Sicherheitsmechanismen in serviceorientierten Architekturen Hauptseminar im SS 2009

Philip Daubmeier

May 29, 2009

Inhaltsverzeichnis

XACML bezogene OASIS Profile

- Vom OASIS Konsortium standardisiert
- Erweitern XACML um Zusatzfunktionalitäten

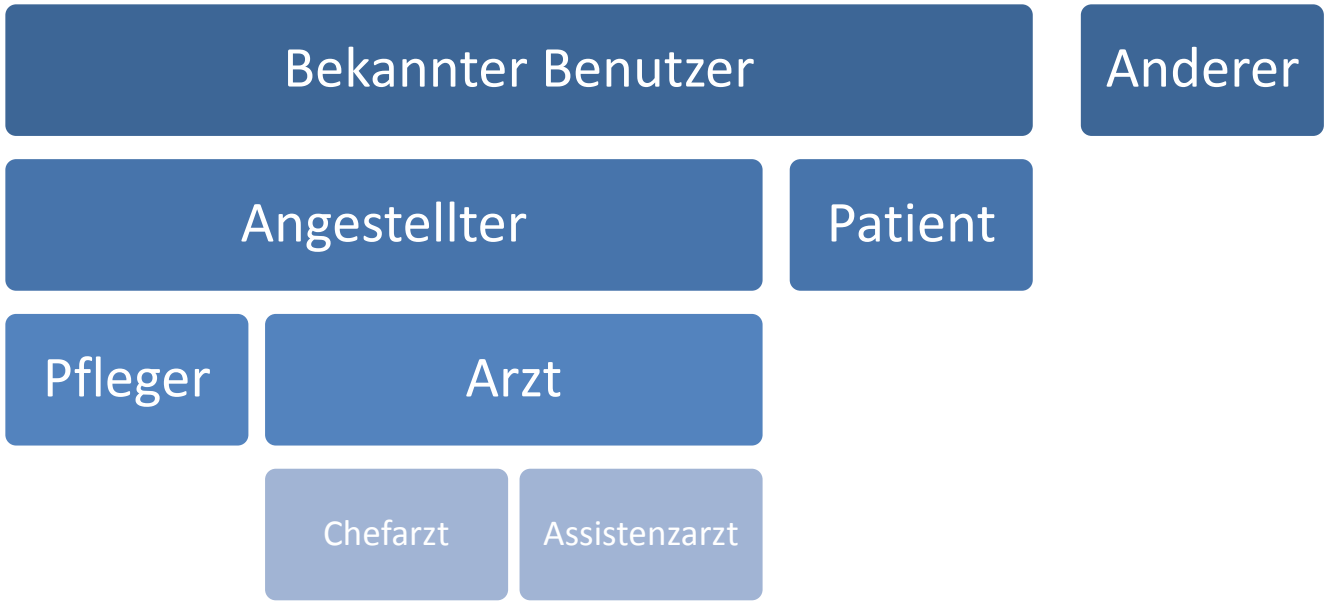
Übersicht

RBAC profile

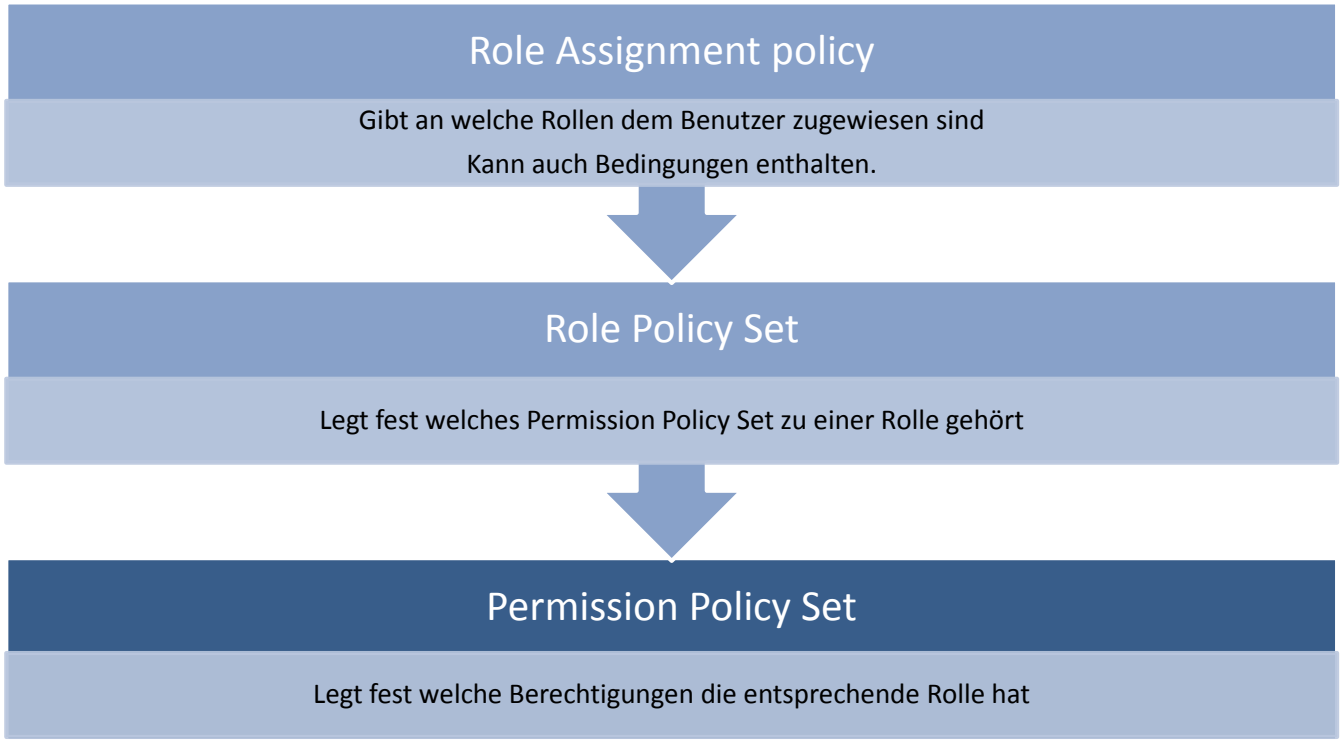
RBAC = role based access control

- Richtlinien (policies) können um Rollen erweitert werden
- Diese Rollen können hierarchisch aufeinander aufgebaut werden

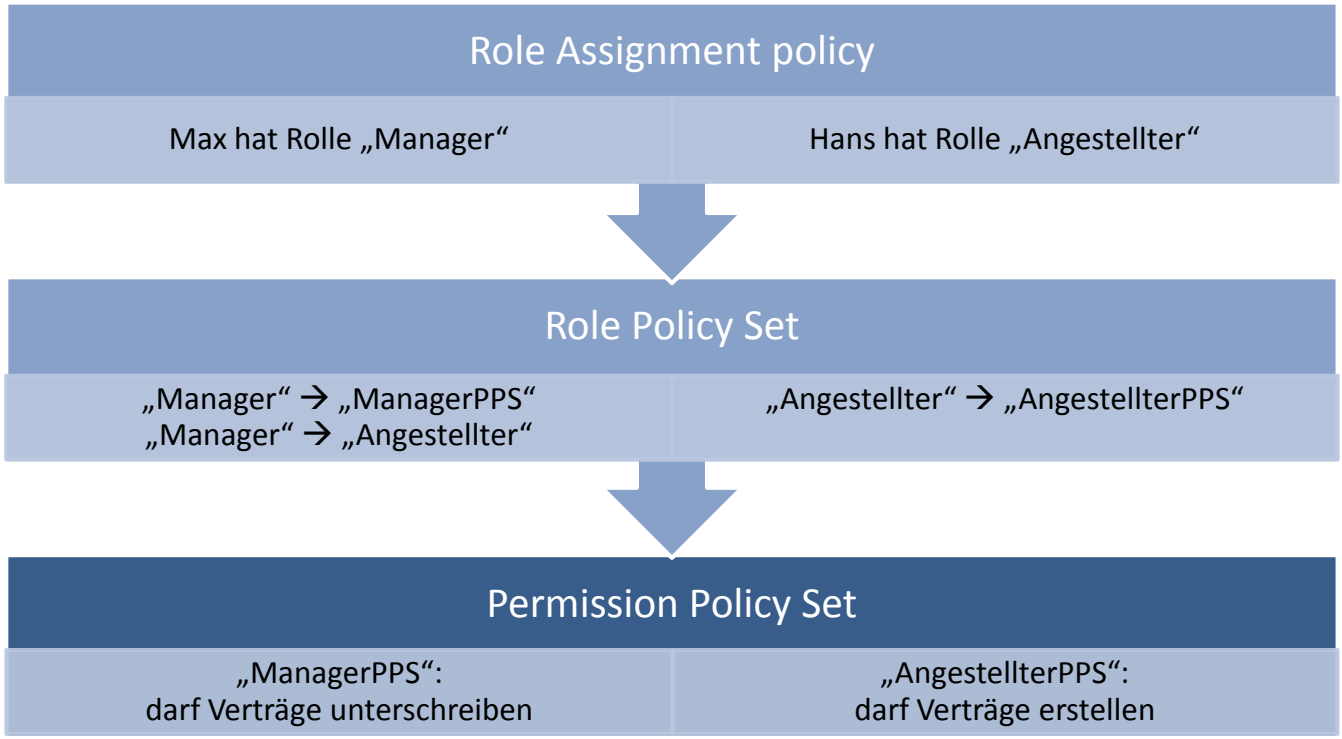
Hierarchie der Rollen



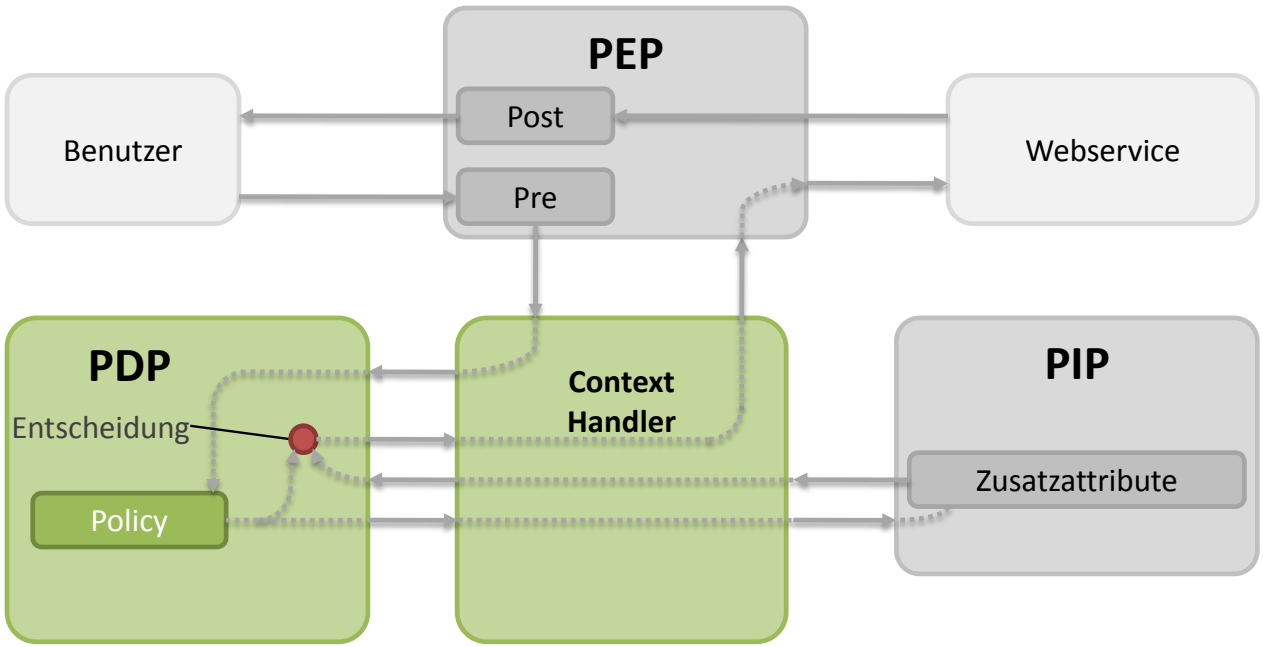
PolicySets


Role Assignment policy
Gibt an welche Rollen dem Benutzer zugewiesen sind
Kann auch Bedingungen enthalten.
Role Policy Set
Legt fest welches Permission Policy Set zu einer Rolle gehört
Permission Policy Set
Legt fest welche Berechtigungen die entsprechende Rolle hat

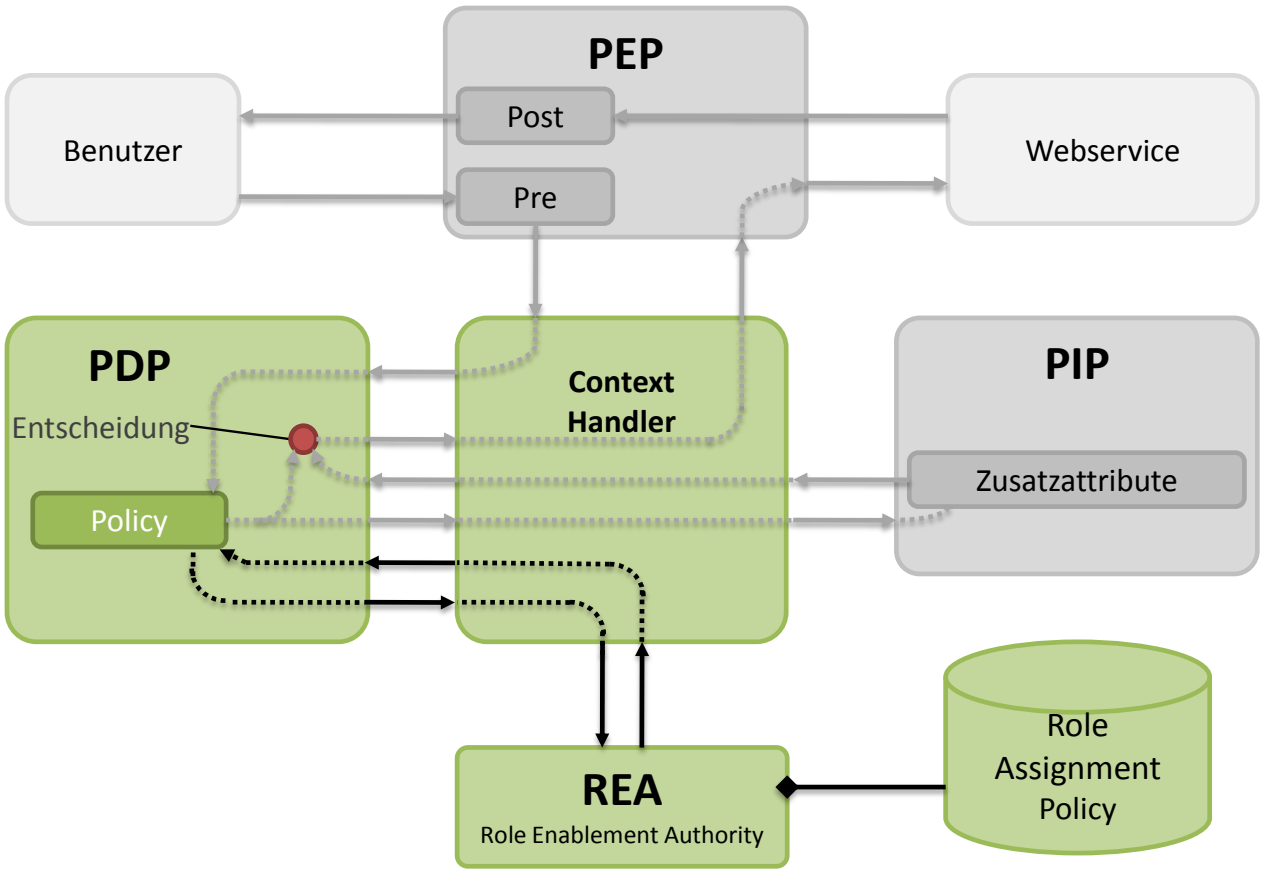
Beispiel


Role Assignment policy
Max hat Rolle „Manager“
Hans hat Rolle „Angestellter“
Role Policy Set
„Manager“ → „ManagerPPS“
„Manager“ → „Angestellter“
„Angestellter“ → „AngestellterPPS“
Permission Policy Set
„ManagerPPS“:
darf Verträge unterschreiben
„AngestellterPPS“:
darf Verträge erstellen

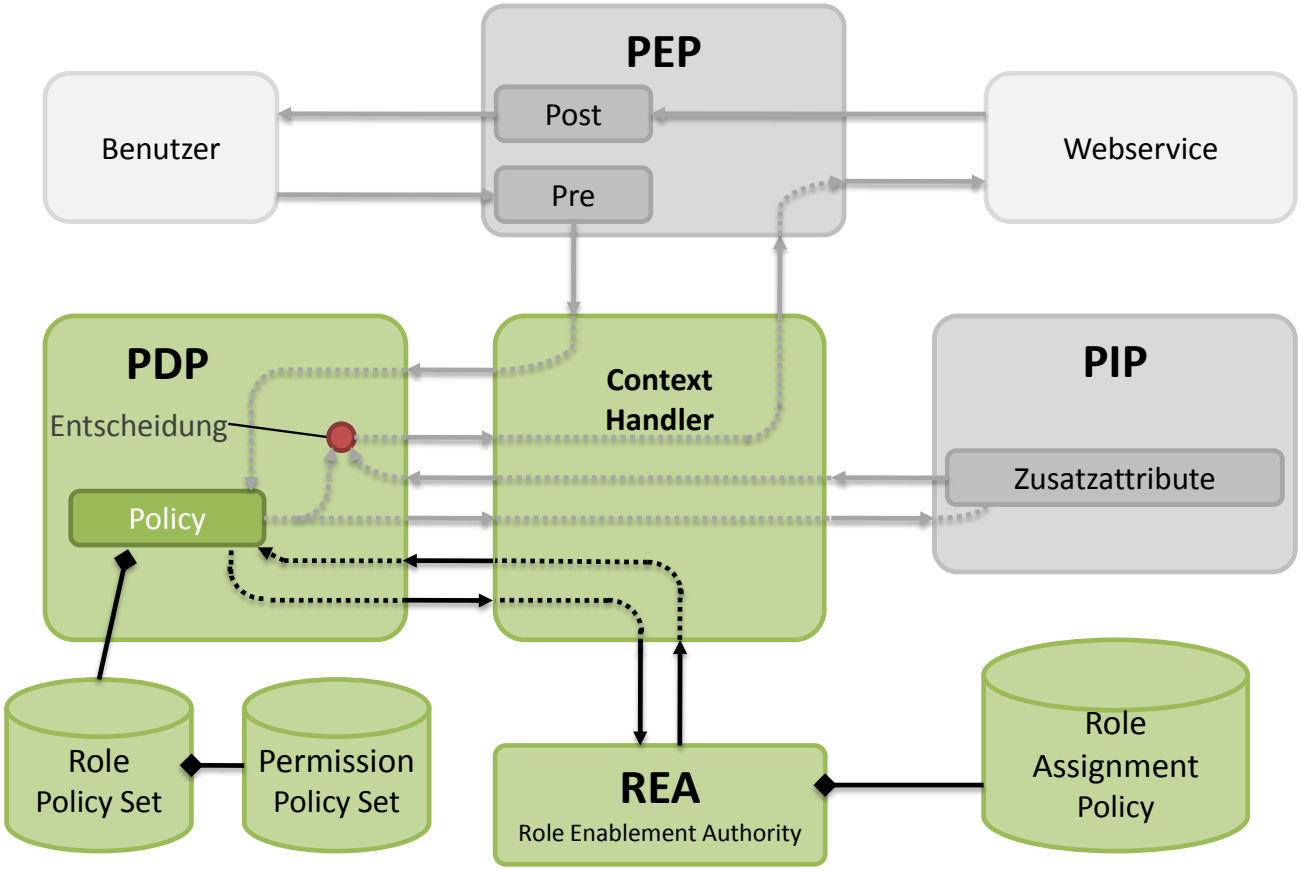
RBAC profile Aufbau



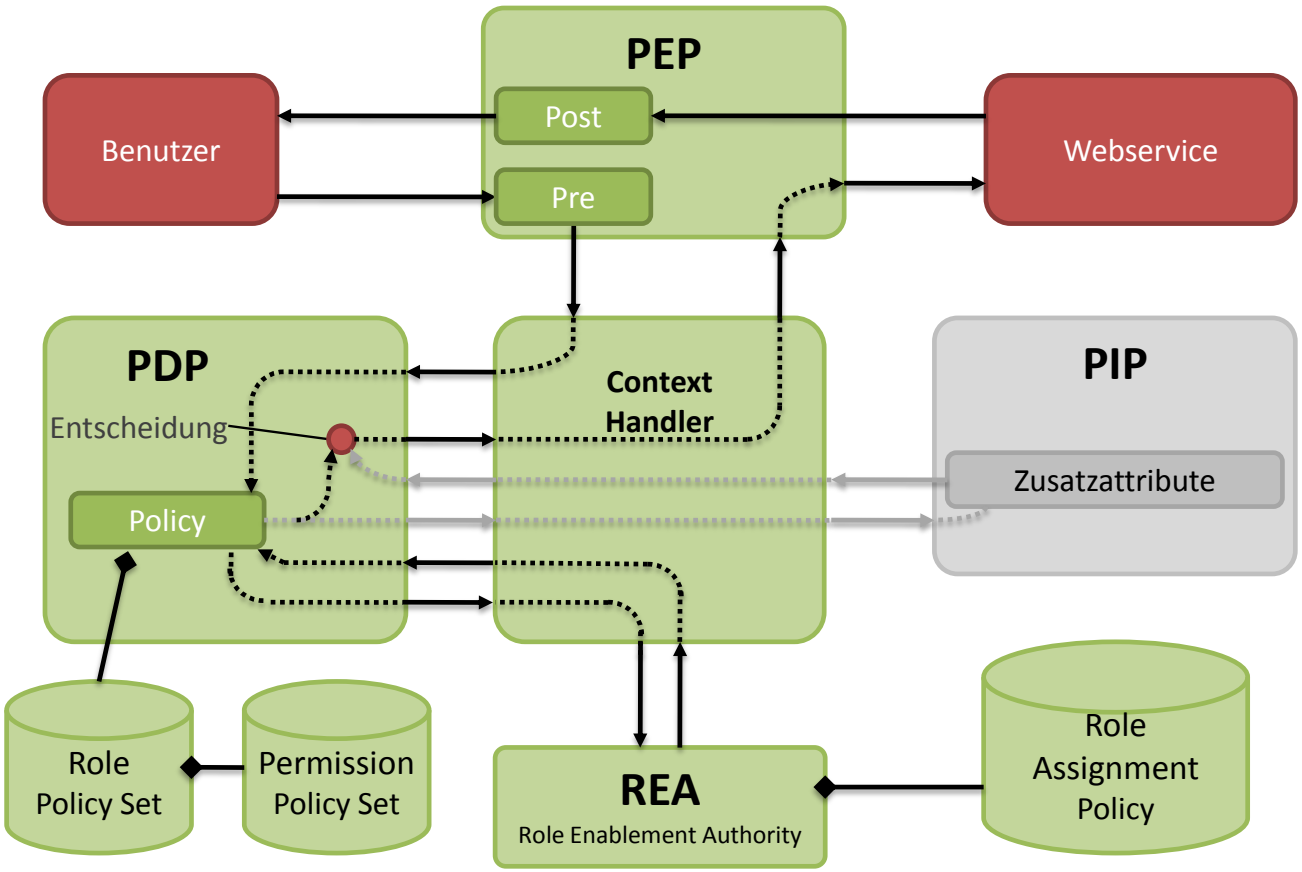
Role Enablement Authority



Role und Permission PolicySets



Datenfluss Gesamt



Beispiel für ein Role Assignment PolicySet

```
<Rule RuleId="manager:role:assignment Effect="Permit">
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch MatchId="&function;string-equal">
          <AttributeValue>Max</AttributeValue>
          <SubjectAttributeDesignator AttributeId="&subject;subject-id"/>
        </SubjectMatch>
      </Subject>
    </Subjects>
    <Resources>
      <Resource>
        <ResourceMatch MatchId="&function;anyURI-equal">
          <AttributeValue>&roles;manager</AttributeValue>
          <ResourceAttributeDesignator AttributeId="&role;"/>
        </ResourceMatch>
      </Resource>
    </Resources>
    <Actions>
      <Action>
        <ActionMatch MatchId="&function;anyURI-equal">
          <AttributeValue>&actions;enableRole</AttributeValue>
          <ActionAttributeDesignator AttributeId="&action;action-id"/>
        </ActionMatch>
      </Action>
    </Actions>
  </Target>
</Rule>
```

Beispiel für ein Role PolicySet

```
<PolicySet xmlns="urn:...:policy:schema:os" PolicySetId="RPS:manager:role"
  PolicyCombiningAlgId="&policy-combine;permit-overrides">
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch MatchId="&function;anyURI-equal">
          <AttributeValue>&roles;manager</AttributeValue>
          <SubjectAttributeDesignator AttributeId="&role;"/>
        </SubjectMatch>
      </Subject>
    </Subjects>
  </Target>

  <!-- Weise der Rolle "Manager" die Rechte aus dem Manager PPS zu  -->
  <PolicySetIdReference>PPS:manager:role</PolicySetIdReference>
</PolicySet>
```

Beispiel für ein Permission PolicySet

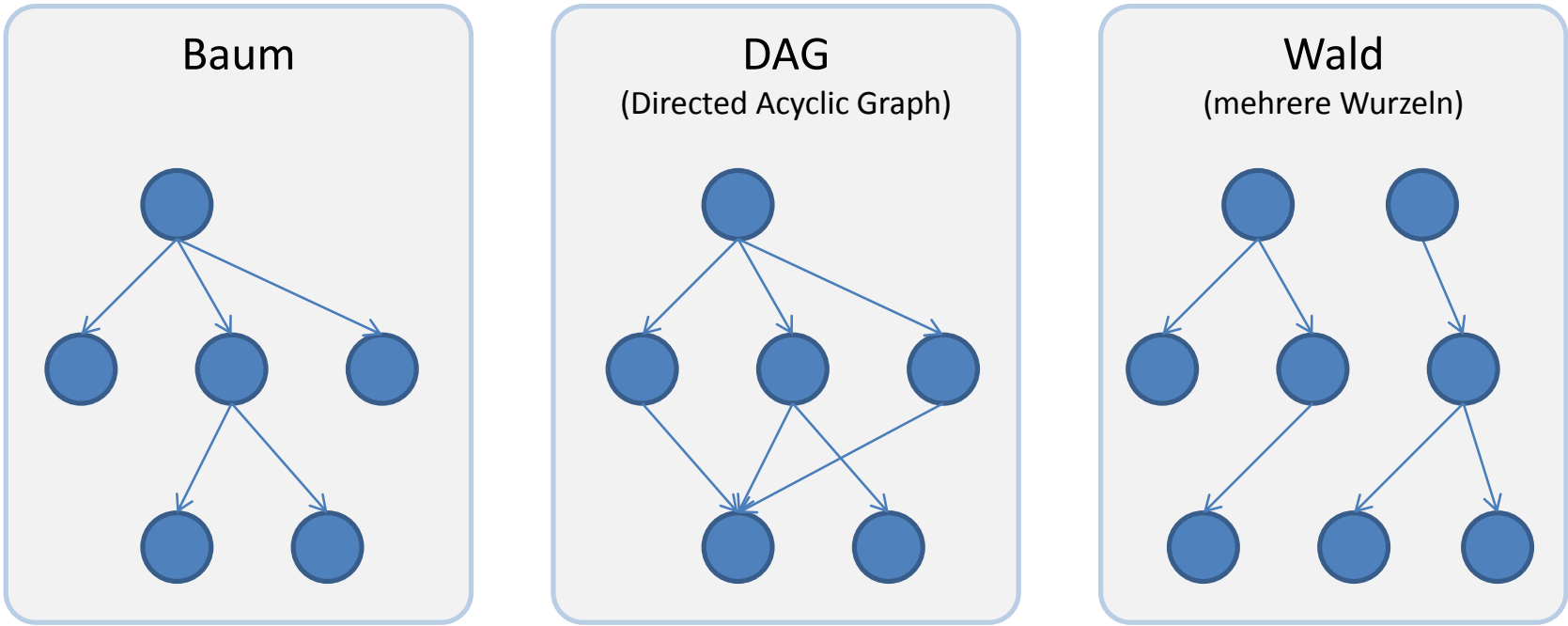
```
<PolicySet xmlns="urn:...:policy:schema:os" PolicySetId="PPS:manager:role"
  PolicyCombiningAlgId="&policy-combine;permit-overrides">
  <Policy PolicyId="Permissions:manager:role"
    RuleCombiningAlgId="&rule-combine;permit-overrides">
    <Rule RuleId="Permission:to:sign:a:purchase:order" Effect="Permit">
      <Target>
        <Resources>
          <Resource>
            <ResourceMatch MatchId="&function;string-equal">
              <AttributeValue>contract</AttributeValue>
              <ResourceAttributeDesignator AttributeId="&resource;resource-id"/>
            </ResourceMatch>
          </Resource>
        </Resources>
        <Actions>
          <Action>
            <ActionMatch MatchId="&function;string-equal">
              <AttributeValue>sign</AttributeValue>
              <ActionAttributeDesignator AttributeId="&action;action-id"/>
            </ActionMatch>
          </Action>
        </Actions>
      </Target>
    </Rule>
  </Policy>

  <!-- Manager hat auch alle Rechte eines Angestellten -->
  <PolicySetIdReference>PPS:employee:role</PolicySetIdReference>
</PolicySet>
```

Übersicht

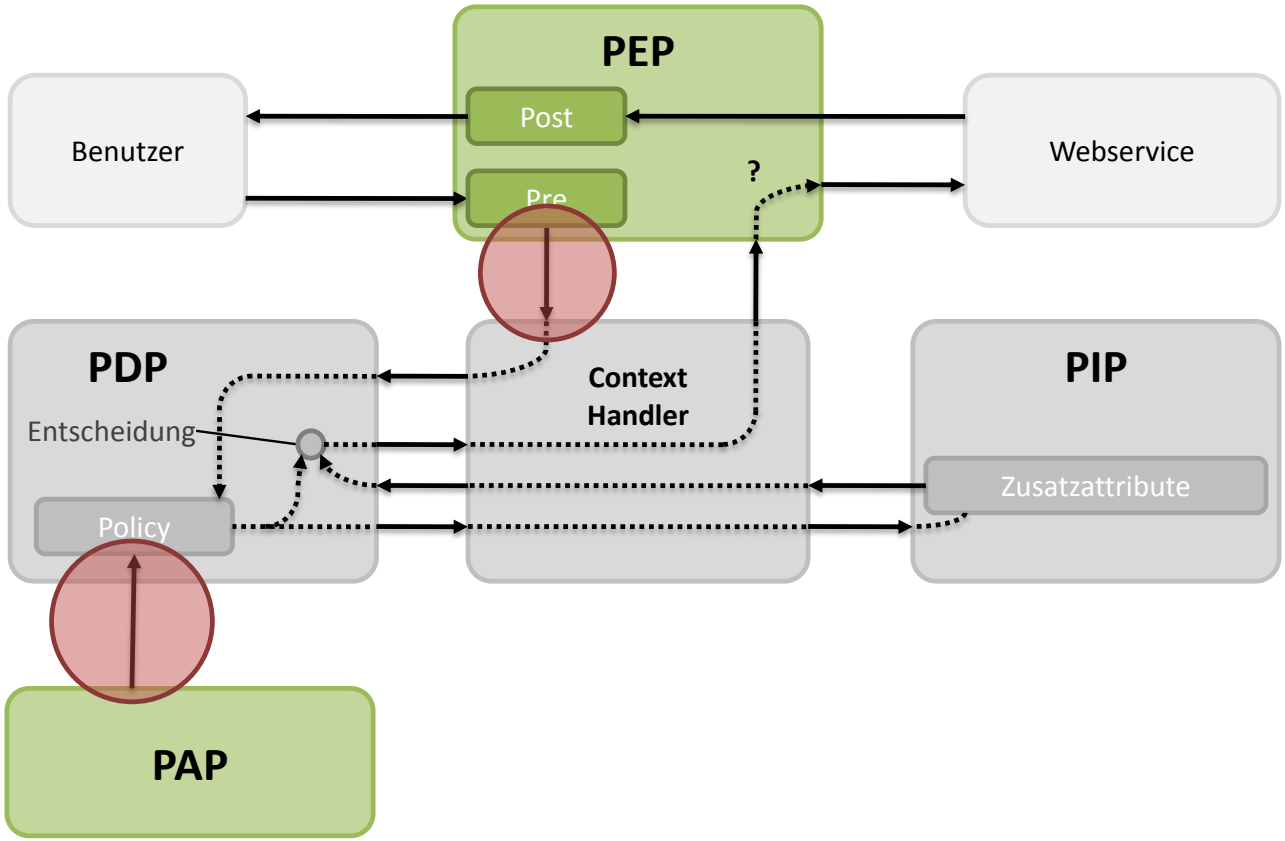
Hierarchical ressource profile

- Anfragen für Ressourcen hierarchischer Form
  - Dateisystem
  - XML Dokumente
  - Organisationsstrukturen
- Auch hierarchische nicht-Baum Strukturen

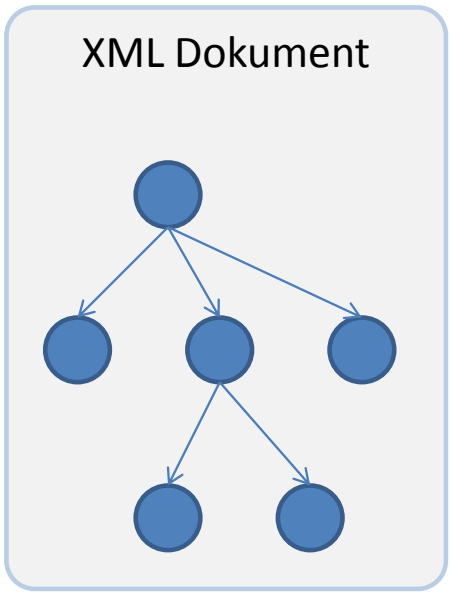
Hierarchische Strukturen



Policy muss mit decision reqest matchen

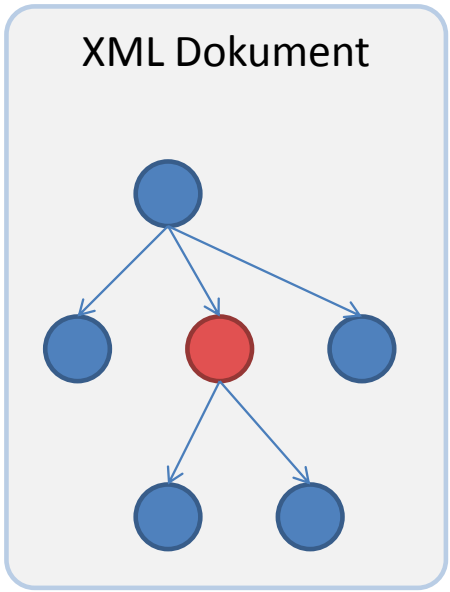


Beispiel



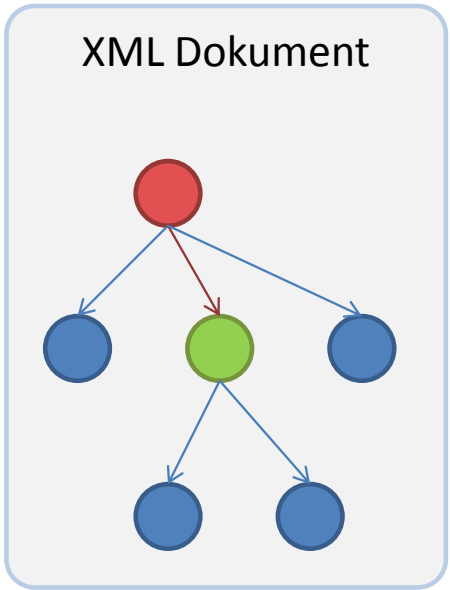

```
<Request>
  <Action><!-- Eine Action --></Action>
  <Subject><!-- Ein Subject --></Subject>
  <Resource>
    <ResourceContent>
      <ExampleRoot>
        <ExampleNode/>
        <ExampleNode>
          <ExampleNode/>
          <ExampleNode/>
        </ExampleNode>
        <ExampleNode/>
      </ExampleRoot>
    </ResourceContent>
    <!-- ... -->
  </Resource>
</Request>
```

Beispiel



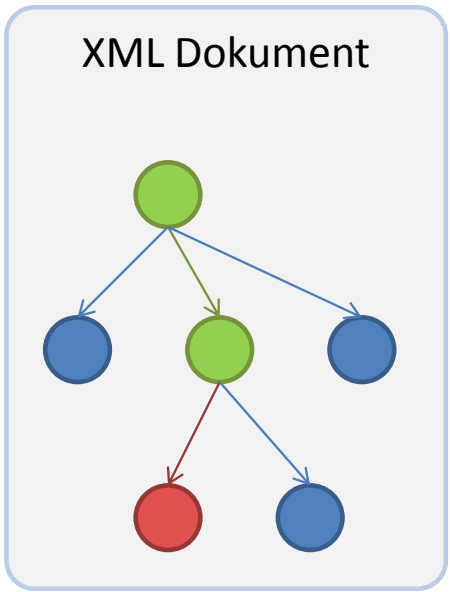

```
<Request>
  <Action><!-- Eine Action --></Action>
  <Subject><!-- Ein Subject --></Subject>
  <Resource>
    <ResourceContent>
      <!-- Das XML Dokument -->
    </ResourceContent>
    <Attribute AttributeId="urn:...:resource-id">
      <AttributeValue>/Request[1]/Resource[1]/ResourceContent[1]/
        ExampleRoot[1]/ExampleNode[2]</AttributeValue>
    </Attribute>
    <!-- ... -->
  </Resource>
</Request>
```

Beispiel




```
<Request>
  <Action><!-- Eine Action --></Action>
  <Subject><!-- Ein Subject --></Subject>
  <Resource>
    <ResourceContent>
      <!-- Das XML Dokument -->
    </ResourceContent>
    <Attribute AttributeId="urn:...:resource-id">
      <AttributeValue>/Request[1]/Resource[1]/ResourceContent[1]/
        ExampleRoot[1]/ExampleNode[2]</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:...:resource-parent">
      <AttributeValue>/Request[1]/Resource[1]/ResourceContent[1]/
        ExampleRoot[1]/</AttributeValue>
    </Attribute>
    <!-- ... -->
  </Resource>
</Request>
```

Beispiel




```
<Request>
  <Action><!-- Eine Action --></Action>
  <Subject><!-- Ein Subject --></Subject>
  <Resource>
    <ResourceContent>
      <!-- Das XML Dokument -->
    </ResourceContent>
    <Attribute AttributeId="urn:...:resource-id">
      <AttributeValue>/Request[1]/Resource[1]/ResourceContent[1]/
        ExampleRoot[1]/ExampleNode[2]</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:...:resource-parent">
      <AttributeValue>/Request[1]/Resource[1]/ResourceContent[1]/
        ExampleRoot[1]/</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:...:resource-ancestor">
      <AttributeValue>/Request[1]/Resource[1]/ResourceContent[1]/
        ExampleRoot[1]/ExampleNode[2]/ExampleNode[1]
      </AttributeValue>
    </Attribute>
  </Resource>
</Request>
```

Übersicht

Multiple ressource profile

Das Multiple ressource profile erlaubt

- eine Decision Request für mehrere Ressourcen zu formulieren
- dadurch feingranularere Entscheidungen

Ausserdem: Einige Regeln lassen sich nur auf einzelne Datensätze anwenden, nicht auf ganze Bags.

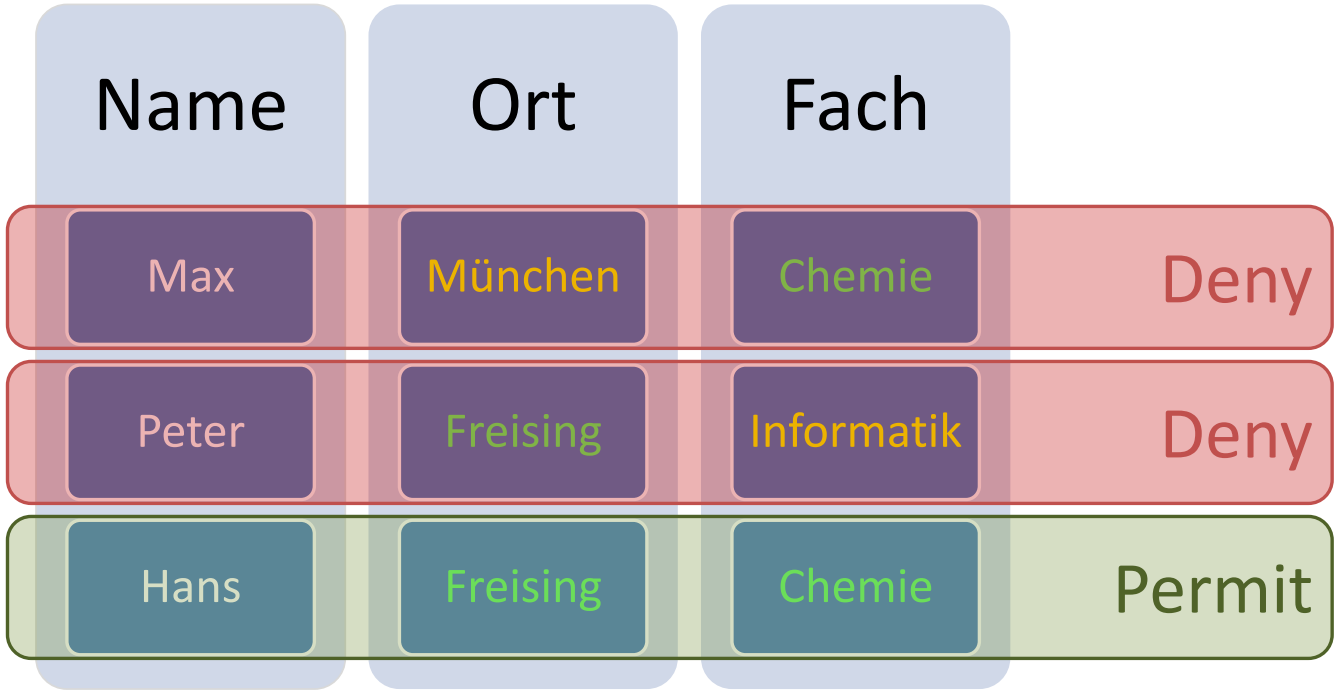
Problematik ohne Multiple ressource profile

Die Regel *"darf nur Informatiker aus München und Chemiker aus Freising sehen"* lässt sich nicht auf Bags von Studenten anwenden:

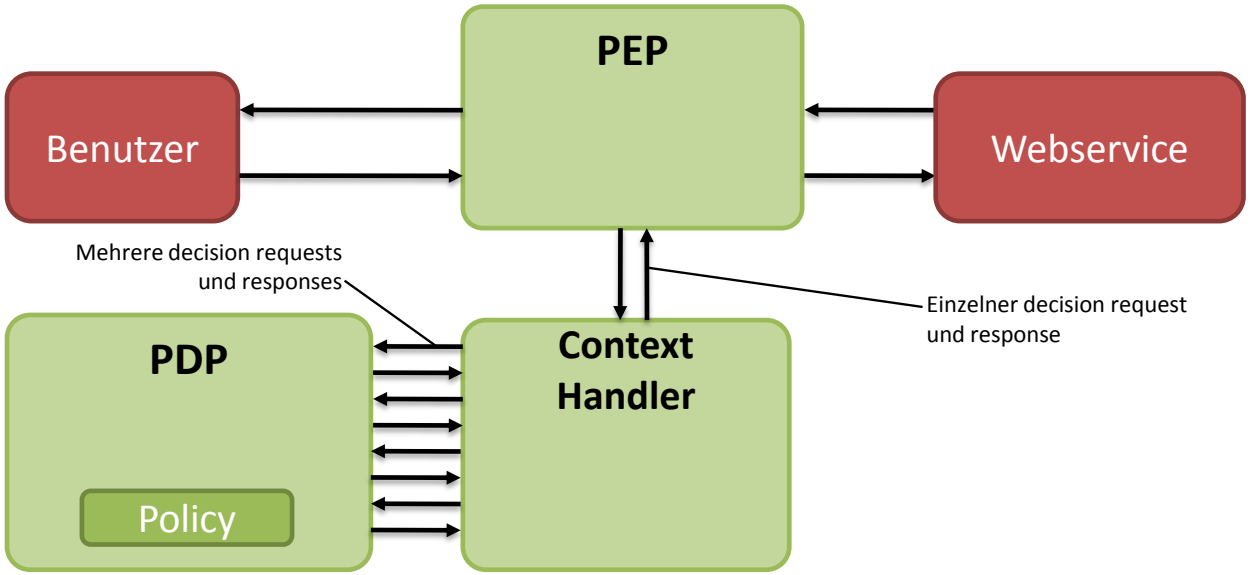
Name	Ort	Fach
Max	München	Chemie
Peter	Freising	Informatik
Hans	Freising	Chemie

Problematik ohne Multiple ressource profile

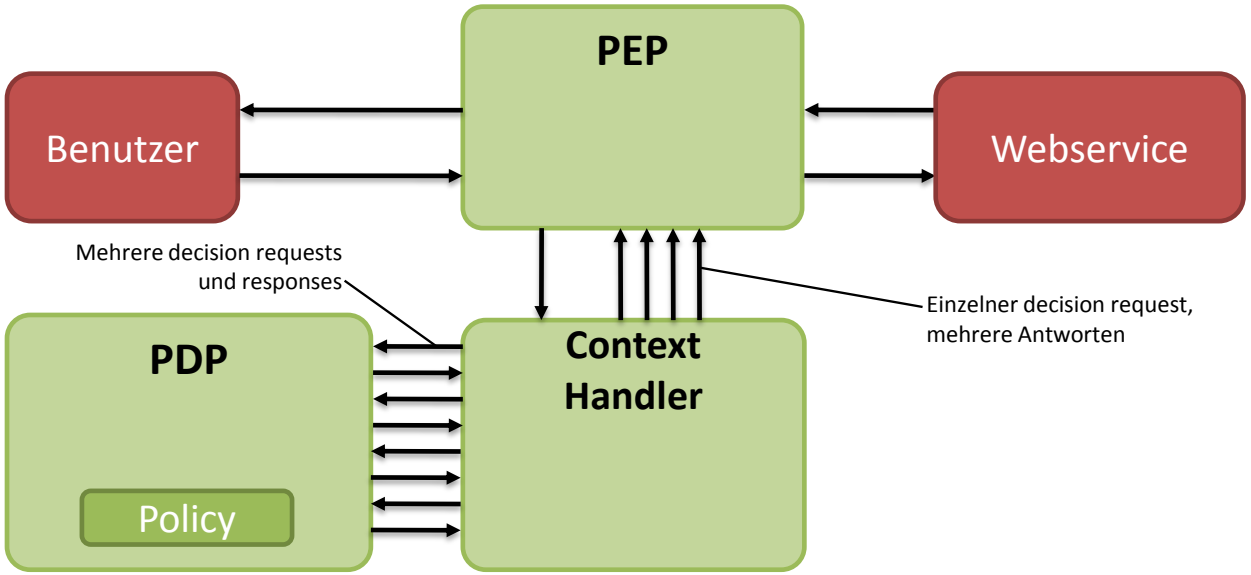
Dagegen liefert eine Anwendung der Regel auf jeden einzelnen Datensatz das gültige Ergebnis.



Eine Anfrage, eine Antwort



Eine Anfrage, mehrere Antworten



Anfrage an den Webservice

```
<?xml version="1.0"?>
<sample:GetStudents service="UniDB">
  <sample:Query>
    <sample:Filter><!-- studiert Informatik --></sample:Filter>
    <sample:Filter><!-- wohnt in München --></sample:Filter>
  </sample:Query>
</sample:GetStudents>
```

Antwort des Webservice

```
<ws:StudentCollection>
  <ws:Student>
    <ws:Name>Max</ws:Name>
    <ws:Wohnort>München</ws:Wohnort>
    <ws:Studium>Chemie</ws:Studium>
  </ws:Student>
  <ws:Student>
    <ws:Name>Peter</ws:Name>
    <ws:Wohnort>Freising</ws:Wohnort>
    <ws:Studium>Informatik</ws:Studium>
  </ws:Student>
  <ws:Student>
    <ws:Name>Hans</ws:Name>
    <ws:Wohnort>Freising</ws:Wohnort>
    <ws:Studium>Chemie</ws:Studium>
  </ws:Student>
</ws:StudentCollection>
```

Global access control desicion request

```
<Request>
  <Subject>
    <Attribute AttributeId="urn:...:xacml:2.0:subject:role" DataType="string">
      <AttributeValue>Mitarbeiter</AttributeValue>
    </Attribute>
  </Subject>
  <Resource>
    <ResourceContent><!-- die Webservice Antwort --></ResourceContent>
    <Attribute AttributeId="urn:...:xacml:2.0:resource:resource-id" DataType="xpath-expression">
      <AttributeValue>/Request[1]/Resource[1]/ResourceContent[1]/
      ws:StudentCollection[1]</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:...:xacml:2.0:resource:scope:xml" DataType="string">
      <AttributeValue>Descendants</AttributeValue>
    </Attribute>
  </Resource>
  <Action>
    <Attribute AttributeId="urn:...:xacml:2.0:action:action-id" DataType="string">
      <AttributeValue>GetStudent</AttributeValue>
    </Attribute>
  </Action>
</Request>
```

Access control desicion request

```
<Request>
  <Subject>
    <Attribute AttributeId="urn:...:xacml:2.0:subject:role" DataType="string">
      <AttributeValue>Mitarbeiter</AttributeValue>
    </Attribute>
  </Subject>
  <Resource>
    <ResourceContent><!-- die Webservice Antwort --></ResourceContent>
    <Attribute AttributeId="urn:...:xacml:2.0:resource:resource-id" DataType="xpath-expression">
      <AttributeValue>/Request[1]/Resource[1]/ResourceContent[1]/
      ws:StudentCollection[1]/ws:Student[1]</AttributeValue>
    </Attribute>
    <!-- Keine Angabe über Scope mehr, da sich diese Anfrage nur noch auf einen Knoten bezieht -->
    <Attribute AttributeId="urn:unidb-example:wohnort" DataType="string">
      <AttributeValue>München</AttributeValue>
    </Attribute>
    <Attribute AttributeId="urn:unidb-example:studium" DataType="string">
      <AttributeValue>Informatik</AttributeValue>
    </Attribute>
  </Resource>
  <Action>
    <Attribute AttributeId="urn:...:xacml:2.0:action:action-id" DataType="string">
      <AttributeValue>GetStudent</AttributeValue>
    </Attribute>
  </Action>
</Request>
```

Rule

```
<Rule RuleId="SelectStudentsRule" Effect="Permit">
  <Target>
    <Subject>
      <SubjectMatch MatchId="string-equal">
        <AttributeValue DataType="string">Mitarbeiter</AttributeValue>
        <SubjectAttributeDesignator DataType="string" AttributeId="urn:...:role"/>
      </SubjectMatch>
    </Subject>
    <Resource>
      <ResourceMatch MatchId="regexp-string-match">
        <AttributeValue DataType="string">
          /Request/Resource/ResourceContent/ws:StudentCollection\[\d+\]/ws:Student\[\d+\]
        </AttributeValue>
        <ResourceAttributeDesignator DataType="string" AttributeId="urn:...:resource-id"/>
      </ResourceMatch>
      <ResourceMatch MatchId="string-equal">
        <AttributeValue DataType="string">München</AttributeValue>
        <ResourceAttributeDesignator DataType="string" AttributeId="urn:unidb-example:wohnort"/>
      </ResourceMatch>
      <ResourceMatch MatchId="string-equal">
        <AttributeValue DataType="string">Informatik</AttributeValue>
        <ResourceAttributeDesignator DataType="string" AttributeId="urn:unidb-example:studium"/>
      </ResourceMatch>
    </Resource>
    <Action>
      <ActionMatch MatchId="string-equal">
        <AttributeValue DataType="string">GetStudents</AttributeValue>
        <ActionAttributeDesignator DataType="string" AttributeId="urn:...:action-id"/>
      </ActionMatch>
    </Action>
  </Target>
</Rule>
```

Vielen Dank für die Aufmerksamkeit!