PrimeLife Reference Group Meeting
March 23 – 24, 2009

Policies

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

March 23-24, 2009 PrimeLife Reference Group Meeting
Providing backbone

A2 Crypto

A4 User interfaces

A5.1 Requirements

A1 Social networks, wikis, blogs

A6 SOA

Container

Feature space

Expressions Protocols

Expressions Protocols
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
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
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’

  (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)
Access control vs. data handling

User

(request ccno)

ACR\textsubscript{U,1}, DHR\textsubscript{U,1}

show BBBlabel, agree DHR\textsubscript{U,1}

ccno

Merchant

(request ccno)

ACR\textsubscript{M,1}, DHR\textsubscript{M,1}

show industry=bank, agree DHR\textsubscript{M,1}

ccno

Bank

(request ccno)

ACR\textsubscript{M,1}, DHR\textsubscript{M,1}

show industry=bank, agree DHR\textsubscript{M,1}

ccno

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

PrimeLife Reference Group Meeting
March 23-24, 2009
Policy matching & composition

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

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

Service A
Policy_A

Service B
Policy_B

Service C
Policy_C

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

Standardization

A research project funded by the European Commission’s 7th Framework Programme
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”
Open Source Approach
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.
  - Authentication: 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 Reference Group Meeting
March 23 – 24, 2009

Outreach

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

Target Groups

Cooperation WS

Summer School

Workshop for PrimeLife Reference Group

Workshop Series

Networking

Open Source

WS for journalists

Standardisation

Standardisation bodies

System developers

Cooperation WS

Business, industry associations

data controllers

User & consumer organisations

Media / journalists

Law enforcement

Privacy commissioners

IT security organisations

Policy makers, parliamentarians

Individuals
Workshops / contact with other projects: FP7

“Secure, dependable & trusted infrastructures”

Type of projects
- Coordination Actions
- STREPs
- NoEs
- IP projects

90 M€

Network
- PRISM
- SWIFT

Privacy
- PICOS
- PRIMELIFE

TURBINE
- MOBIO
- ACTIBIO

Biometry
- TAS3

TAS3
- CONSEQUENCE

Networking & coordination
- INCO-TRUST
- AMBER
- SecureSCM

Forward
- SHIELDs

Think Trust

Secure computing
- TECOM

Secure implementation
- CACE

Master
- AVANTSSAR

Services
Contact with other projects

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

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