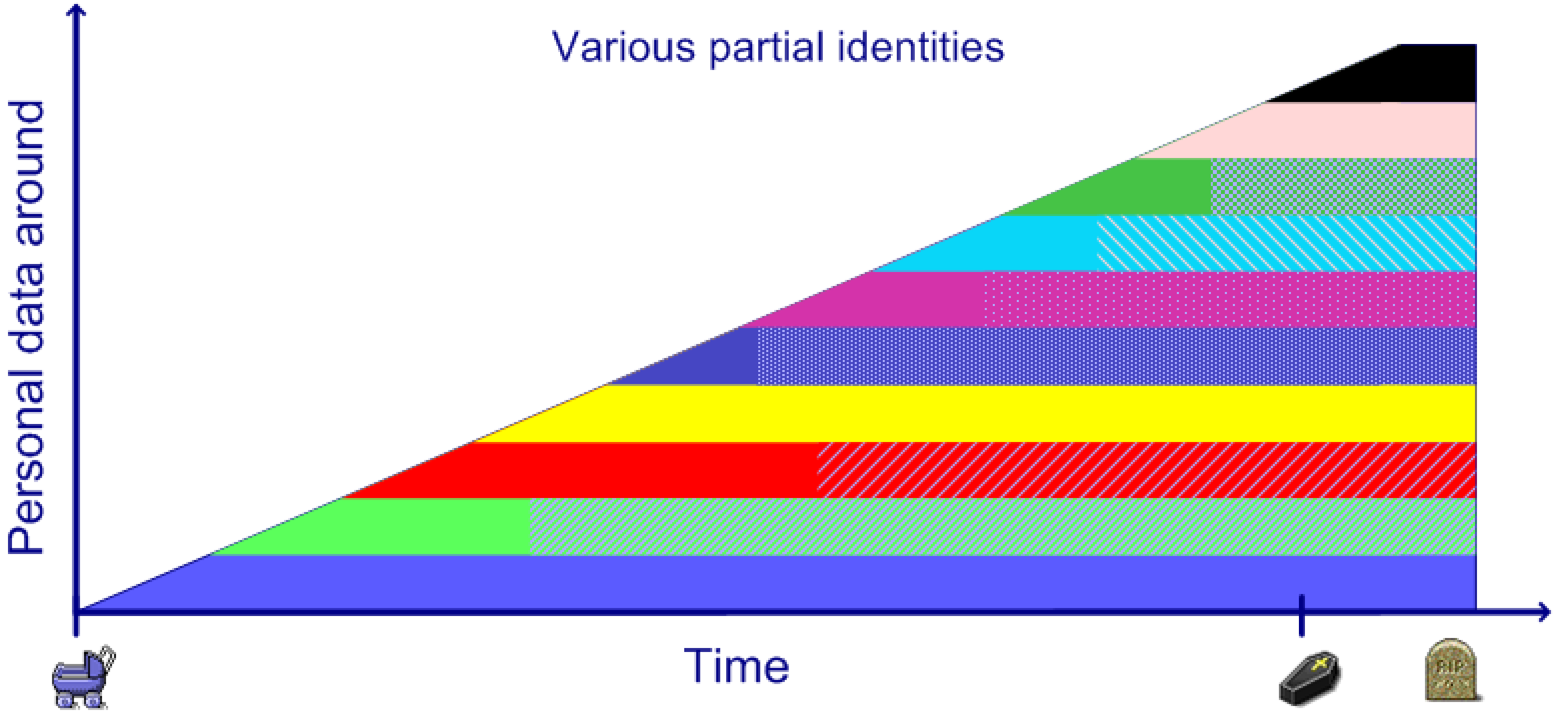
Prototypes – lessons learned and what to do next

- deployed on corporate intranet for several months
  - encouraging qualitative feedback (internal and external)
  - limited quantitative feedback (download of extension, use of tool)
- this and other evidence show for the next prototype (a wiki)
  - consider author, content and rater reputation
    - make a feedback loop and let the user decide
    - but do not bother users with all details
  - implement incentives to receive meaningful participation
    - monetary payments as incentives (e.g. anonymous e-cash)
    - other valuations as incentives (e.g. reputations)
    - side-effects as incentives (e.g. games with a purpose)
    - privacy protection as incentives (think: protect sources)
  - privacy as addressed by PrimeLife also highly relevant to several of these enabling categories

Extending trust and privacy throughout life – privacy (I)



Extending trust and privacy throughout life – privacy (II)



Extending trust and privacy throughout life

- trust evolving over time vs. basic trust
- system trust vs. inter-personal trust
- trust vs. privacy
- short-term vs. long-term effects
- constant vs. changing abilities/behaviour of individuals
- context-specific vs. context-spanning

IDM

covering the full lifespan

covering all stages of life

covering all areas of life

IdM covering all areas of life

- formal areas (I have to participate in):
  - government
  - education
  - work
  - health care
  - ...
- informal areas (I might choose to participate in – or others decide for me):
  - family
  - friends
  - shopping
  - sport
  - ...

Technological, social, legal, …. mechanisms

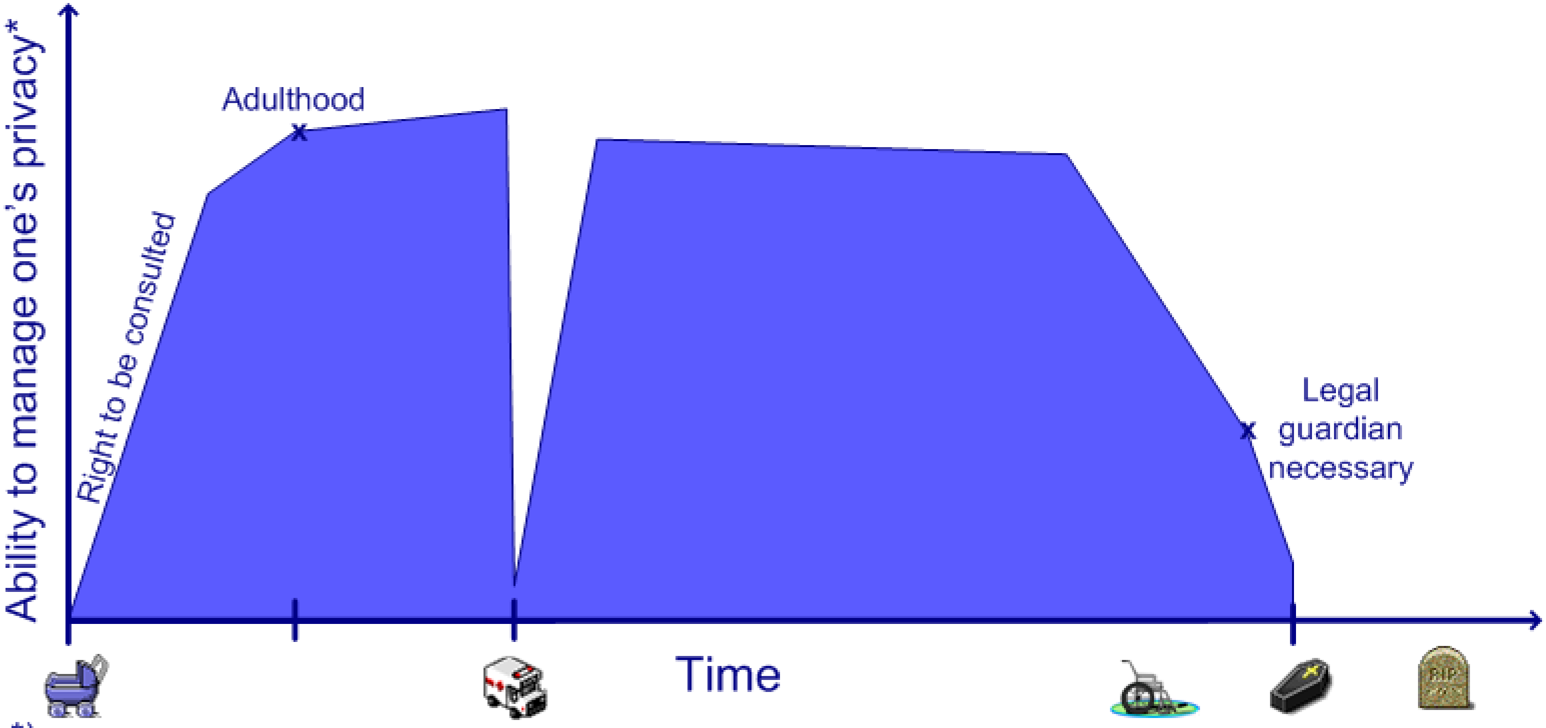
What we have:

- technological mechanisms for user-controlled privacy
  - handling of partial identities
  - data minimisation
  - enforceable rules for data processing
  - transparency functionality

What we need to develop/adapt:

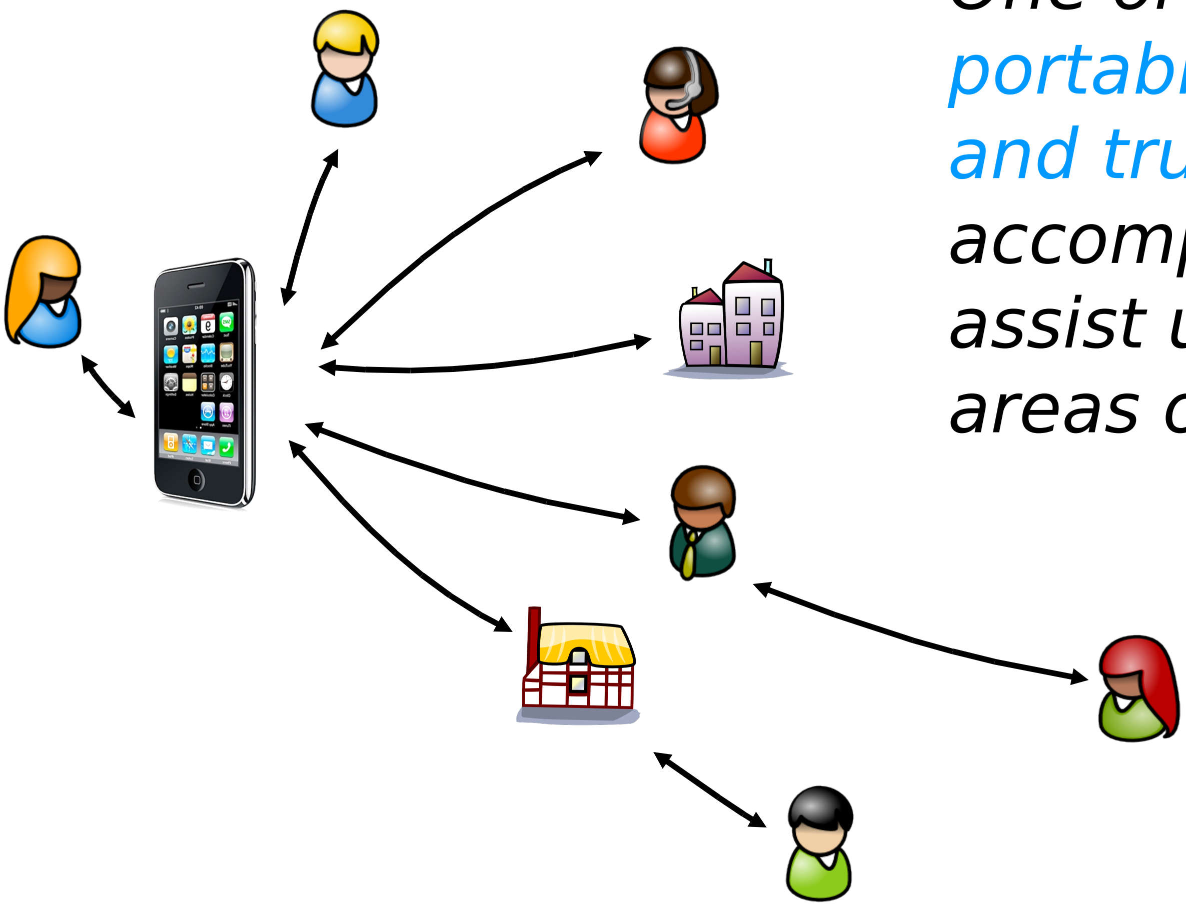
- mechanisms for covering all areas of life
- mechanisms for covering all stages of life
- mechanisms for covering the full lifespan

Ability to manage one's privacy



*)
- Ability to understand
- Ability to act accordingly
- Ability to use required (technical) means

Trusted device as basis for mechanisms covering all areas of life



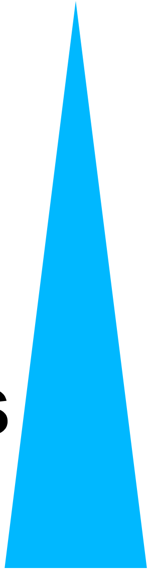
One or more ***portable, personal, and trusted devices*** *accompany and assist users in all areas of life.*

But does the trusted device as mechanism cover the full lifetime?

What happens if …?

desired response

- **the device is lost or stolen**
  - “In the UK, one mobile phone is stolen every 12 seconds.”
- **the device owner deceases**



device not useful at all (except modest incentive to return)

heirs-at-law should be able to extract selected content

beneath: technology development

Mechanism – Conditional Recovery

- **Let users define "post-mortem" access rights**
  - for local objects *and* reference to remote resources (key-chain)
  - RQ: Find adequate trade-off between expressiveness and complexity
  - RQ: Protection goals for those rights (and their enforceability)
  - Consider integration in PE-IMS frameworks
- **Distributed backup with two recovery modes**
  - 1: Complete restoration if owner is unambiguously present, alive, and consents with the recovery
  - 2: Distribution of "digital estate" according to the "post mortem" access rights

Trust in “digital estate“

- **Authenticity of “digital estate”**
  - digital signatures verifiable (long) after the signer’s death

- **Integrity of division of “digital estate”**
  - integrity of the information about one’s death (digital certificate of one’s death)
  - integrity of complete set of post mortem policies (if possible, while maintaining confidentiality of their contents)
  - all-or-nothing (ideally: all) settlement despite possible unavailability of some heirs

Does an infrastructure exist for a full lifetime?

Straight technical solutions to the above problems exist, if the state takes a role as trusted third party. Can we do otherwise?

- **Community approach to “digital estate”**
  - secret sharing as a mechanism to ensure recovery
  - integrate distribution of secrets in social networking systems
  - RQ: Re-use mechanisms of trust computation
  - RQ: Consistency or diversity between distribution of shares across multiple partial identities

But does the trusted device as mechanism cover all stages of life? (I)

Are current solutions still adequate for ...?

- very young people, especially children
- parents assisting children
- people with handicaps
- old people
- old people needing assistance
- people assisting others in interacting

But does the trusted device as mechanism cover all stages of life? (II)

Are current solutions still adequate if …?

- **some users own more than one device**
  - Each device holds information belonging to various partial identities, possibly overlapping between devices.
- **some devices belong to more than one user**
  - Example: digital photo album shared in the family or among friends
- **no personal trusted devices exist**
  - Vision of ambient intelligence: devices deployed in the environment

Resulting questions

- Do we address the right areas of life?
- Would a demonstrator for digital heritage be the right one as the third year's focal prototype?
- Or do you have better ideas?

- How can people make the right decisions for their privacy?
- Is "consent" a sufficient mechanism?
- Which alternatives?

Thank You!