



Long term changes to P3P

Long Term Future of P3P Workshop

Giles Hogben

Joint Research Centre European
Commission

Summary



- MAIN GOAL: Expanding the scope of P3P
- Preference Exchange Language + Identity Management
- Against Compact Policies
- Consent
- Enterprise and Audit Trails
- Data Typing Schema
- Ontology and Useability

Preference Exchange Language

– Why do we need one?



APPLY RULE

Description (May be used to describe what the rule does)

FOR DATA OF THE FOLLOWING KIND (What kind of data you want to apply this rule to?)
Describe briefly in words what kind of data the rule applies to. Over- specify the data type using the list below.

Yes (Do not Specify) **Do not Specify (Do not want to specify)**

Data Categories: **Force Data Type**

<input type="checkbox"/> All Information Data	<input type="checkbox"/> All of Selected
<input type="checkbox"/> All Information Data	<input type="checkbox"/> Other Information
<input type="checkbox"/> All Information Data	<input type="checkbox"/> Governmental Information
<input type="checkbox"/> All Information Data	<input type="checkbox"/> Geographic & Topographic
<input type="checkbox"/> All Information Data	<input type="checkbox"/> Identifier
<input type="checkbox"/> All Information Data	<input type="checkbox"/> Location
<input type="checkbox"/> All Information Data	<input type="checkbox"/> Numeric Data
<input type="checkbox"/> All Information Data	<input type="checkbox"/> Preference Data
<input type="checkbox"/> All Information Data	<input type="checkbox"/> Text

IF THE RULE TRIGGERS (What the rule should look for)

RETENTION (How long) | RECIPIENTS (Who to) | PURPOSE (What for) | ACCESS to data after submitting

<input checked="" type="checkbox"/> All of Selected	<input checked="" type="checkbox"/> Do not Specify - None set of rule	<input type="checkbox"/> All others
<input type="checkbox"/> None of Selected	<input type="checkbox"/> All others for specified condition	<input type="checkbox"/> All of Selected
<input type="checkbox"/> All Information Data	<input type="checkbox"/> To receive the data purpose set	<input type="checkbox"/> All of Selected
<input type="checkbox"/> All Information Data	<input type="checkbox"/> To receive the data purpose set	<input type="checkbox"/> All of Selected
<input type="checkbox"/> All Information Data	<input type="checkbox"/> To receive the data purpose set	<input type="checkbox"/> All of Selected

THEN DO THE FOLLOWING (What to do if the rule conditions are met)

What to do if the rule conditions are met:

Ask my permission to do this:

What to say when you ask my permission:

OK Cancel

Preference Exchange Language

– Why do we need one?



- Configuring preferences is too complex and time consuming for users.
- But defaults should be open to experts and 3rd parties e.g. law enforcement.
- Preferences should be able to take account of e.g. cultural diversity
- For “sticky” preference sets and moving between browsers.

What went wrong with APPEL?



- Syntax too quirky
- Logic unintuitive (lots of ways to say the same thing)
- Logically ambiguous (see paper).
- No Involvement of implementers.

Appel:What can we do?



- Use Xpath for rule “Body”
- Example

```
<appel:RULE behavior="block" prompt="yes" promptmsg="Resource will use your home info beyond current purpose ">  
    <appel:MATCHQUERY query="//DATA[not(substring(@ref,'dynamic.clickstream.clientip.fullip') or  
        substring(@ref,' dynamic.http.useragent'))]" querylanguage="XPATH">  
</appel:RULE>
```

(block all sites which collect any information beyond clickstream data.)

- Advantages
 - Standards compliant
 - Widely known by developers
 - Flexible and General
 - Uses optimised systems

Appel:What can we do?



- Drop ordering constraint – all rules fire with rules for what to do on conflict?

Needs further research...

Appel:What can we do?



- Link to identity management systems
 - Greater range of behaviors
 - Link to mechanism for information request (link to Xforms)
 - P3P cannot provide a data request because it is a policy language (general statements).
- Ability to associate P3P policies at the level of the form field (we will do x with your email and y with your medical details)

Appel:What can we do?



Involve implementers

Against Compact Policies



- “A site **MUST** honor a compact policy for a given URI in any case (even when the full policy referenced in the policy reference file for that URI does not correspond ... to the compact policy itself).” *P3P 1.0 specification*
- BUT compact policies only “provide hints” to user agents to enable the user agent
- Rely on a handful of tokens to summarize a full policy so necessarily corrupt the meaning of many policies.
- In practice, compact policies have been used to replace full policies.

Why did we think needed Compact Policies?



- Speed of evaluation?
 - not a significant problem.
- Saving on roundtrips?
 - with caching not a significant problem.
- Ease of expression?
 - not an issue due to policy GUIs.

Solution



- Get rid of them!
- Publish guidelines on how to reduce round-trips.
- Publish fast matching algorithm guidelines.

Data Typing Schema



- We now have XML Schema version of base data schema and xslt's to make the relevant conversions.

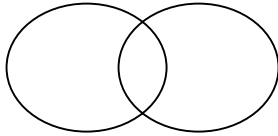
BUT 1.

- No way to simply specify whether a data type is personally identifiable.

Data Typing Schema



BUT 2.

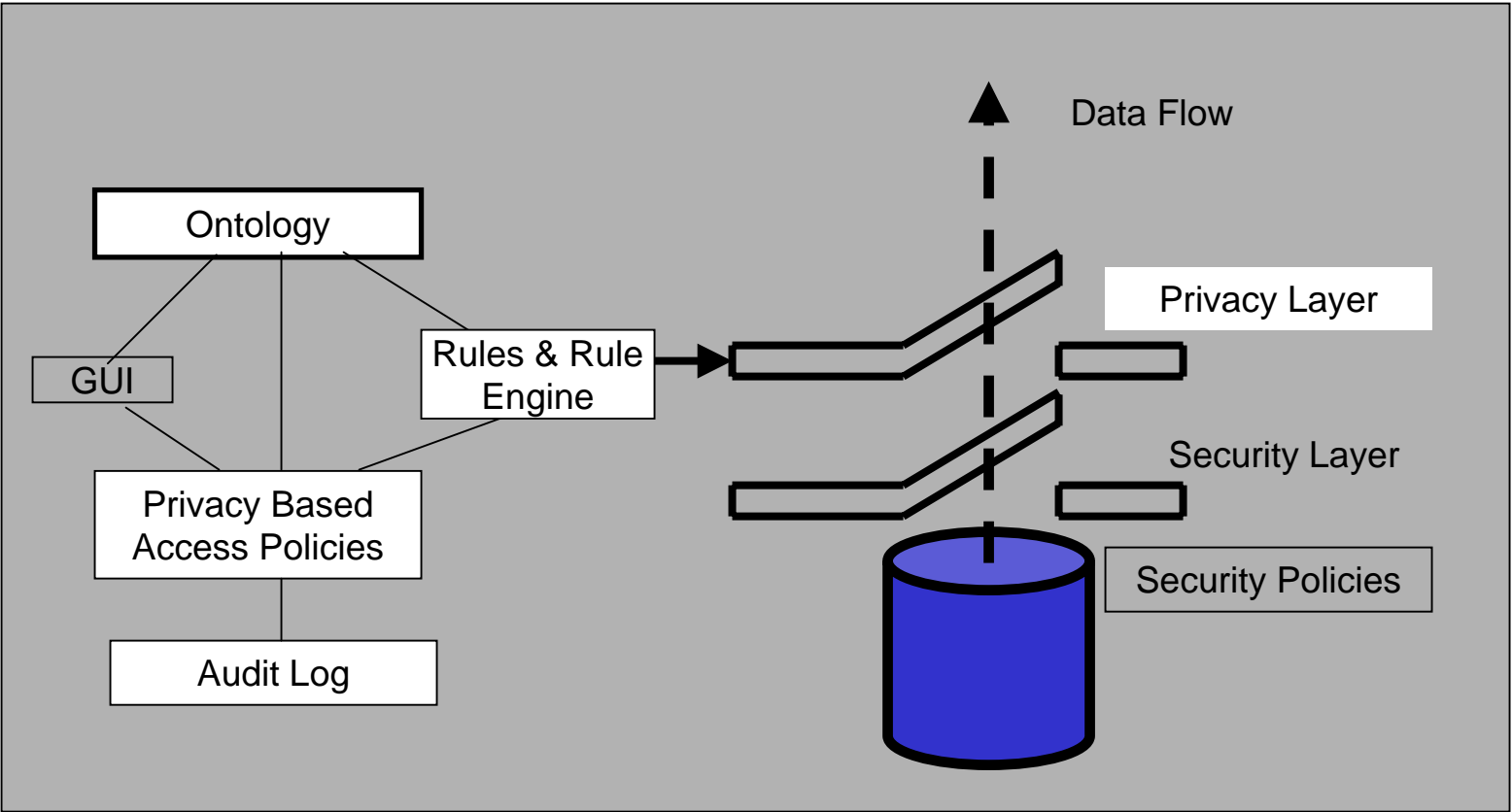
- Semantics is unnecessarily confused and complex:
 - 2 orthogonal systems: categories and data elements.
 - No formal semantics.
E.g does “user” mean users or does it mean the class of data about users.
This seems trivial but without clear semantics, its useage is restricted.
 - Categories are ambiguous (not disjoint) e.g.  political/government).
 - it is possible to write inconsistent descriptions (e.g. non-identifiable + physical category???)
 - Other small points of detail – see paper.

Enterprise Audit Trails and P3P: Why?



- Crucial issue for P3P1.0: “That’s what they say – but what if they don’t do what they say?”
- Audit trails are a way of automatically checking on actual practices.
- Accountability mechanism.

Enterprise Privacy Audit architecture



Requirements from P3P



- Adaptation of semantics for privacy access profiles (APPEL+).
- Adaptation of semantics for privacy-crucial event trail logs.
- Mapping tools for aligning internal data models with P3P standardised semantics.
- Rule based system for analysing logs.

Why Consent in P3P?



LAW:

- The EU's Article 29 working group.
"Internet users must have a real possibility of objecting on-line by clicking a box"
- The need to prove that consent has been collected is increasingly important.

Why consent in P3P?



ARCHITECTURE:

- P3P's is always going to be at the exact point in the system where the user is deciding whether to submit data.
- Works cross-context (e.g. AMI – smart coffee cups etc...) – not just HTML forms.
- With P3P, consent could be collected in any situation where privacy policies are provided (assuming we go beyond HTTP)

How to apply a consent mechanism in P3P: consent request



- Semantics for requesting consent attached to the policy for an information request: e.g.

```
<DATA ref="user.home-info">  
  <CONSENTREQUEST method="httpheader" headername="consent1">  
    <DATAREQUIRED certificate="X.509" algothmtype="RSA" minkeylength="128">  
      I agree that my data in this form will be published on the internet.  
    </DATAREQUIRED>  
  </CONSENTREQUEST>  
</DATA/>
```

How to apply a consent mechanism in P3P: structure of message



Structure of message:

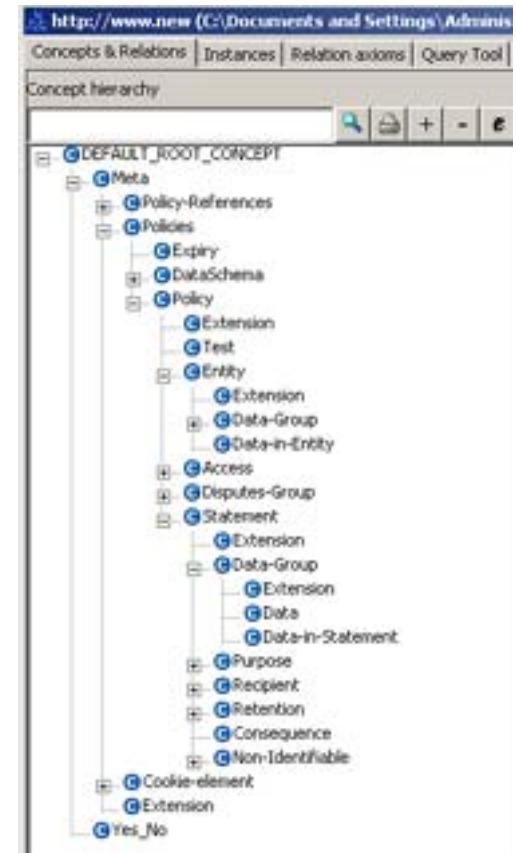
- Using a proposed RDF ontology version of P3P, we could give some semantics to the consent messages.

E.g. "I (data subject) agree that the information transferred in this request may be received by third parties." (ontological terms underlined)

Ontology of P3P



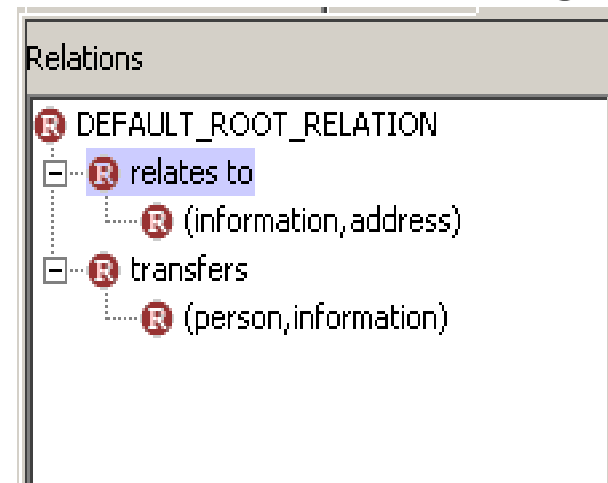
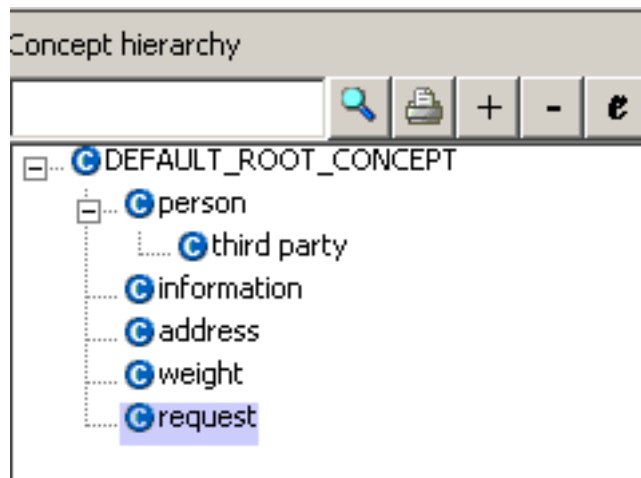
- Current semantics of P3P
Based around the policy
- Predicates key to flexibility
Currently missing
 - “Information”
 - “Transfers” (no predicates at all)
 - “Relates to”



Revised ontology of P3P: Why



- Allows greater flexibility of expression and uses for P3P.
- Greater legal accountability.
- More flexibility in translation between different user-groups.
- User translations based on situational testing.



More information



- Ontologies for Privacy – <http://pronto.jrc.it>
- P3P proxy <http://p3p.jrc.it>

- Questions ?