Patient consent policies

From User to XACML

Project

- Ongoing master thesis project
- In cooperation with Philips
- EHR with centralized access
- Enable user specified policies
- User requirements translated to XACML
    - Reuse of existing XACML tools
    - Rule priorities added

Other Projects

- TAS3 (EU)
    - Trust; LoA, behaviour, certificates, KPIs,
        - validation level, etc. also possible
    - Ontologies
    - Also WPs on
        - Legal&Privacy
        - Work flows
        - Data protection
        - ID management
    - Health care & employability
- Poseidon
    - Trust, Ontologies, Marine safety

Motivation

- Current consent paper based
  - Static, inflexible, no customization
- Allow patients to determine policies
  - Current trend
  - Needed for use, acceptance new e-health systems
  - Patient centric health care
  - To satisfy privacy laws

Patient specification of policies

- Current state of the art: text with restricted syntax
  - Interpretation free text far not yet possible
    - and often ambiguous
  - decided not to focus on this in this project
- Baseline: Policy specified in GUI and/or with aid security officer
  - Result table of rules
  - Build by hand (aided by GUI) from user requirements
  - Focus on conflicts, possible confusions & translation to XACML

Example user requirements

- General denial with exceptions:
  - I would like my doctor to read and write my medical data for treatment, payment, operations, public health and quality measures.
  - I would like all other doctors to read and write my data for treatment purposes only for the next one year.
  - Dr. John Mathews can only read or write to my data for treatment in an emergency.
  - I would like my husband to have read access to all my data.
  - I would also like my mother to have read access to my data. However, my mother should not read my gynecological information and the blood pressure measurements taken within the last 3 months.

Conflicts

- Conflicting requirements
  - I would like all other doctors to read and write my data for treatment purposes only for the next one year
  - Dr. John Mathews can only read or write to my data for treatment in an emergency
- Detect
  - Check rules for overlaps
- Resolve
  - Automated resolution rules; e.g. 2nd is clearly an exception of 1st so should take precedence.
  - If not clear: request clarification from Patient
    - Setting policies interactive process
    - Need to find & resolve conflicts when policies defined

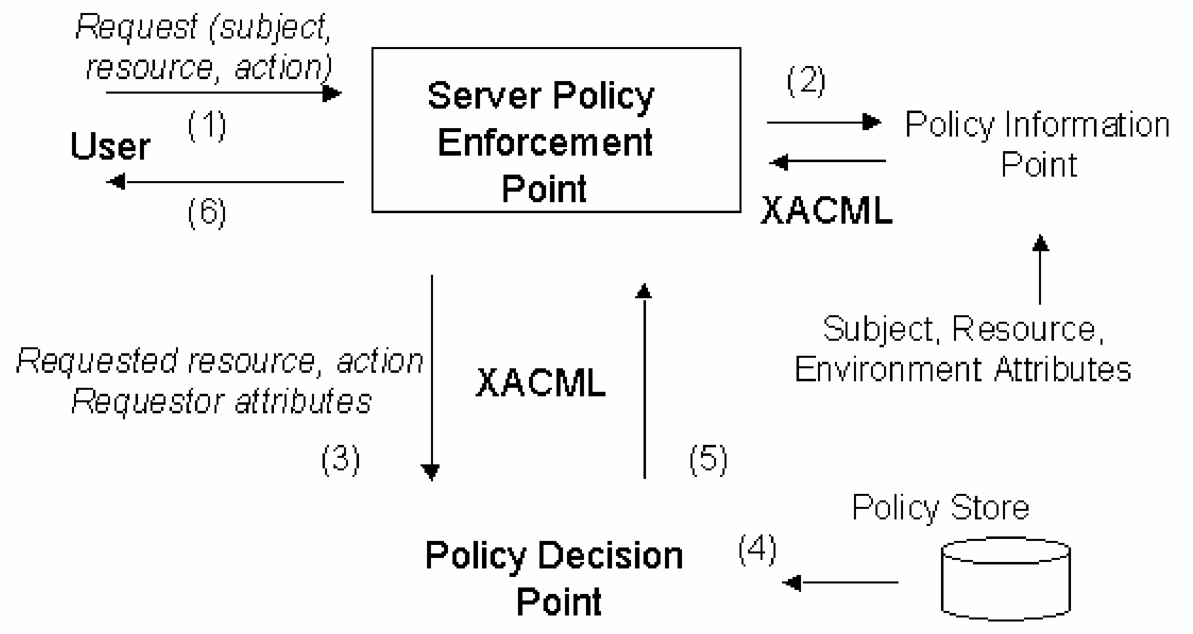
Confusion

- I.e. is given consent clear?
- Situations which indicate possible unintended access; e.g. assuming husband is a doctor...
  - □ I would like my husband to have read access to all my data.
  - □ I would like all other doctors to read and write my data for treatment purposes only for the next one year.

  Rules not in conflict but perhaps user not aware 2nd also applies to husband...(better examples exist).
- Not yet clear whether we can actually define these situations without getting to many...

XACML Basics

- eXtensible Access Control Markup Language
- Oasis Standard
- Policy Enforcement point (PEP)
  - □ Receives user requests
  - □ Handle request after response PDP:
- Policy Decision Point (PDP)
  - □ Checks request permitted based on policies


Request (subject, resource, action)
(1)
User
(6)
Server Policy Enforcement Point
(2)
Policy Information Point
XACML
Subject, Resource, Environment Attributes
Requested resource, action
Requestor attributes
(3)
XACML
(5)
Policy Decision Point
(4)
Policy Store

XACML Policy (sets):

- Policy set
  - Combining Algorithm
  - Set of Policies
- Policy
  - Target (applicable to what)
    - Attributes of Subject, Resource, Action, Environment
  - Rule (when applicable)
    - Attributes as above and conditions.
  - Obligations

A Request in XACML

```
<Request>
  <Subject>
     <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id“
                    DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name">
       <AttributeValue>seth@users.example.com</AttributeValue>
     </Attribute>
    <Attribute AttributeId="group"DataType="http://www.w3.org/2001/XMLSchema#string"
      Issuer="admin@users.example.com"> <AttributeValue>developers</AttributeValue>
      </Attribute>
  </Subject>
 <Resource>
   <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
      DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      <AttributeValue>http://server.example.com/code/docs/developer-
      guide.html</AttributeValue> </Attribute>
  </Resource>
  <Action> <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
      DataType="http://www.w3.org/2001/XMLSchema#string">
      <AttributeValue>read</AttributeValue> </Attribute>
  </Action>
</Request>
```

source: sunxacml.sourceforge.net/guide.html

A policy in XACML

```
<Policy PolicyId="ExamplePolicy"
     RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
     algorithm:permit-overrides">
<Target>
 <Subjects> <AnySubject/> </Subjects>
 <Resources> <Resource>
   <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">
     http://server.example.com/code/docs/developer-guide.html</AttributeValue>
       <ResourceAttributeDesignator
                  DataType="http://www.w3.org/2001/XMLSchema#anyURI"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"/>
   </ResourceMatch>
 </Resource></Resources>
<Actions> <AnyAction/> </Actions>
</Target>
...
```

source: sunxacml.sourceforge.net/guide.html

A policy in XACML (cont.)

```
...
 <Rule RuleId="ReadRule" Effect="Permit">
  <Target> <Subjects> <AnySubject/> </Subjects>
  <Resources> <AnyResource/> </Resources>
  <Actions> <Action>
    <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
       <AttributeValue DataType=“...#string">read</AttributeValue>
       <ActionAttributeDesignator
                               DataType="...#string" AttributeId="urn:...:action-id"/>
     </ActionMatch> </Action> </Actions>
  </Target>
  <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <Apply FunctionId="urn:...:function:string-one-and-only">
     <SubjectAttributeDesignator DataType=“...#string" AttributeId="group"/>
    </Apply>
    <AttributeValue DataType=“...#string">developers</AttributeValue>
  </Condition>
 </Rule>
</Policy>
```

source: sunxacml.sourceforge.net/guide.html

PDP responce in XACML

```
<Response>
  <Result>
    <Decision>Permit</Decision>
    <Status>
     <StatusCode
    Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
   </Status>
  </Result>
</Response>
```

source: sunxacml.sourceforge.net/guide.html

Translation into XACML

- Specify requirements as table
- Determine priorities to resolve conflicts
- Translate table rows to XACML rules
- Rule combining algorithm implements priorities
- Set Policy in Rule combining engine

Consent policy building blocks

- Grantor; the patient, a legal guardian
- Grantee; A personal doctor, hospital staff, anyone...
- Patient
- Action; read, write, disclose, amend, etc.
- Data; EHR, an XRay, Blood pressure measurements
- Effect; permit / deny.
- Situation description; Purpose, Context, Validity period

	grantor	grantee	patient	Action	data	Effect	Purpose	Context	Valid Period
	patient ID		patient ID	read	patient ID/*	-			
	patient ID		patient ID	write	patient ID/*	-			
	patient ID	personal doctor	patient ID	read	patient ID/*	+	treatment		
	patient ID	personal doctor	patient ID	read	patient ID/*	+	payment		
	patient ID	personal doctor	patient ID	read	patient ID/*	+	operations		
	patient ID	personal doctor	patient ID	read	patient ID/*	+	public health		
	patient ID	personal doctor	patient ID	read	patient ID/*	+	quality measures		
	patient ID	personal doctor	patient ID	write	patient ID/*	+	treatment		
	patient ID	personal doctor	patient ID	write	patient ID/*	+	payment		
	patient ID	personal doctor	patient ID	write	patient ID/*	+	operations		
	patient ID	personal doctor	patient ID	write	patient ID/*	+	public health		
	patient ID	personal doctor	patient ID	write	patient ID/*	+	quality measures		
	patient ID	doctor	patient ID	read	patient ID/*	+	treatment		1 year
	patient ID	doctor	patient ID	write	patient ID/*	+	treatment		1 year
	patient ID	Dr. John Mathews ID	patient ID	read	patient ID/*	+	treatment	emergency	
	patient ID	Dr. John Mathews ID	patient ID	write	patient ID/*	+	treatment	emergency	
	patient ID	Husband ID	patient ID	read	patient ID/*	+			
	patient ID	Mother ID	patient ID	read	patient ID/*	+			
	patient ID	Mother ID	patient ID	read	patient ID /Gynecological Information/*	-			
	patient ID	Mother ID	patient ID	read	patient ID /Blood pressure [age <= 3 months]	-			

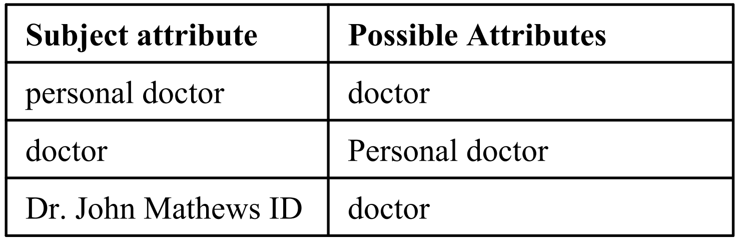
Table 1: Decision table for the working example patient consent policy

Conclusions

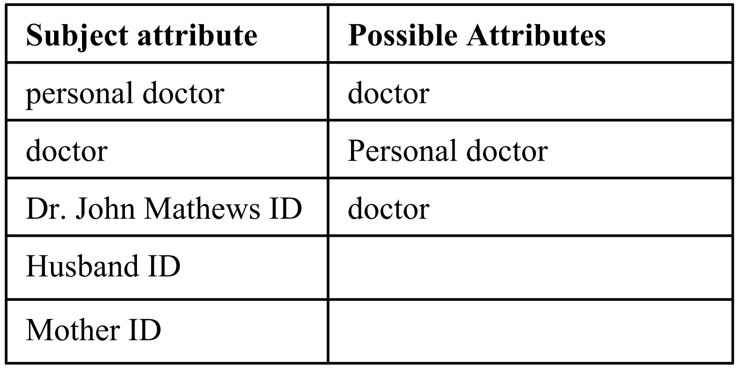
Assumptions

- Role relations known and fixed;
  - Expresses legal requirements & health care providers policies; relatively static.
  - E.g.
- Two disjoint groups;
  - Health care professionals
  - Other grantees
  - Distinction known, exceptions specified by patient

Conflict Detection



Subject attribute	Possible Attributes
personal doctor	doctor
doctor	Personal doctor
Dr. John Mathews ID	doctor

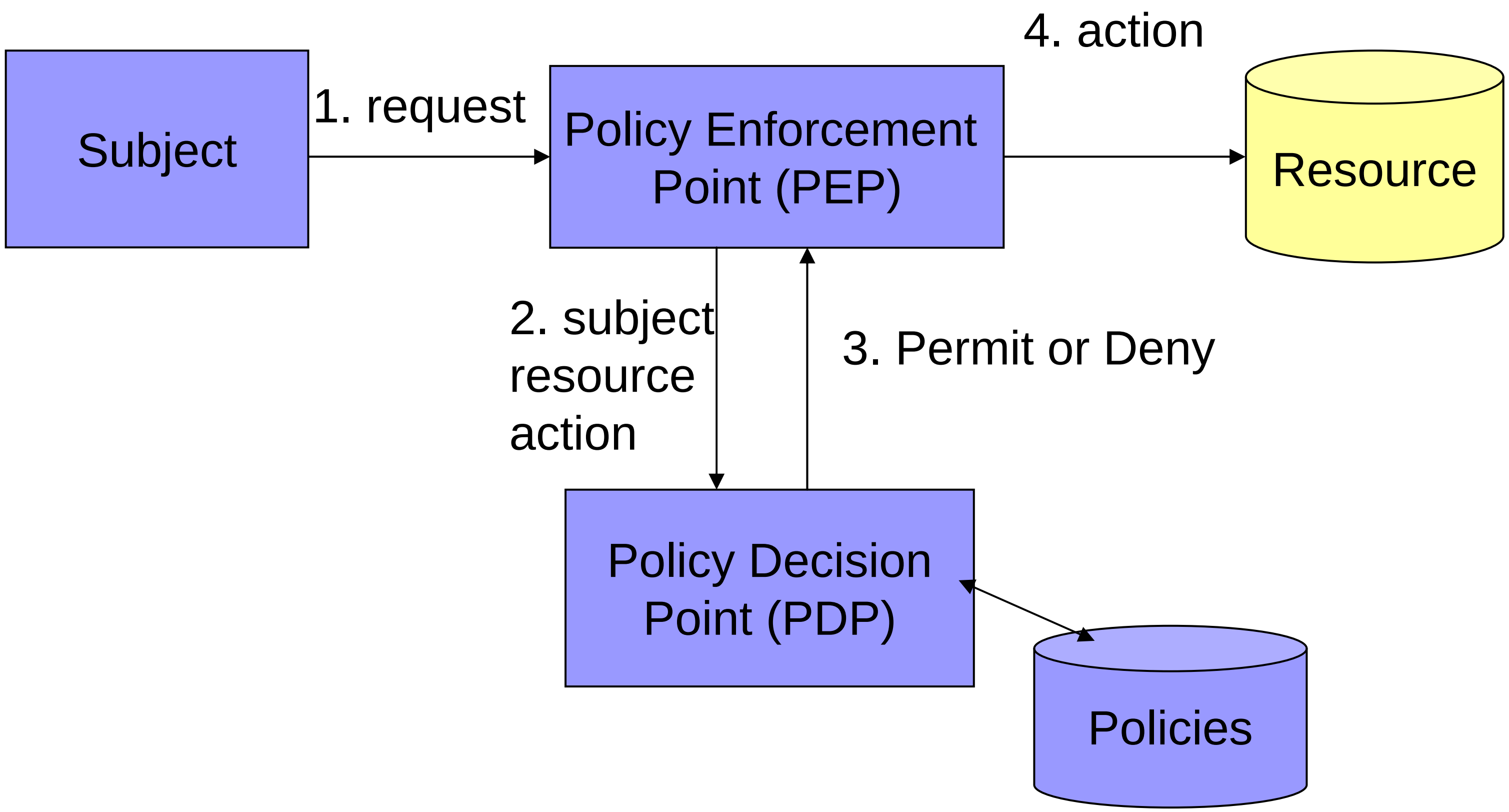


Subject attribute	Possible Attributes
personal doctor	doctor
doctor	Personal doctor
Dr. John Mathews ID	doctor
Husband ID	
Mother ID	

Authorization specification language

- cando(o, s, < sign > a) ← L1 & ………. & Ln
- cando(go, p, d, < sign > a, ge) ← L1 & ………. & Ln
- Straightforward translation from table row to rule
- Translation rule to XACML rule, list of rules to XACML policy
  - Rule combining engine uses priority of rules to obtain a conclusion.

XACML model (basic idea)


Subject
1. request
Policy Enforcement Point (PEP)
4. action
Resource
2. subject resource action
3. Permit or Deny
Policy Decision Point (PDP)
Policies