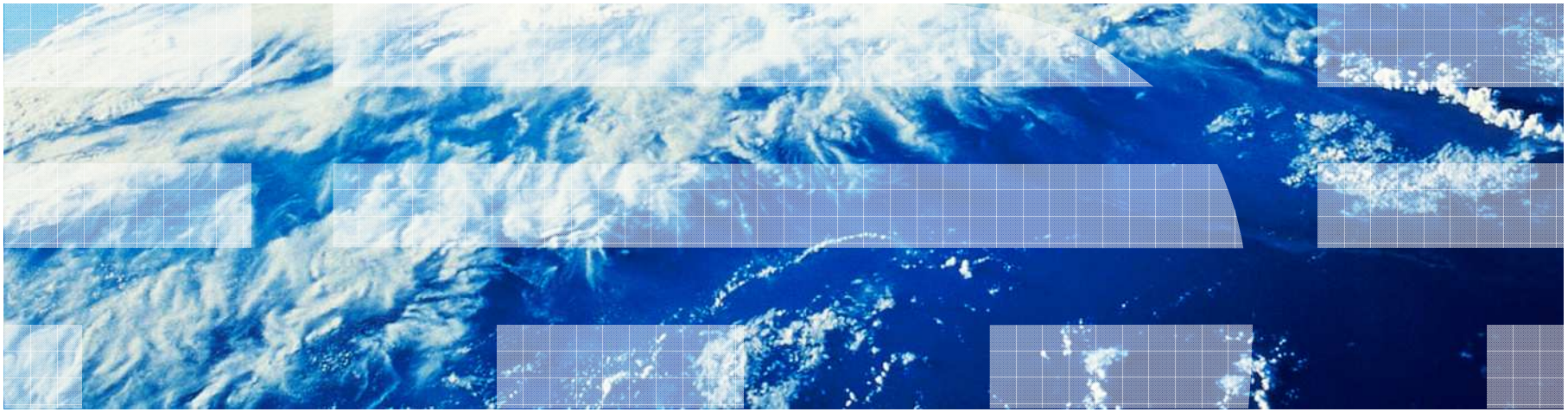
Gregory Neven, IBM Research – Zurich

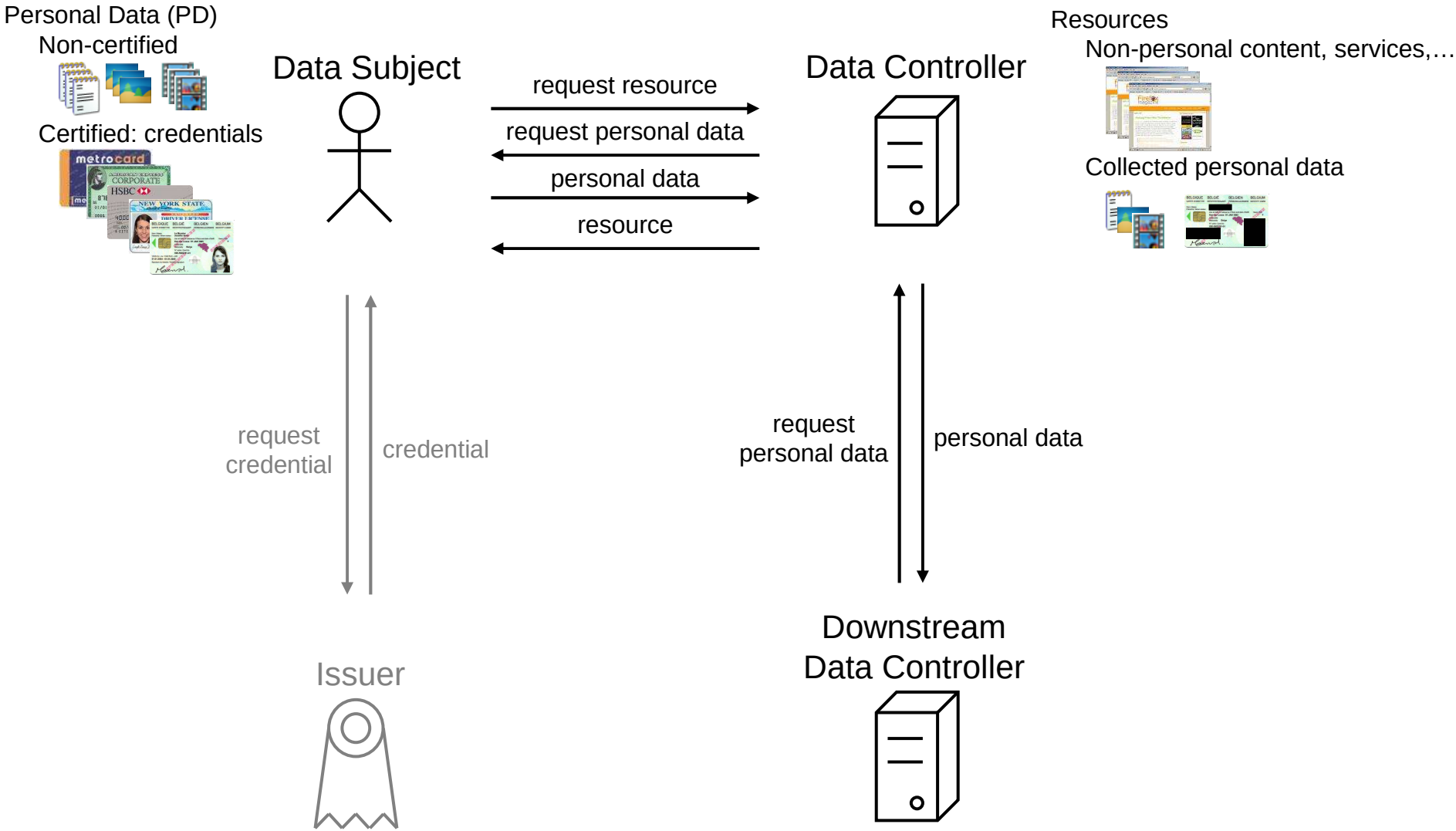
W3C Workshop on Access Control Scenarios, Nov. 18th, 2009, Luxembourg

Claudio Ardagna, Eros Pedrini, Sabrina De Capitani di Vimercati, Pierangela Samarati,
Laurent Bussard, Gregory Neven, Franz-Stefan Preiss, Stefano Paraboschi,
Mario Verdicchio, Dave Raggett, Slim Trabelsi

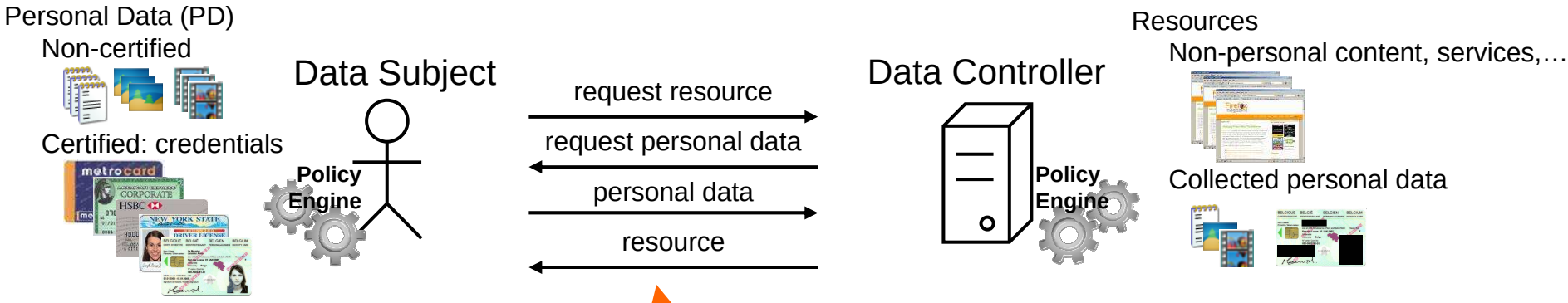
PrimeLife Policy Language



Scenario


Personal Data (PD)
Non-certified
Certified: credentials
Data Subject
request resource
request personal data
personal data
resource
Data Controller
Resources
Non-personal content, services,…
Collected personal data
request credential
credential
request personal data
personal data
Issuer
Downstream Data Controller

Types of policies



Specific Policy:
over specific personal data (e.g. birth date)
- **Access control policy (ACP):**
  who can access (e.g. PrivacySeal silver)
- **Data handling preferences (DHPrefs):**
  how is to be treated when revealed
  - **Authorizations** (e.g. marketing purposes, forwarded to PrivacySeal gold)
  - **Obligations** (e.g. delete after ≤2y)

Generic Preferences:
DHPrefs over implicitly revealed personal data (e.g. IP address, cookies,…)
- **Authorizations** (e.g. admin purposes)
- **Obligations** (e.g. delete after ≤2y)

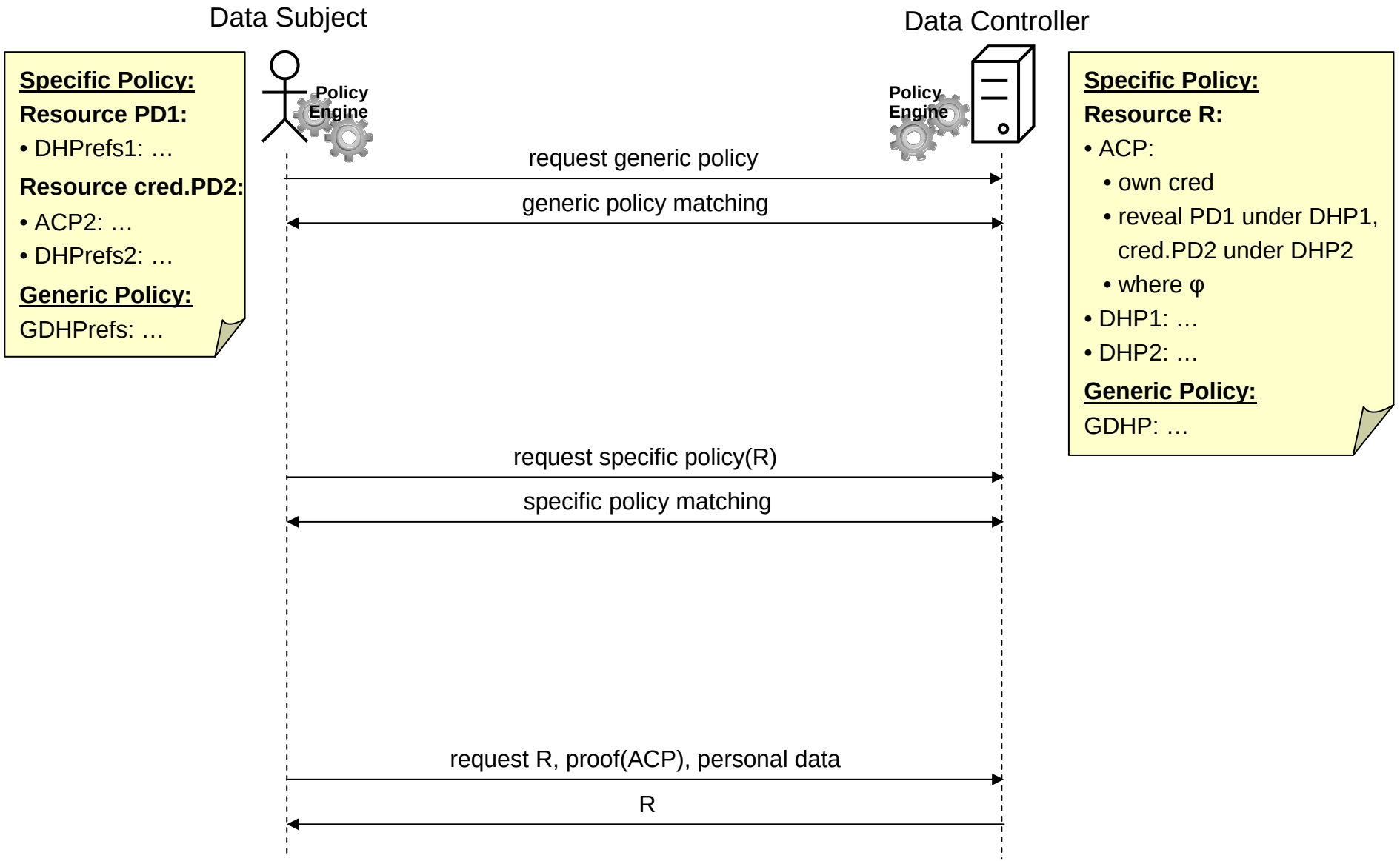
SAML

XACML

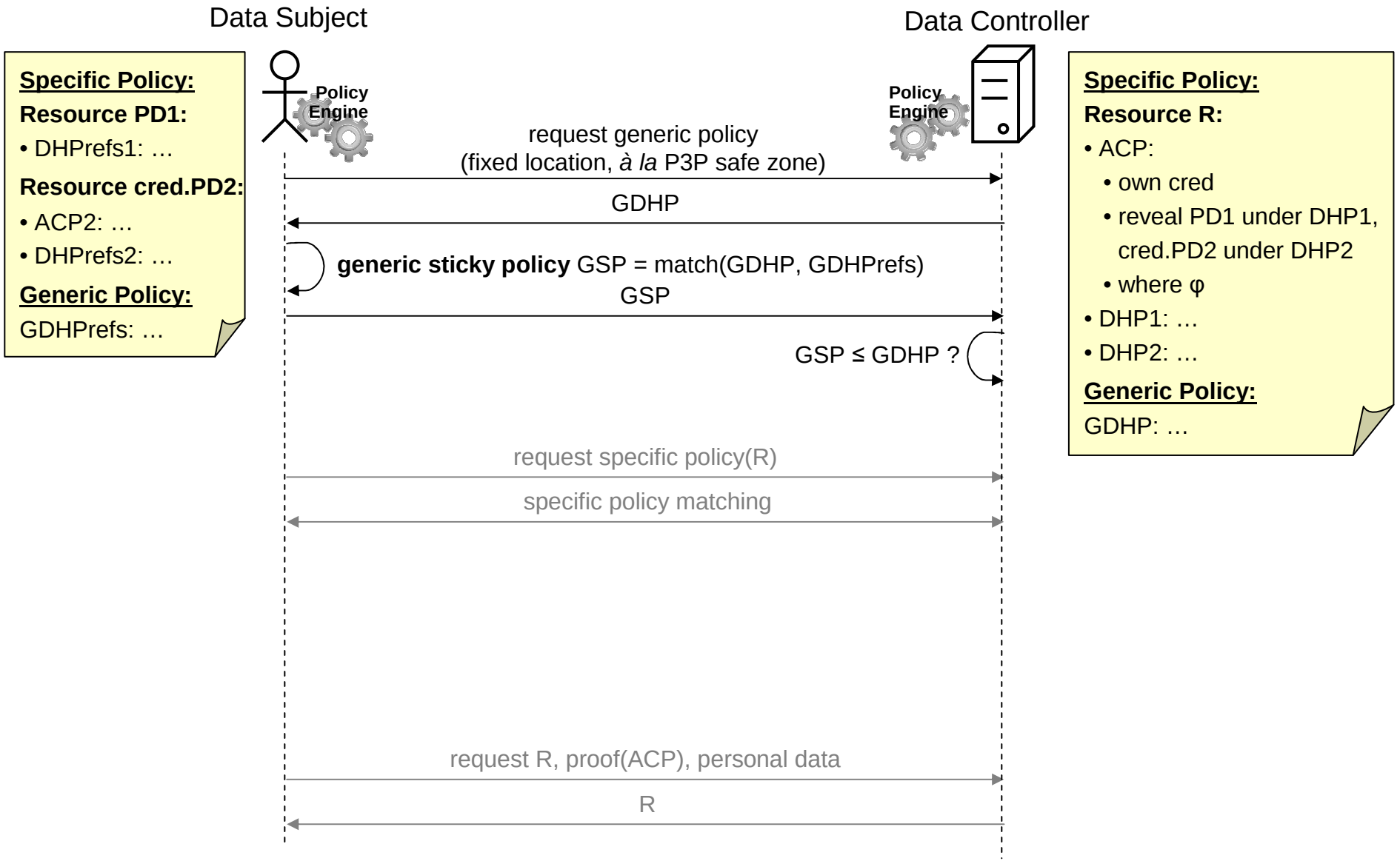
Specific Policy:
over specific resource (e.g. BuyService)
- **Access control policy (ACP):**
  who can access
  - credentials to possess (e.g. ID card)
  - personal data to reveal (e.g. nationality)
  - conditions to satisfy (e.g. age>18)
- **Data handling policy (DHP):**
  how revealed personal data will be treated
  - **Authorizations** (e.g. marketing purposes)
  - **Obligations** (e.g. delete after 1y)

Generic Policy:
DHP over implicitly revealed personal data (e.g. IP address, cookies,…)
- **Authorizations** (e.g. admin purposes)
- **Obligations** (e.g. delete after 1y)

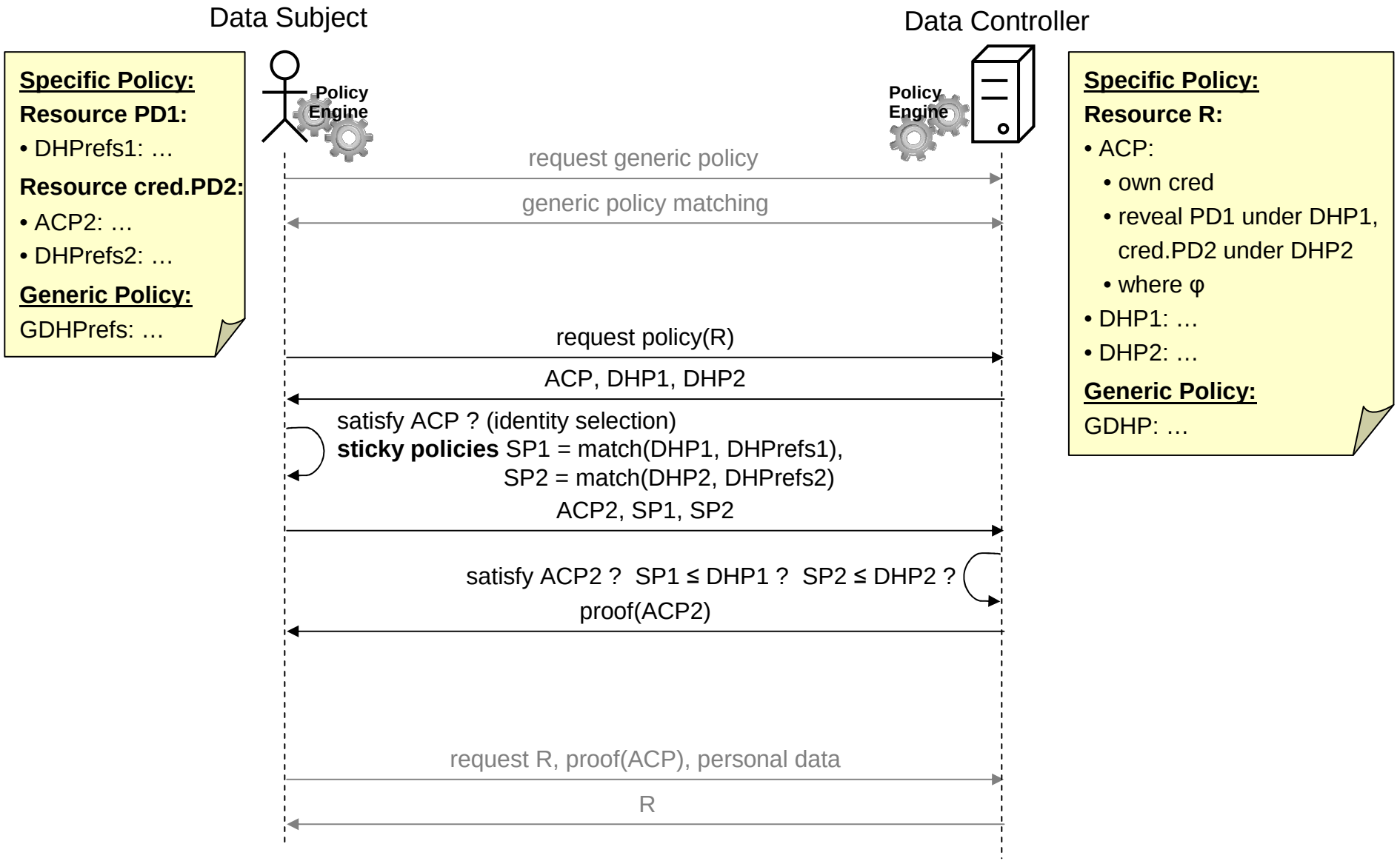
Interaction overview



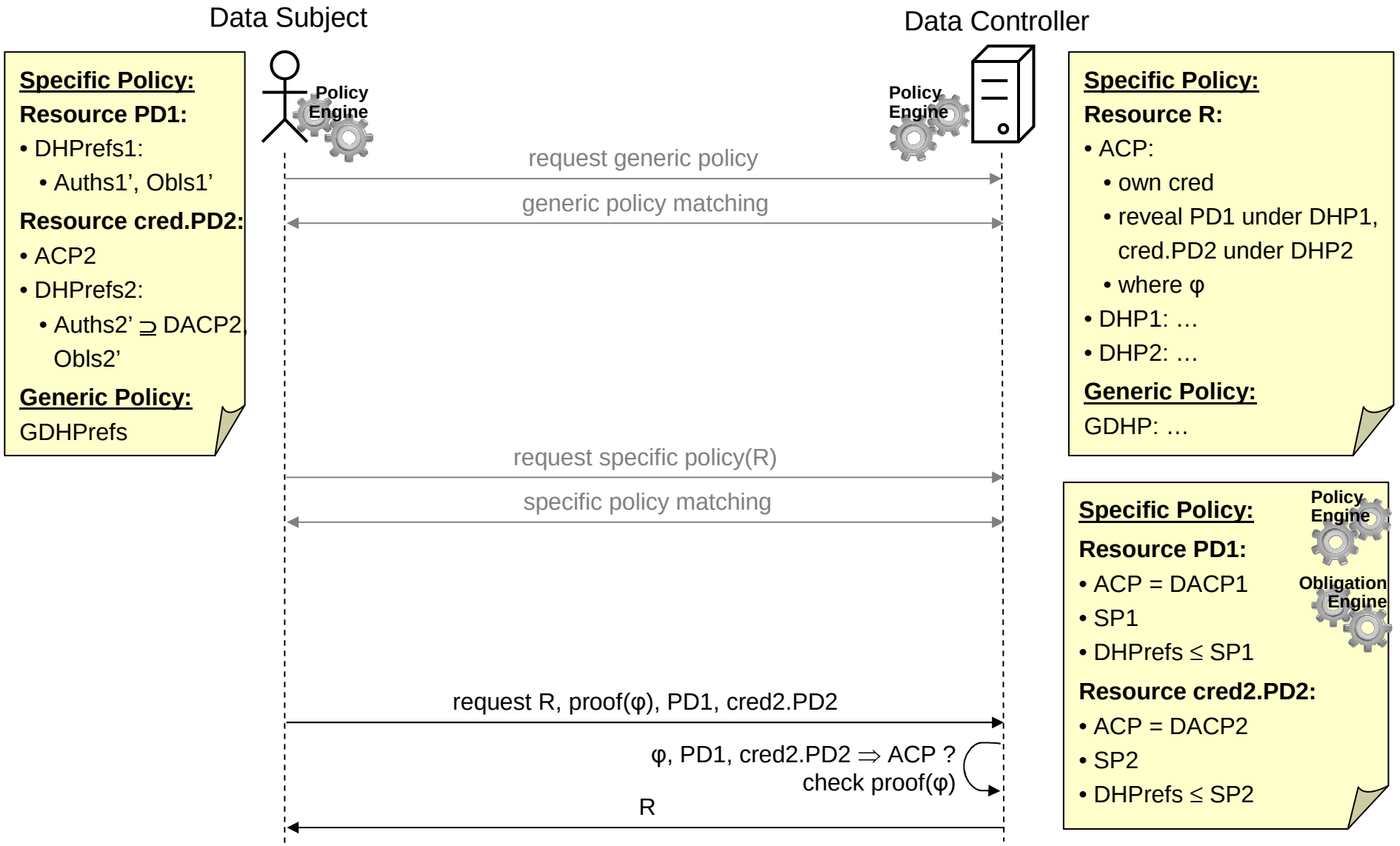
Interaction overview: generic policy negotiation



Interaction overview: specific policy negotation



Interaction overview: resource request



Authorizations and obligations

- General principle: provide
  - wrapper for user-extensible vocabularies
  - basic pre-defined vocabulary
- Authorizations
  - “use for purpose”
    - user-extensible (OWL?) ontology of purposes,
    - basic pre-defined ontology available
  - “forward to ACP” = downstream access control
- Obligations
  - general structure: **do** action **when** trigger (**from** start **to** end)
  - pre-defined actions:
    - “delete data”
    - “anonymize data”
    - “notify data subject”
    - “write to (secure) log”
  - pre-defined triggers:
    - at time, periodic
    - data access, data deletion
    - data loss, obligation violation
    - aliens landing on earth

Obligation & authorization matching

automated matching of **any** two data handling preferences/policies via **"less permissive than"** relation (≤) defined on

- authorizations, e.g.

  use for {delivery} ≤ use for {delivery,marketing}

- triggers, e.g.

  trigger at 2010/01/01 ≤ trigger at 2010/12/31

- actions, e.g.

  delete firstname, lastname ≤ delete firstname

- obligations

  action
  trigger
  validity

  $o_1=(a_1,t_1,v_1) \leq o_2=(a_2,t_2,v_2) \Leftrightarrow (a_1 \leq a_2) \wedge (t_1 \leq t_2) \wedge (v_1 \leq v_2)$

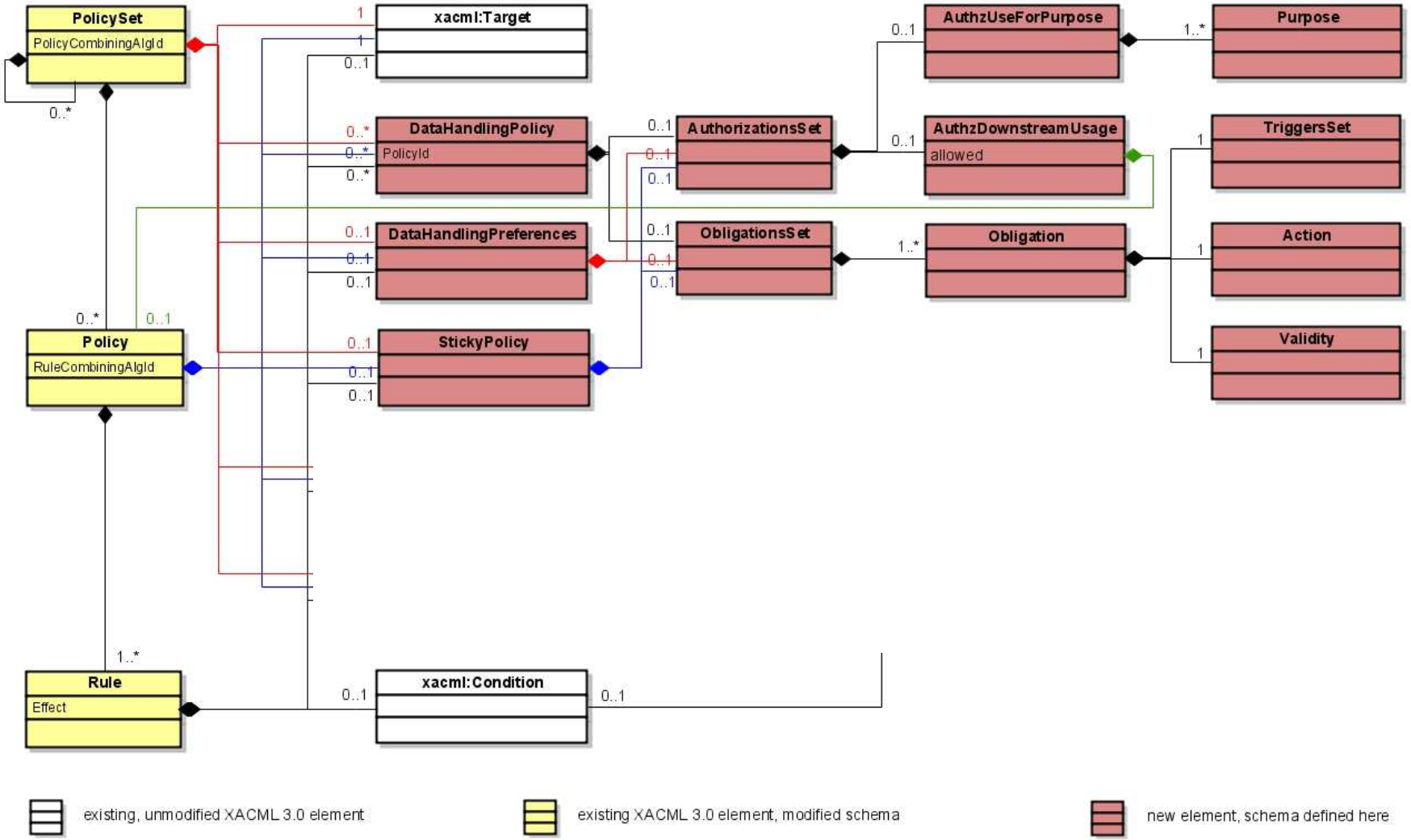
- sets of authorizations and obligations

  $O_1 \leq O_2 \Leftrightarrow \forall o_1 \in O_1 \; \exists o_2 \in O_2 : o_1 \leq o_2$

- data handling policies

  $P_1 = (A_1,O_1) \leq P_2 = (A_2,O_2) \Leftrightarrow A_1 \leq A_2 \wedge O_1 \leq O_2$

Embedding into XACML



Summary

- Privacy enhancements
  - step-wise interaction: generic policy, specific policy, resource
  - reveal attributes vs. prove condition holds
  - two-sided data handling policies/preferences, automated matching
  - user-extensible authorization/obligation vocabularies, basic vocabularies provided
- Credential-based access control
  - attributes grouped in credentials
  - technology independence
  - policy sanitization
- Based on existing standards: XACML & SAML