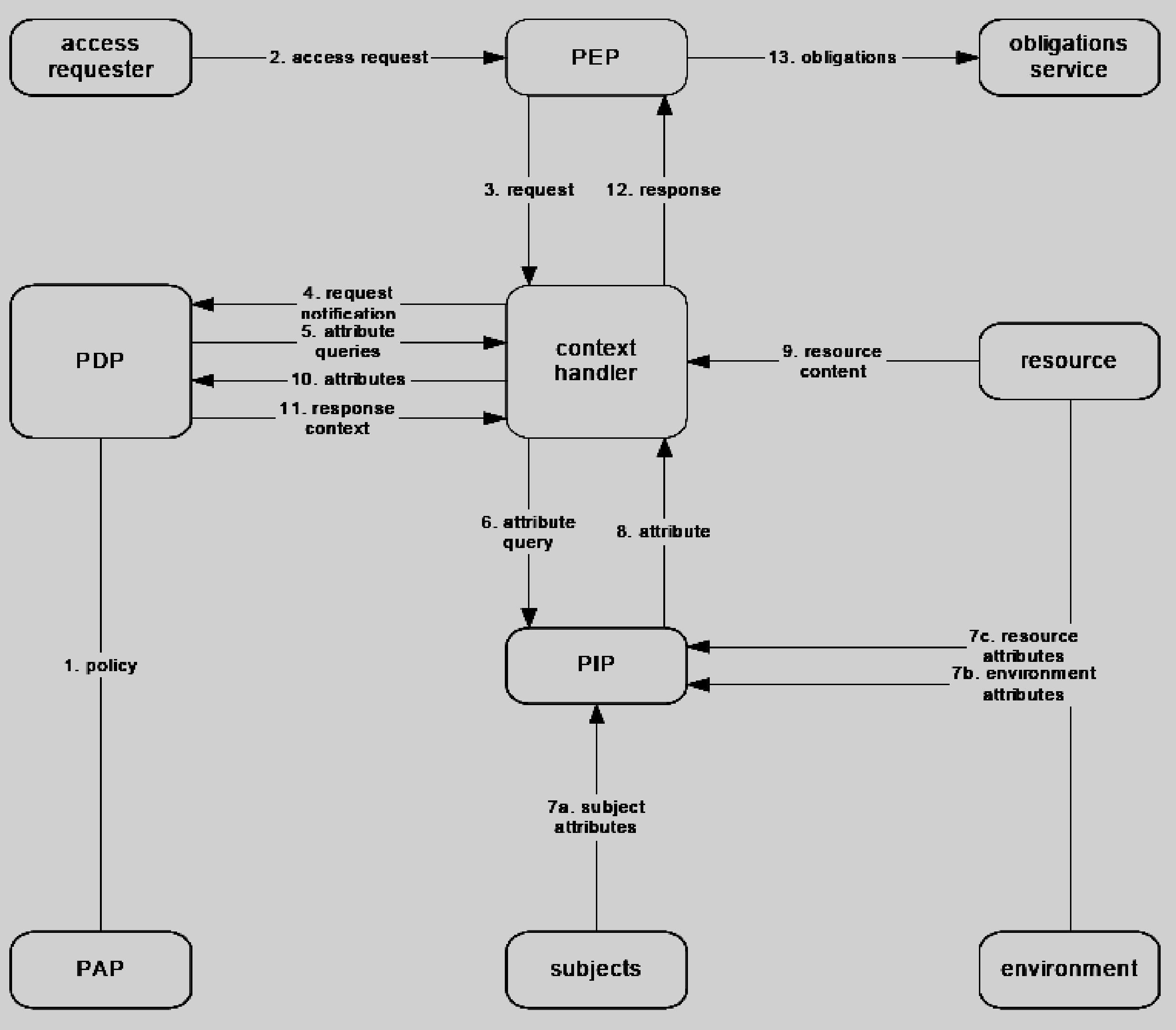
Authorization

- Determining whether to permit or deny a requested action

- Critical questions:
  - What is the model of the authorization system?
  - What languages are used to represent the policy by which decisions are made?

Dataflow Model

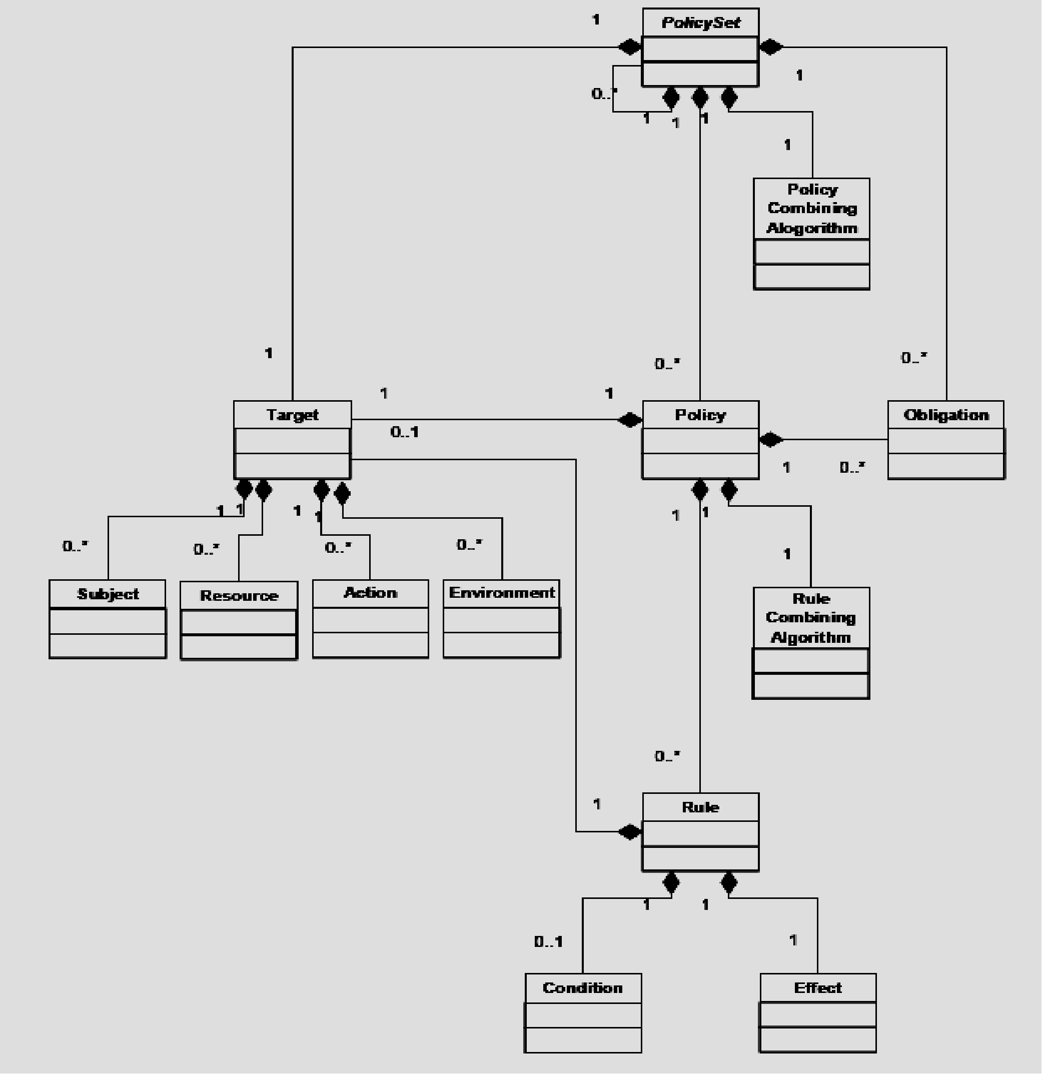


From: OASIS XACML Specification

Request and Response Context

- Request Context
  - Attributes of:
    - Subjects – requester, intermediary, recipient, etc.
    - Resource – name, can be hierarchical
    - Resource Content – specific to resource type, e.g. XML document
    - Action – e.g. Read
    - Environment – other, e.g. time of request
- Response Context
  - Resource ID
  - Decision
  - Status (error values)
  - Obligations

Language Model (UML)

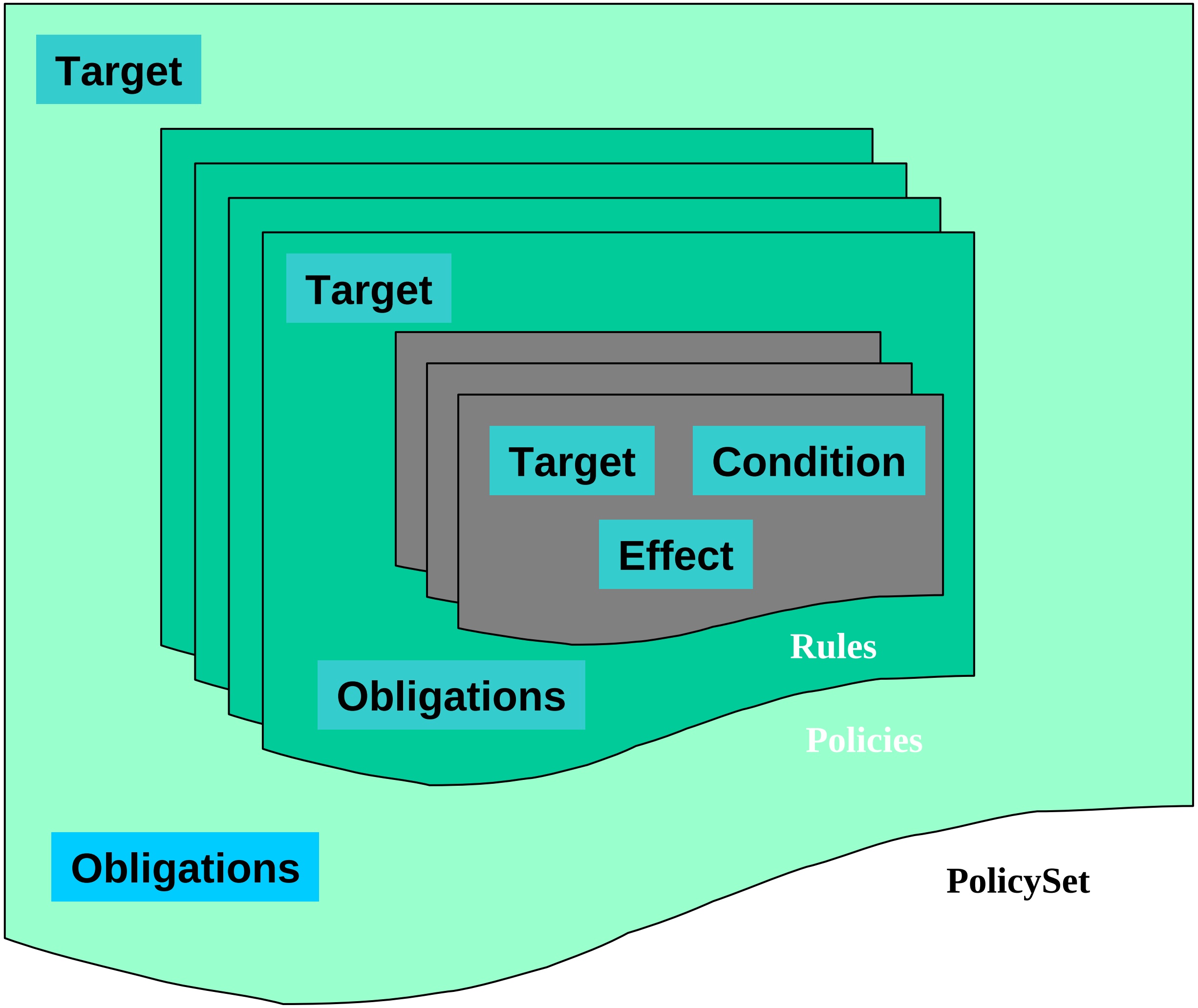


From: OASIS XACML Specification

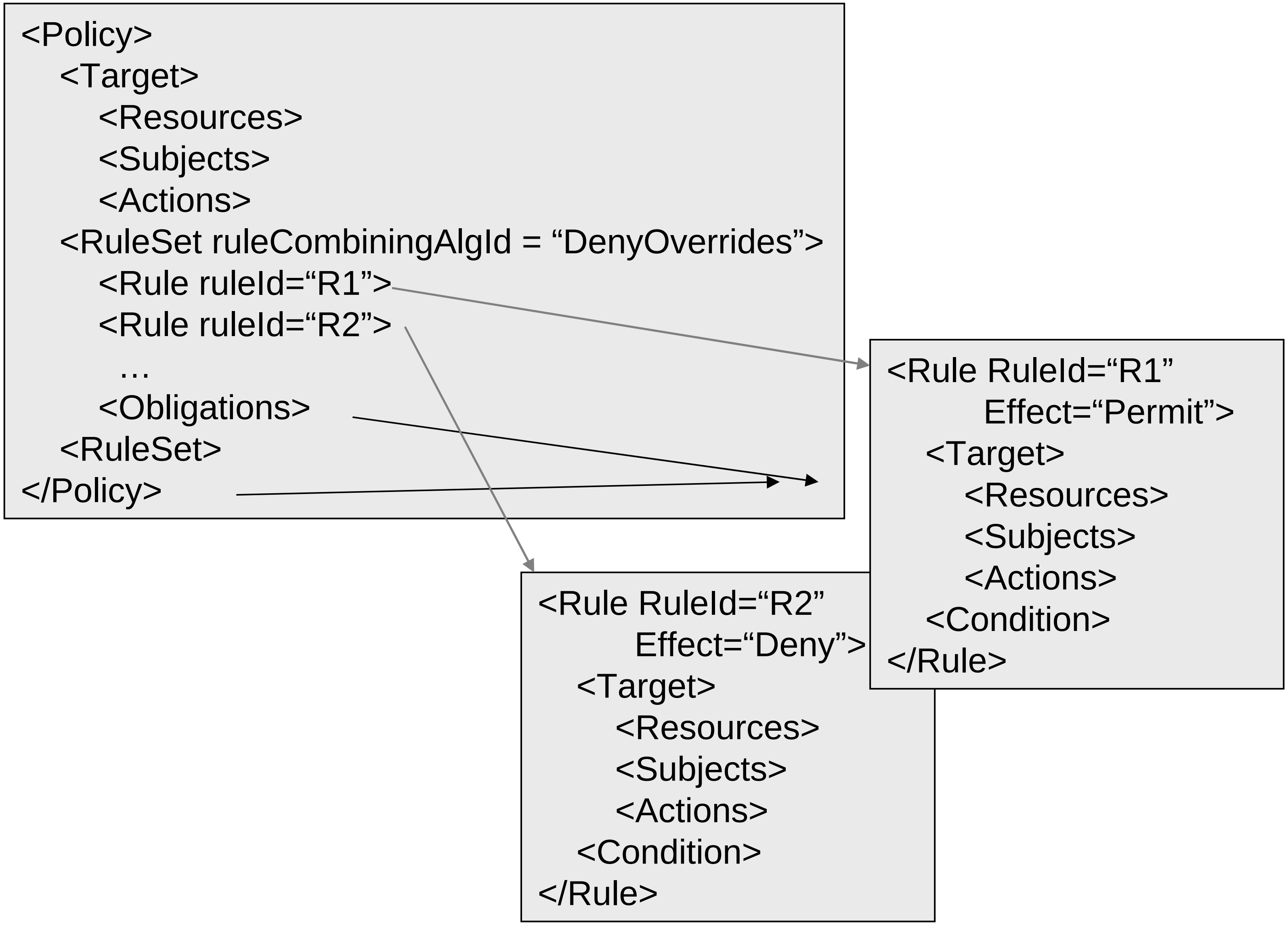
Policies and Policy Sets

- Policy
  - Smallest element PDP can evaluate
  - Contains: Description, Defaults, Target, Rules, Obligations, Rule Combining Algorithm
- Policy Set
  - Allows Policies and Policy Sets to be combined
  - Use not required
  - Contains: Description, Defaults, Target, Policies, Policy Sets, Policy References, Policy Set References, Obligations, Policy Combining Algorithm
- Combining Algorithms: Deny-overrides, Permit-overrides, First-applicable, Only-one-applicable

Language Model (Graphical)



Language Model (XML)



```
<Policy>
    <Target>
        <Resources>
        <Subjects>
        <Actions>
    <RuleSet ruleCombiningAlgId = “DenyOverrides”>
        <Rule ruleId=“R1”>
        <Rule ruleId=“R2”>
          …
        <Obligations>
    <RuleSet>
</Policy>
```

```
<Rule RuleId=“R1”
          Effect=“Permit”>
    <Target>
        <Resources>
        <Subjects>
        <Actions>
    <Condition>
</Rule>
```

```
<Rule RuleId=“R2”
          Effect=“Deny”>
    <Target>
        <Resources>
        <Subjects>
        <Actions>
    <Condition>
</Rule>
```

Example Request

```
<Request …>
    <Subject>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
          DataType="http://www.w3.org/2001/XMLSchema#string">
            <AttributeValue>
                John
            </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>
                Door
            </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>
                open
           </AttributeValue>
       </Attribute> </Action>
</Request>
```

Rules

- Smallest unit of administration, cannot be evaluated alone
- Elements
  - Description – documentation
  - Target – select applicable policies
  - Condition – boolean decision function
  - Effect – either “Permit” or “Deny”
- Results
  - If condition is true, return Effect value
  - If not, return NotApplicable
  - If error or missing data return Indeterminate
    - Plus status code

Targets

- Designed to efficiently find the elements (policies, rules) that apply to a request
- Makes it feasible to have very complex Conditions
- Attributes of Subjects, Resources and Actions
- Matches against value, using match function
  - Regular expression
  - RFC822 (email) name
  - X.500 name
  - User defined
- Attributes specified by Id or XPath expression

Example Rule

```
  Rule RuleId=“Door Control Rule" Effect="Permit">
     <Target>
          <Subjects> <Subject>
               <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                         John
                    </AttributeValue>
                    <SubjectAttributeDesignator
                          AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                          DataType="http://www.w3.org/2001/XMLSchema#string"/>
               </SubjectMatch> </Subject> </Subjects>
            Resources> <Resource>
               <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">
                         Door
                    </AttributeValue>
                   <ResourceAttributeDesignator
                        AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                        DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
              </ResourceMatch>

          <Actions> <Action>
                <AnyAction/>
           </Action> </Actions>
     </Target>
</Rule>
```

Example Response

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

Conditions

- Boolean function to decide if Effect applies
- Inputs come from Request Context
- Values can be primitive, complex or bags
- Can be specified by id or XPath expression
- Fourteen primitive types
- Rich array of typed functions defined
- Functions for dealing with bags
- Order of evaluation unspecified
- Allowed to quit when result is known
- Side effects not permitted

Example Condition

```
<Condition>
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
           <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:physician-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Apply>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
            <AttributeSelector
                RequestContextPath= "//xacml-context:Resource/xacml
                context:ResourceContent/md:record/md:primaryCarePhysician
                /md:registrationID/text()"
               DataType="http://www.w3.org/2001/XMLSchema#string"/>
         </Apply>
    </Apply>
</Condition>
```

Rule applies if physician-id equals primaryCarePhysician

Obligations

- Additional constraints to an authorization decision
- If PEP cannot fulfill an obligation then it disallows access

Example Obligation

```
<Obligation
          ObligationId="urn:oasis:names:tc:xacml:example:obligation:email“ FulfillOn="Permit">
          <AttributeAssignment
               AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:mailto"
               DataType="http://www.w3.org/2001/XMLSchema#string">
               <AttributeSelector RequestContextPath=
                    "//md:/record/md:patient/md:patientContact/md:email"
                    DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </AttributeAssignment>
          <AttributeAssignment
               AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:text"
               DataType="http://www.w3.org/2001/XMLSchema#string">
                    Your medical record has been accessed by:
           </AttributeAssignment>
           <AttributeAssignment
                  AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:text"
                  DataType="http://www.w3.org/2001/XMLSchema#string">
                 <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                  DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </AttributeAssignment>
</Obligation>
```

Send email to patient’s email address when medical records accessed by subject-id