Can Access Control be Extended to Deal with Data Handling in Privacy Scenarios?

Laurent Bussard and Moritz Y. Becker
Microsoft (EMIC and MSRC)

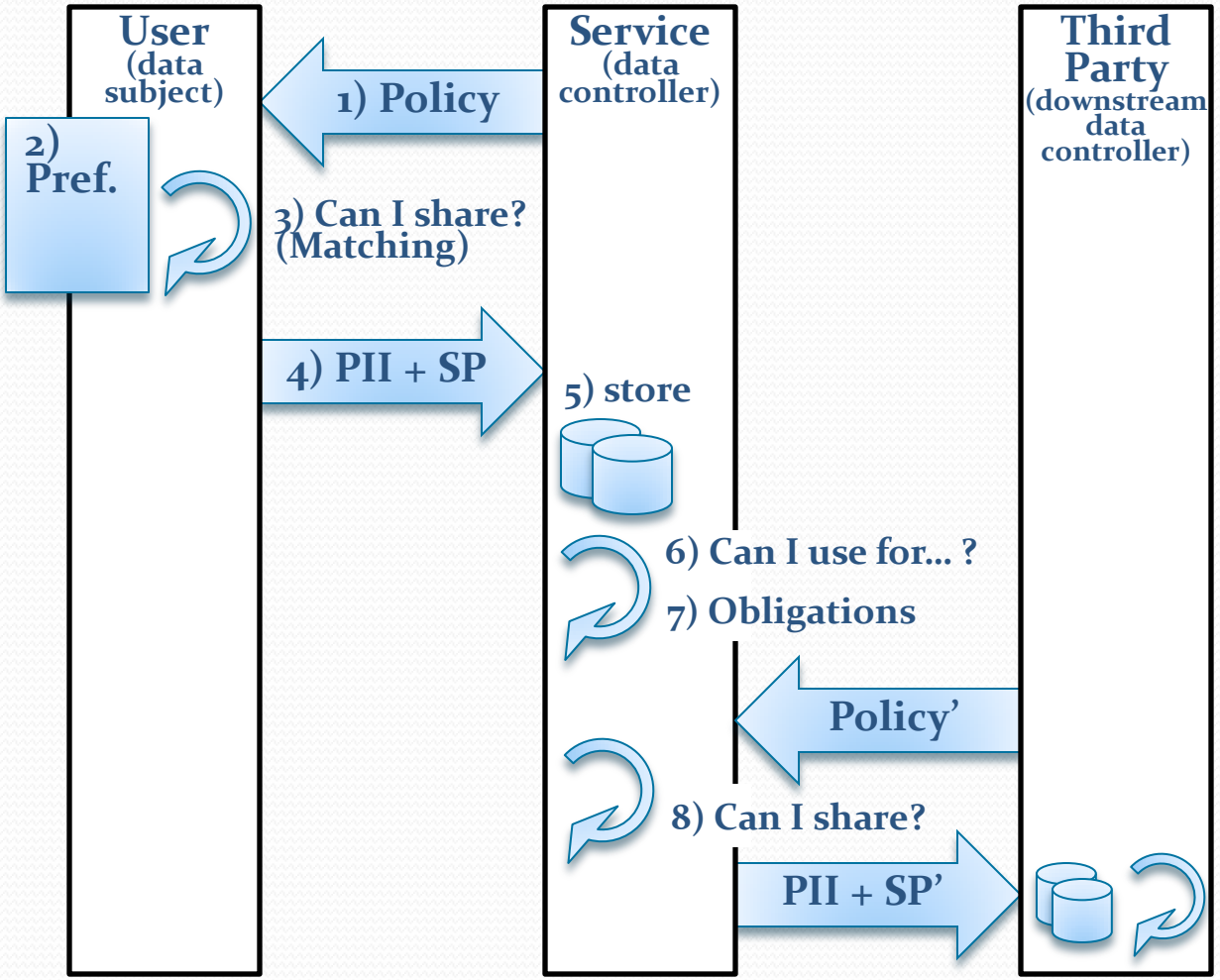
W3C Workshop on Access Control Application Scenarios
November 17th 2009
Luxembourg

Outlines

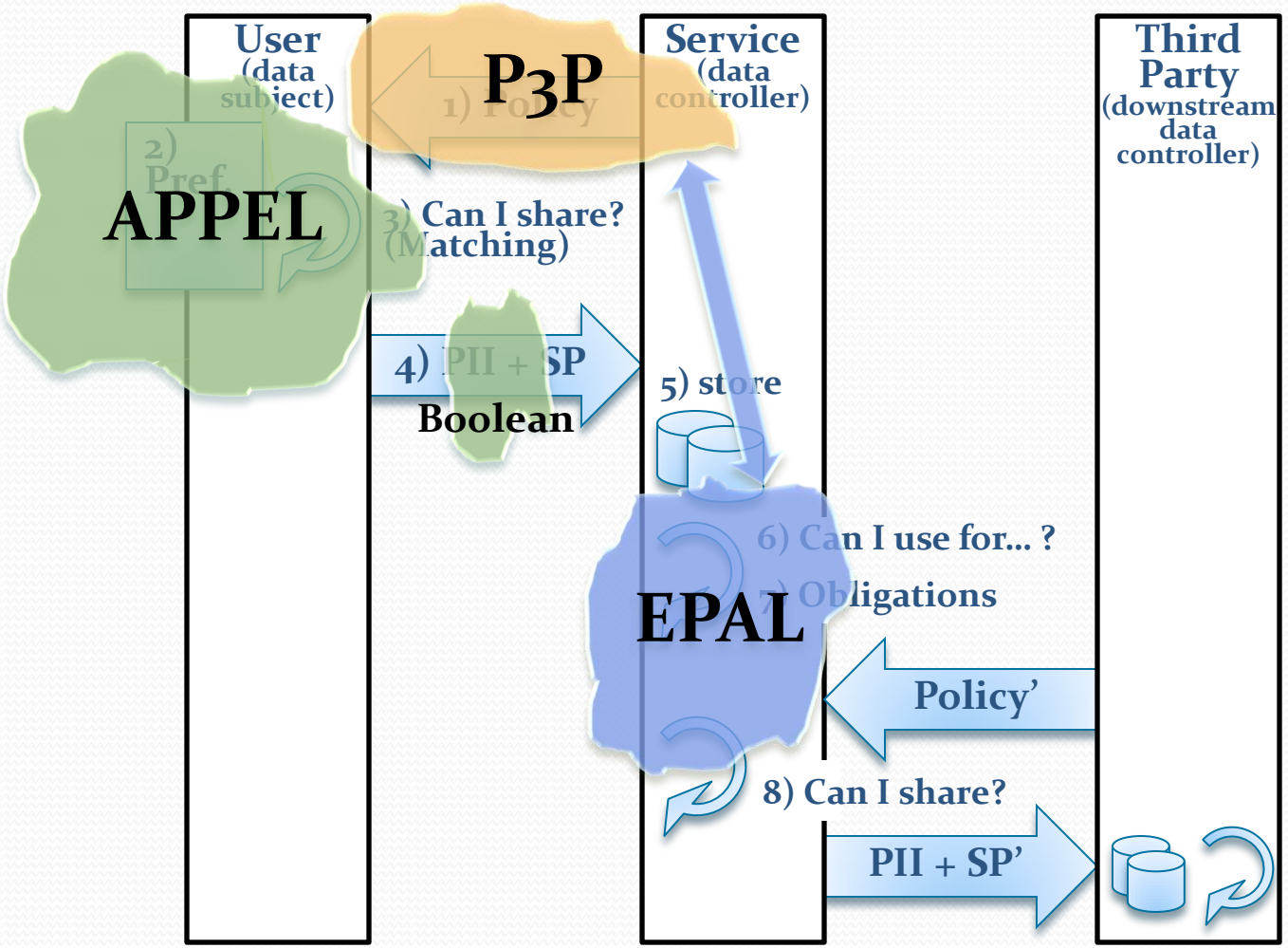
- Scenario: Privacy Policies and Preferences
- Links with Access Control
- Our work: from access control to data handling
  - SecPAL
  - SecPAL for Privacy
- Relevance for XACML

- Questions and Discussion

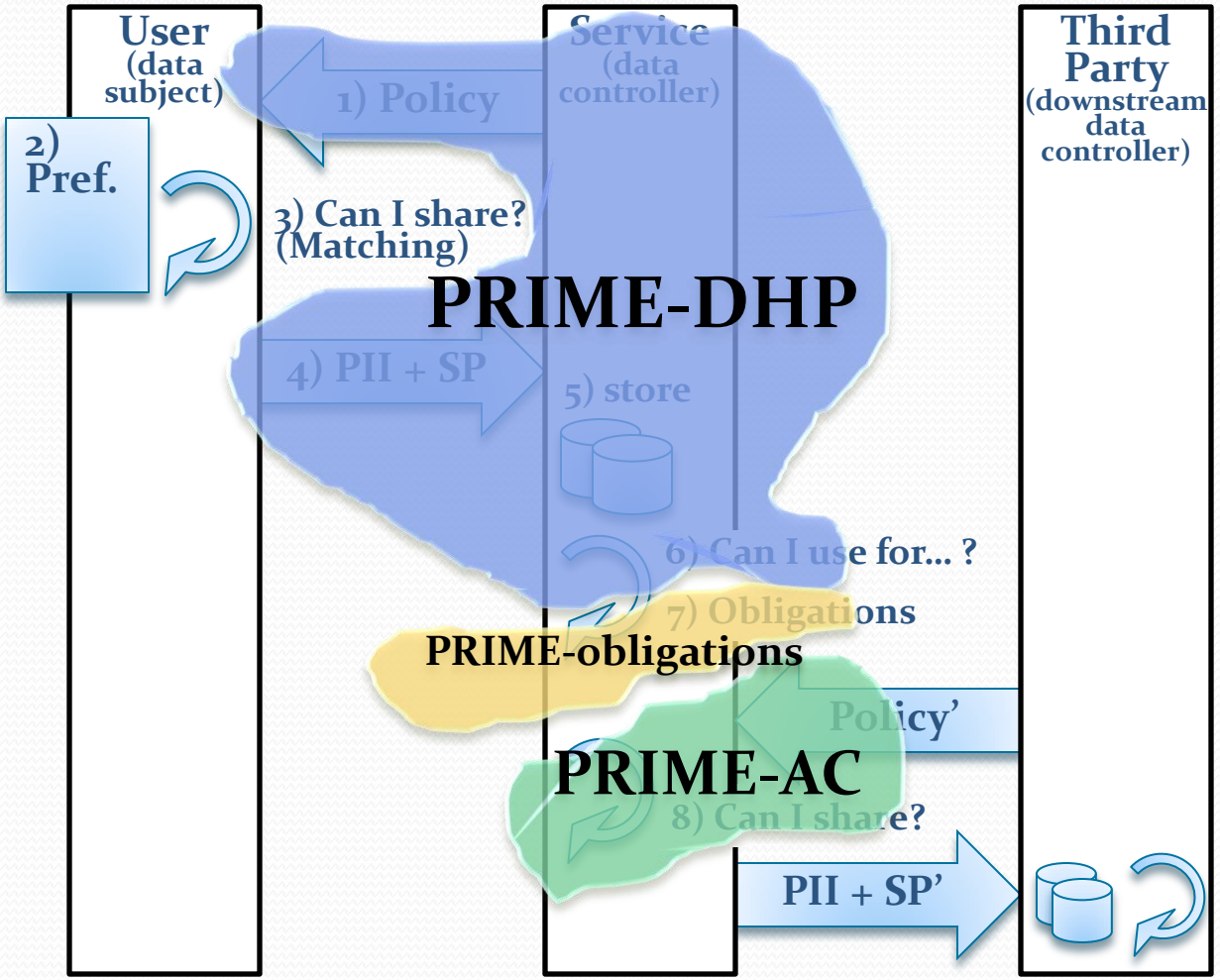
General Scenario



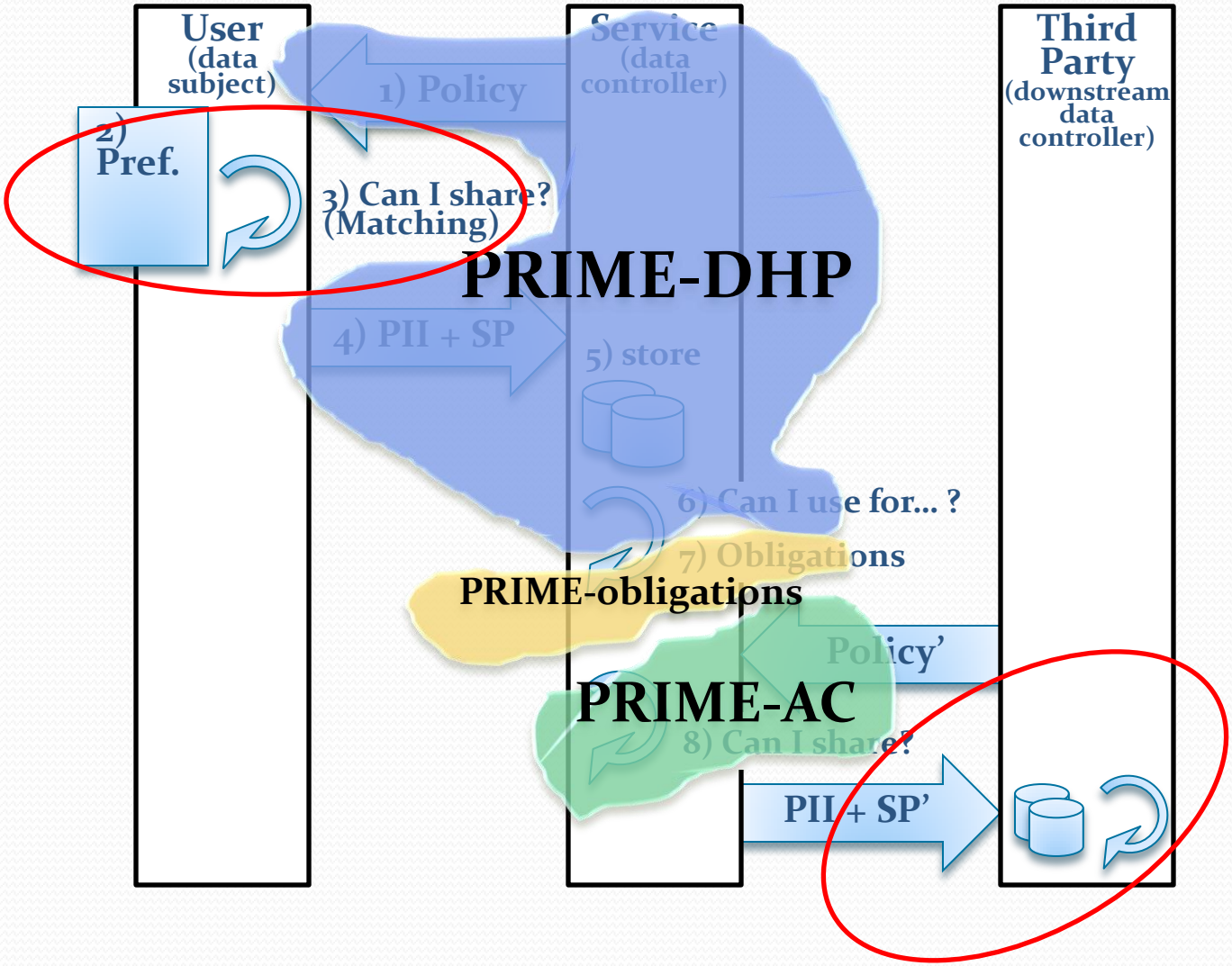
State of the art: APPEL, P3P, EPAL



state of the art: PRIME

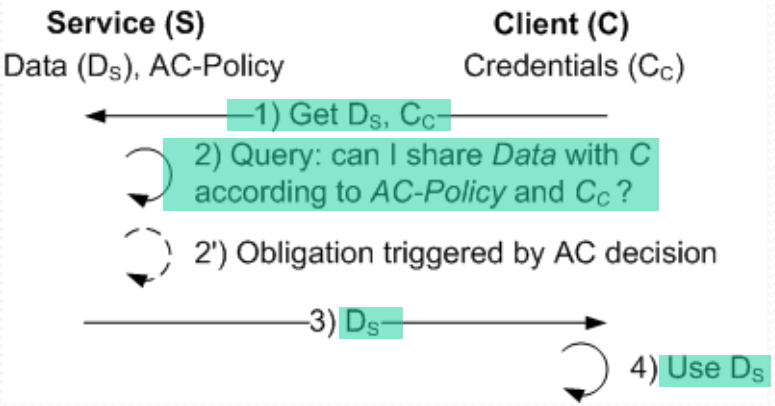


Shortcoming of state of the art

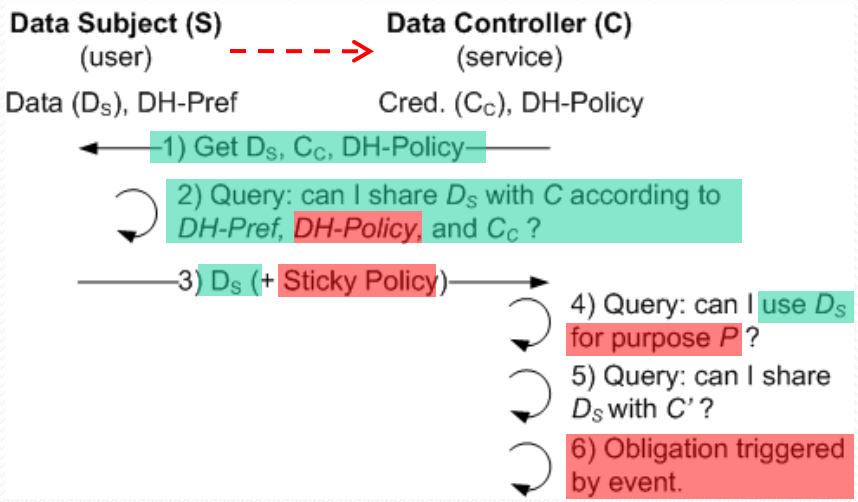


Access Control vs. Data Handling

Access Control (AC)



Data Handling (DH)



- Main differences:
  - In DH, "AC" query (2) takes two "policies" into account.
  - In DH, two parties specify (Sticky) Policy of C (including obligations)
  - In DH, C has to evaluate "AC" queries.
  - In DH, obligations are not only triggered by AC decisions

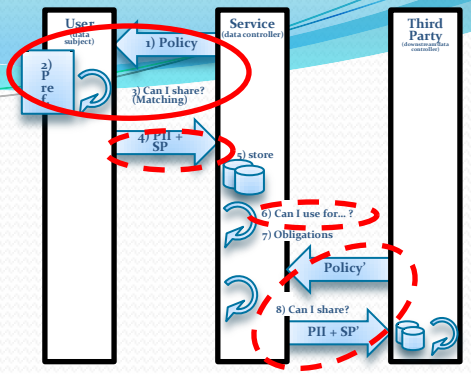
SecPAL (in one slide)

- AC Policy (assertions)
  - Service **says** CA **can say**$_0$ *x* **is a** researcher (A1)
  - Service **says** *y* **can read** /project/data **if** *y* **is a** researcher (A2)
- Credentials (assertions)
  - CA **says** Bob **is a** researcher (A3)
- AuthZ Query:
  - Service **says** Bob **can read** /project/data/file$_1$? (Q1)

  Q1 succeeds because A1 + A3 → Service **says** Bob **is a** researcher
  and because A2 + (A1 + A3) → Service **says** Bob **can read** /project/data

- Key features:
  - Balance between simplicity and expressiveness
  - Syntax close to natural language
  - Semantics consists of just three deduction rules
  - Logic-based: translation to "Datalog with Constraints"

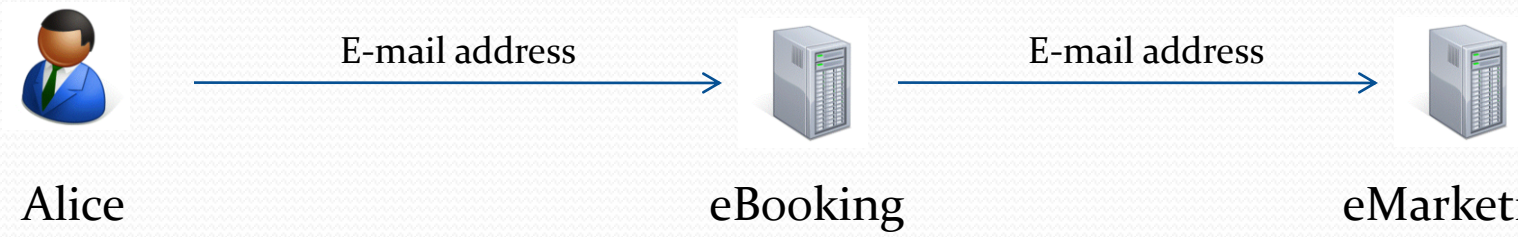
SecPAL for Privacy



- User's Preference
  - Rights
    <Usr> **says** <Svc> **may use** Email **for** *p* **where** (MA1)
    $p \in$ {Confirm; Marketing; Stats}
  - Obligations
    $\exists t$ (<Svc> **says** <Svc> **will delete** Email **within** $t \wedge t \leq 2$ yr) ? (WQ1)
- Service's Policy
  - Rights
    <Usr> **says** <Svc> **may use** Email **for** Marketing ? (MQ1)
  - Obligations
    <Svc> **says** <Svc> **will delete** Email **within** 1 yr (WA1)
- Data is shared if WQ1 and MQ1 succeed.
- This is not a complete example
  - Oversimplified policy and preference
  - Only shows matching (other queries at service)
  - Multi-hops data sharing and delegation are not presented here

9

Example: SecPAL for Privacy



Alice's preference

Pr.1 Alice says x may use Email for p if
x is a BookingSvc,
where $p \in \{\text{Confirmation}, \text{Newsletter}, \text{Stats}\}$

Pr.2 Alice says x may delete Email within t

Pr.3 Alice says x may send Email to y if
x is a BookingSvc,
y is a TrustedPartner

Pr.4 Alice says CA can say x is a y

Pr.5 Alice says x can say y is a TrustedPartner if
x is a BookingSvc

PrQ.6 Alice says $\langle$Svc$\rangle$ is a RegisteredSvc? $\wedge$
$\exists t$ ($\langle$Svc$\rangle$ says $\langle$Svc$\rangle$ will delete Email within t? $\wedge$ $t \leq$ 30 days?)

eBooking's policy

Pl.1 eBooking says eBooking will delete Email within 15 days

Pl.2 CA says eBooking is a RegisteredSvc

Pl.3 CA says eBooking is a BookingSvc

PlQ.4 $\langle$Usr$\rangle$ says eBooking may use Email for Confirmation? $\wedge$
$\langle$Usr$\rangle$ says eBooking may use Email for Stats? $\wedge$
$\langle$Usr$\rangle$ says eBooking may delete Email within 15 days? $\wedge$
$\langle$Usr$\rangle$ says eBooking may send Email to eMarketing?

eBooking says eMarketing is a TrustedPartner

eMarketing's preferences

Pl′.1 eMarketing says eMarketing will delete Email within 30 days

Pl′.2 CA says eMarketing is a RegisteredSvc

PlQ′.3 $\langle$Usr$\rangle$ says eMarketing may use Email for Marketing? $\wedge$
$\langle$Usr$\rangle$ says eMarketing may delete Email within 30 days?

XACML as DH-aware AC?

Requirements	SecPAL for Privacy	DH-aware XACML
Specification of access control rules	may-assertions	XACML policy (+ extensions)
Authorization queries	may-queries	XACML query (input to PDP)
Specification of generic obligations	will-assertions	XACML-obligation (+ extensions)
Obligation queries	will-queries	-
Specification of attributes and rights	usual SecPAL assertions	SAML assertions

Actors	SecPAL for Privacy	DH-aware XACML
User agent	SecPAL engine	XACML PDP

Upper bound (may) in XACML

- Expressing the upper bound on behaviors (may verb) should be possible with XACML.
  - Data subject's preferences: a XACML policy
  - Data controller's preferences would be a set of queries.
- The user agent = Policy Decision Point.
- Extensions required:
  - handle “purpose”
  - placeholders that are instantiated before evaluating the query.

Lower bound (will) in XACML

- Data controller's side:
  - complete specification of XACML obligations
  - support for obligations that are not triggered by access control decision.
  - Part of this may be covered by ongoing work on a proposal for obligations1 in XACML 3.0.
- Data subject's side:
  - a language to query obligations would be necessary.

- Lower and upper bound should be comparable.

Questions and Discussion

- Should we consider XACML in such scenarios?
- Are lessons learned from extending SecPAL towards data handling applicable to XACML?
- Should XACML obligations support other types of triggers?
- How to serialize “XACML queries”?
- How to specify “obligation queries”?
- Multiple languages (upper and lower)?

Contact: LBussard@microsoft.com
Details on SecPAL (for Privacy): http://research.microsoft.com/SecPAL

Backup slides

SecPAL for Privacy: User's Preferences

Pr.1 Alice says x may use Email for p if
x is a BookingSvc,
where $p \in \{\text{Confirmation}, \text{Newsletter}, \text{Stats}\}$

Pr.2 Alice says x may delete Email within t

Pr.3 Alice says x may send Email to y if
x is a BookingSvc,
y is a TrustedPartner

Pr.4 Alice says CA can say x is a y

Pr.5 Alice says x can say y is a TrustedPartner if
x is a BookingSvc

PrQ.6 Alice says $\langle \text{Svc} \rangle$ is a RegisteredSvc? $\wedge$
$\exists t$ ($\langle \text{Svc} \rangle$ says $\langle \text{Svc} \rangle$ will delete Email within t? $\wedge$ $t \leq$ 30 days?)

SecPAL for Privacy: Services' Policy

Pl.1 eBooking says eBooking will delete Email within 15 days

Pl.2 CA says eBooking is a RegisteredSvc

Pl.3 CA says eBooking is a BookingSvc

PlQ.4 ⟨Usr⟩ says eBooking may use Email for Confirmation? ∧
⟨Usr⟩ says eBooking may use Email for Stats? ∧
⟨Usr⟩ says eBooking may delete Email within 15 days? ∧
⟨Usr⟩ says eBooking may send Email to eMarketing?

eBooking says eMarketing is a TrustedPartner

Pl′.1 eMarketing says eMarketing will delete Email within 30 days

Pl′.2 CA says eMarketing is a RegisteredSvc

PlQ′.3 ⟨Usr⟩ says eMarketing may use Email for Marketing? ∧
⟨Usr⟩ says eMarketing may delete Email within 30 days?