PrimeLife

Reference Group Meeting

March 23 – 24, 2009

Policies

Collecting input

A1
Social networks,
wikis, blogs

A2
Crypto

A4
User
interfaces
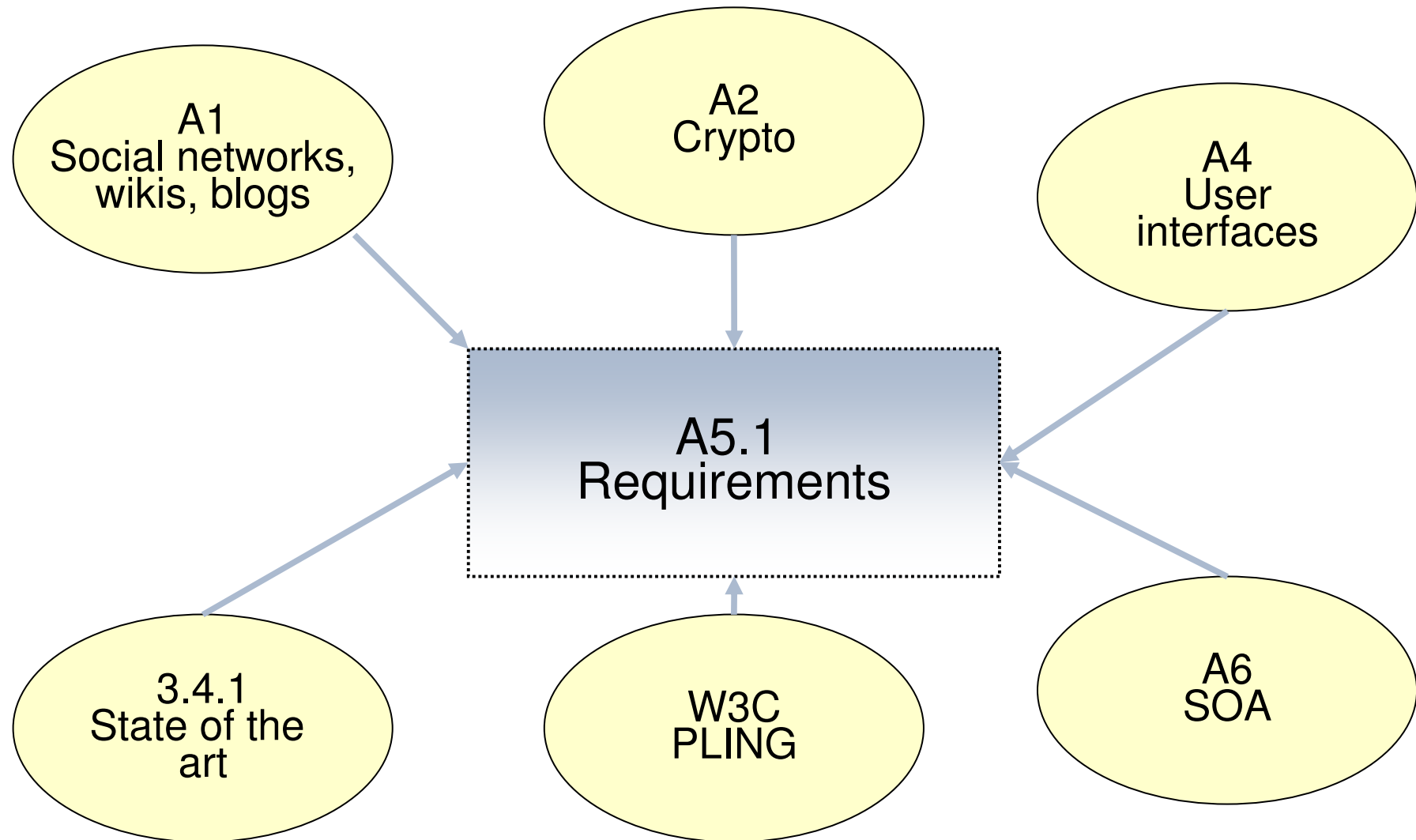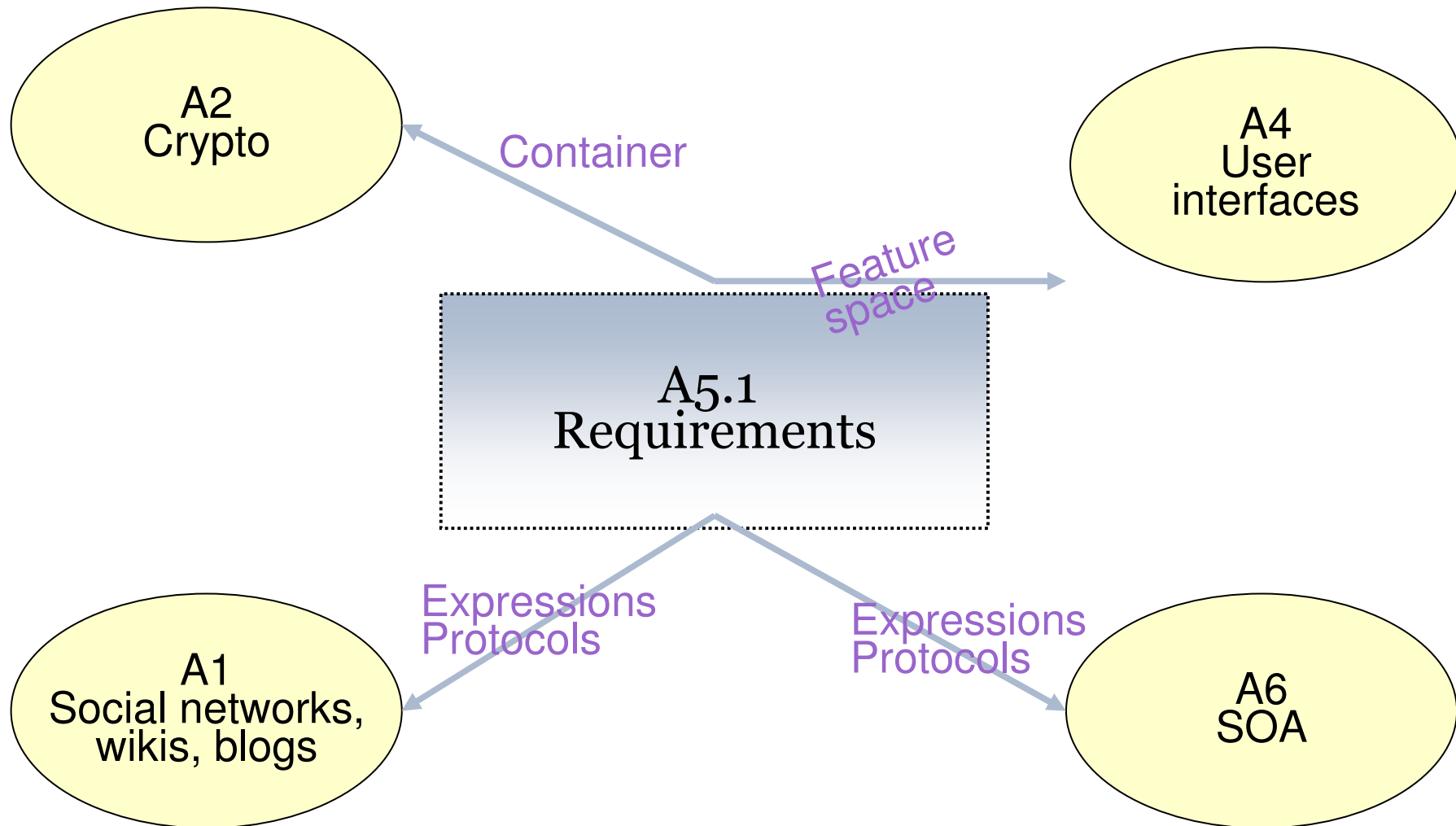
A5.1
Requirements

3.4.1
State of the
art

W3C
PLING

A6
SOA

PrimeLife Reference Group Meeting

March 23-24, 2009

Providing backbone

A2
Crypto

Container

A4
User
interfaces

Feature
space

A5.1
Requirements

Expressions
Protocols

Expressions
Protocols

A1
Social networks,
wikis, blogs

A6
SOA

WP5.3: Policy implementation

A5.1
Requirements

D3.4.1
Available
Languages

A6
Policy
Composition

XACML +Extensions
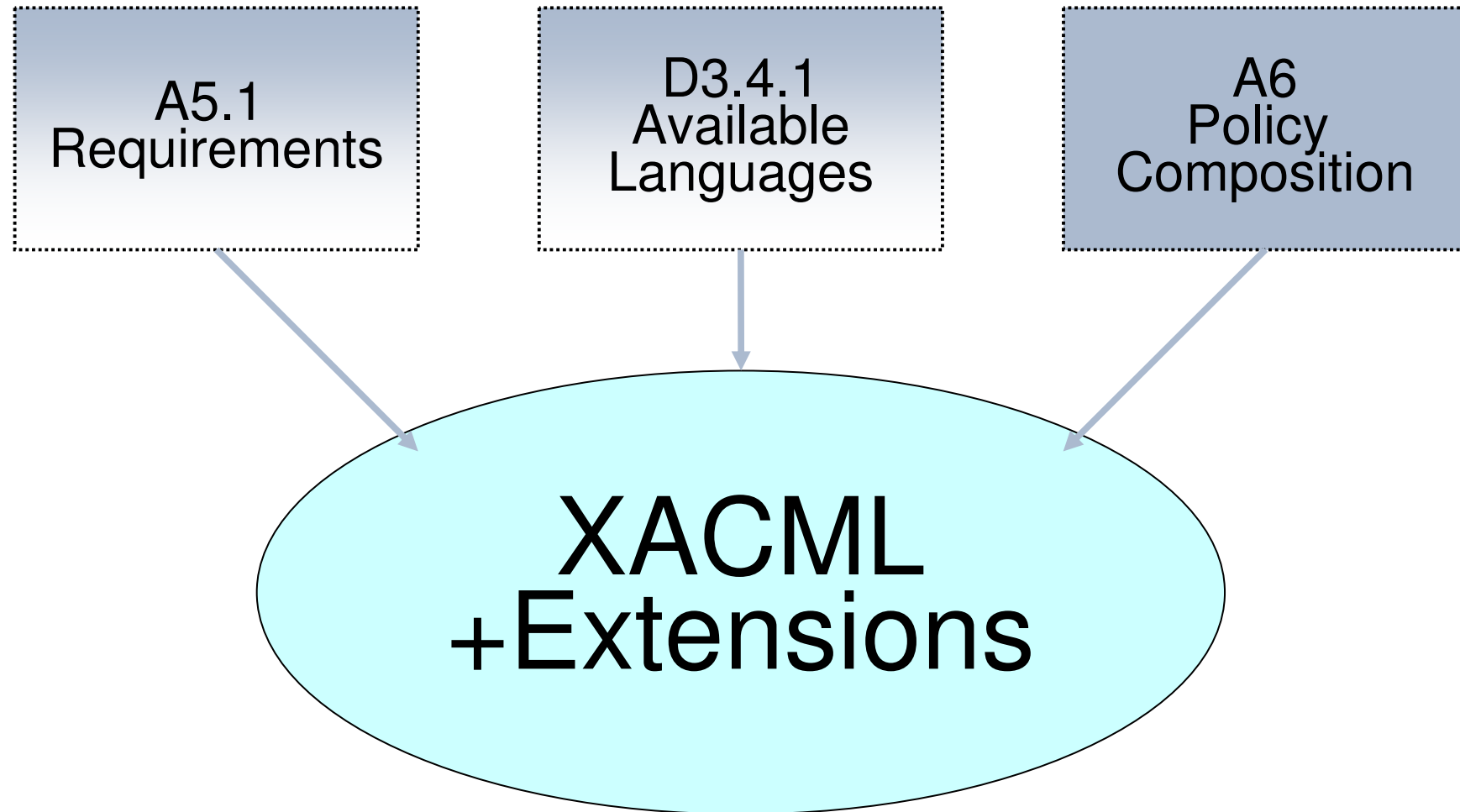
Feature forecast

- Privacy-friendly access control

- Trust expressions

- Sticky policies

- Data handling

- Service composition

PrimeLife Reference Group Meeting **March 23-24, 2009**

WP5.2: Policy research

Topics include:

- Access control language for anonymous credentials
- Access control versus data handling policies
- Policy composition
- Graph-based permission composition
- Legal vs technical policies

Goals:

- Scientific output
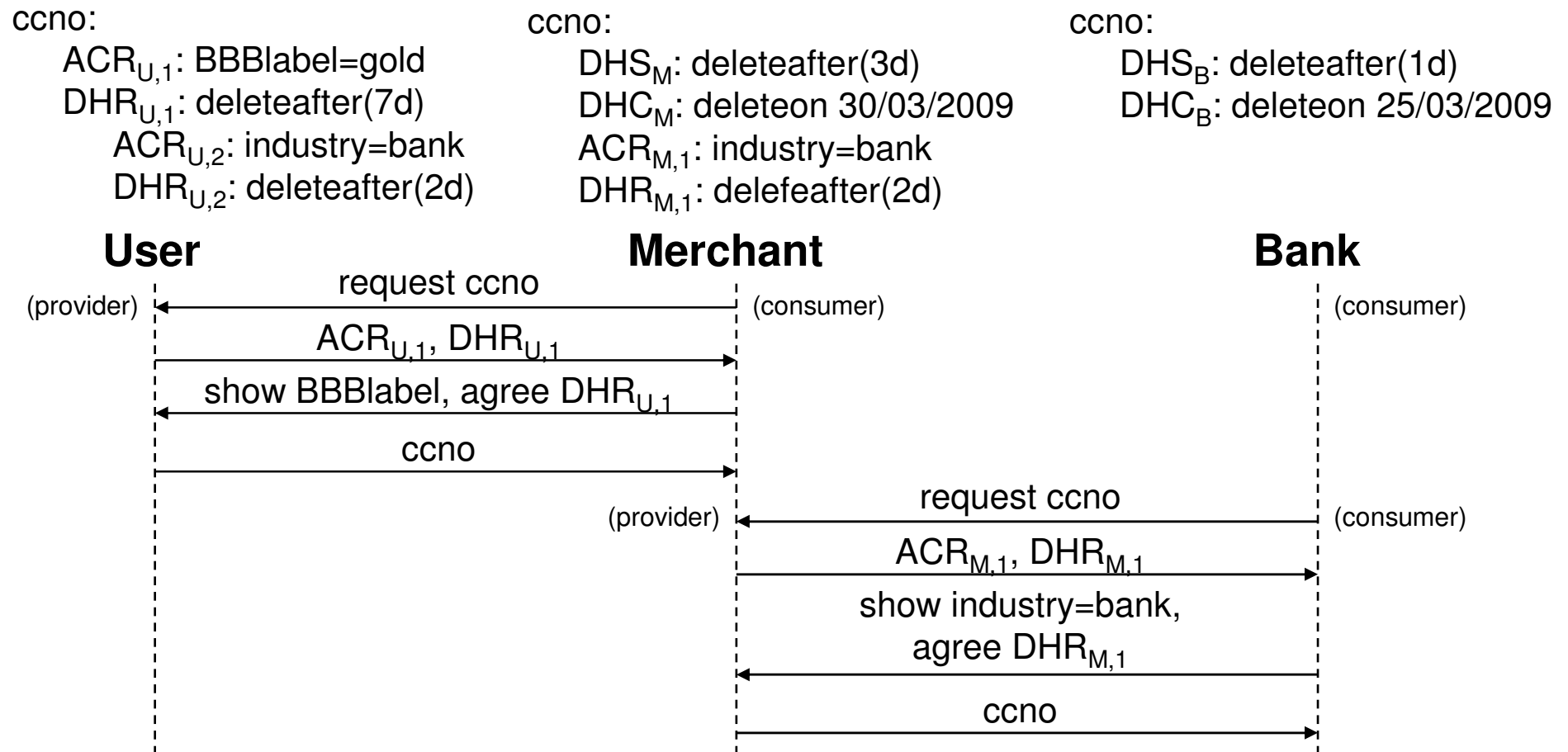- Feed design & implementation of WP5.3

PrimeLife Reference Group Meeting   March 23-24, 2009

Privacy-friendly access control

- **possess** pp::Passport **issued-by** *http://admin.ch*
  possess rp::ResidencePermit **issued-by** *http://zurich.ch*
  possess cc::CreditCard issued-by cci
  reveal cc.number
  reveal rp.address **to** *http://ups.com* **for** 'shipment'
  where (cci = *http://visa.com* ∨ cci = *http://amex.com*) ∧
          (pp.bearer = cc. bearer = rp. bearer) ∧
          (year(today) – year(pp.dateOfBirth)) > 18

- **possess** money::Spendable **issued-by** *http://ubs.ch*
  spend k **units-of** money **to** *http://a123.accounts.ubs.ch*
  where (time() < 8am ∧ k = 1) ∨ (time() ≥ 8am ∧ k = 2)

PrimeLife Reference Group Meeting

Access control vs. data handling

ccno:
   $ACR_{U,1}$: BBBlabel=gold
   $DHR_{U,1}$: deleteafter(7d)
     $ACR_{U,2}$: industry=bank
     $DHR_{U,2}$: deleteafter(2d)

ccno:
   DHS_M: deleteafter(3d)
   DHC_M: deleteon 30/03/2009
   $ACR_{M,1}$: industry=bank
   $DHR_{M,1}$: delefeafter(2d)

ccno:
   DHS_B: deleteafter(1d)
   DHC_B: deleteon 25/03/2009

User   **Merchant**   **Bank**

(provider)   request ccno   (consumer)   (consumer)

$ACR_{U,1}$, $DHR_{U,1}$

show BBBlabel, agree $DHR_{U,1}$

ccno

(provider)   request ccno   (consumer)

$ACR_{M,1}$, $DHR_{M,1}$

show industry=bank, agree $DHR_{M,1}$

ccno

ACR = Access control requirements
DHR = Data handling requirements
DHS = Data handling support
DHC = Data handling contract

Policy matching & composition

User → Service

john@abc.com:
  purpose = contact, statistics
  retention < 6 months
  forward to PrivLabel>silver

matching

email:
  purpose = contact
  retention = 3 months
  forward to PrivLabel=gold

Service A

$Policy_A$

User → Mash-up

Preferences

matching

$Policy_{A,B,C}$

Service B

$Policy_B$

Service C

composition

$Policy_C$

PrimeLife Reference Group Meeting

March 23-24, 2009
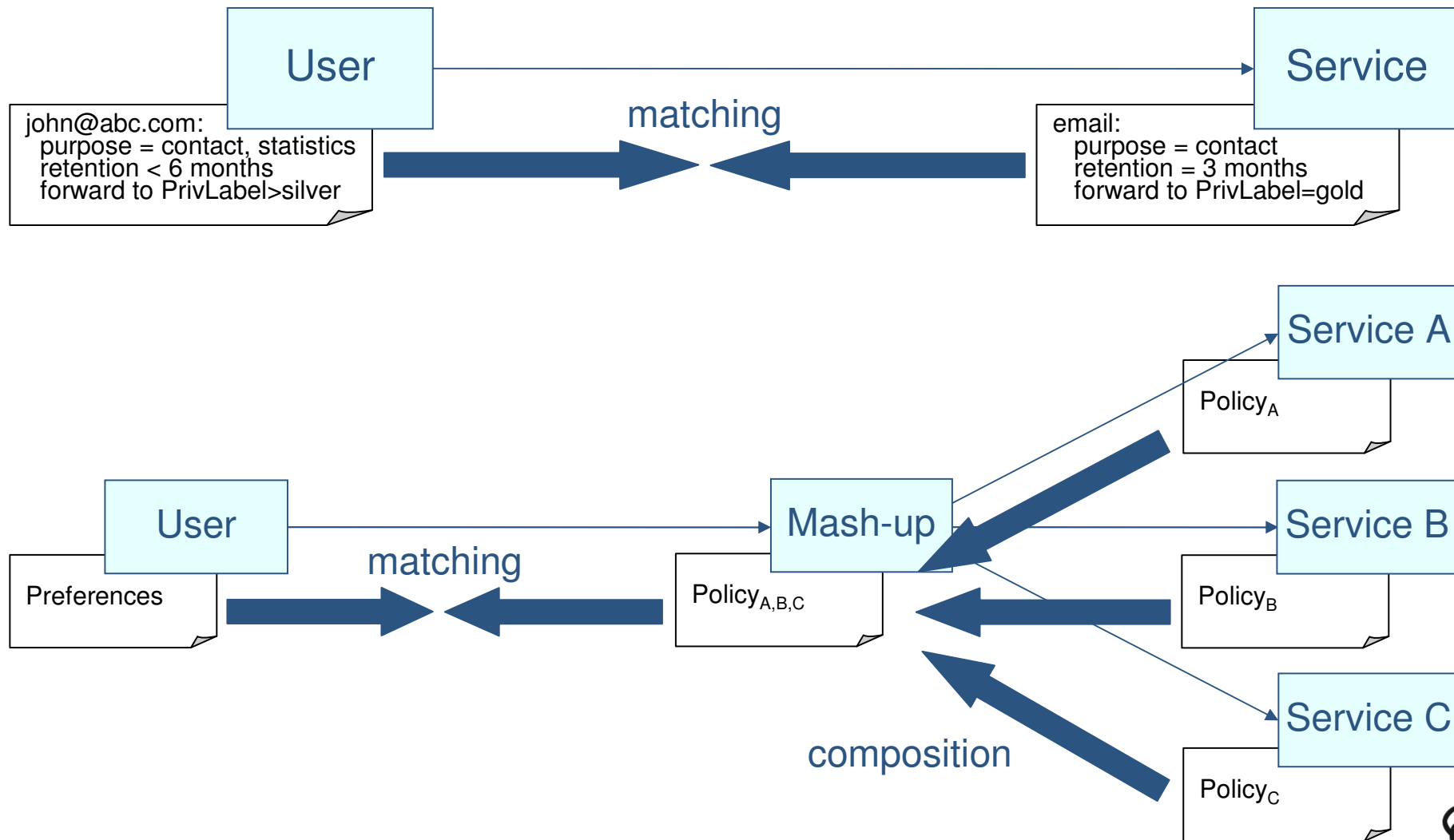
Questions

- Is XACML + Extensions the right choice?

- Where to put most of the effort?

- What are our chances for real market impact?

- Does data handling need rules; is RIF a good choice?

- Can we stick Rules into the XACML <obligation> element?

PrimeLife Reference Group Meeting **March 23-24, 2009**

Standardization

- ## W3C PLING

- ## ISO/IEC

  - JTC 1/SC 27/WG 5: "Identity management and privacy technologies"

    - ISO/IEC 24760: "Identity management framework"

    - ISO/IEC 29100: "Privacy framework"

    - ISO/IEC 29101: "Privacy reference architecture"

PrimeLife's Aproach to Open Source

Goal: Make as much available as possible

- Mature Components
  - Work on documentation, usability, code quality
  - Licenses EPL where possible, specific licenses otherwise
  - PRIME components
    - Data Track, ID manager, Identity Mixer
  - Possible PL components
    - Policy engines, HCI components, Wiki components

- Demonstrators and Prototypes
  - Provide basically on as is basis
  - E.g., Activity 1 Demonstrators and Experiements

PrimeLife's Aproach to Open Source

Analysis of Open Source Landscape (D1.1.1)

- Many relevant initiatives (OS and Standards)
  - Higgins, Open ID, Liberty, WS-Federation etc
  - Policies & Rules : XACML, P3P, etc.
  - Authenticiation: X.509, XML Sigs,

- Where to Contribute?
  - Many initiatives, no clear winner
  - Provide our components as standalone
  - Rather spend resources on documentation and examples than interaction with specific initiatives
  - But close to standards when ever possible

PrimeLife Outreach Target Groups

other projects

Cooperation WS

research communities

Summer School

law enforcement

privacy commissioners

IT security organisations

policy makers, parliamentarians

Workshop for PrimeLife Reference Group

Workshop Series

Cooperation WS

system developers

standardisation bodies
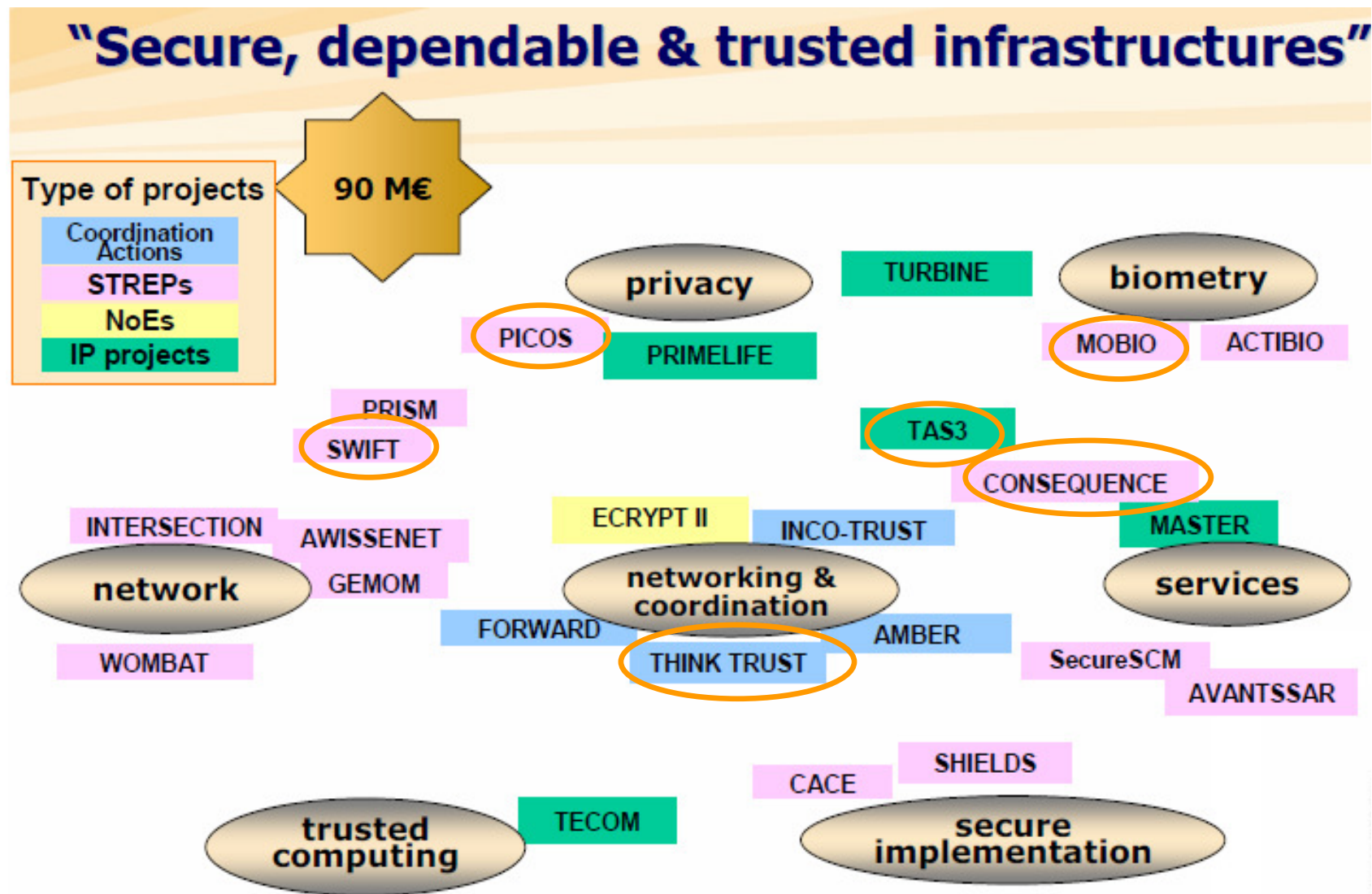
Standardisation WS

Networking

media / journalists

WS for journalists

Open Source

Standardisation

business, industry associations

data controllers

user & consumer organisations

individuals

Contact with other projects

- Daidalos II
- SWIFT
- TAS3
- PICOS
- MOBIO
- MASTER
- AVANTSSAR
- Stork

- CERP
- NESSI
- Think-Trust
- EnCoRe
- RESERVOIR
- EuroPriSe