

➔ Samuel Kaluvuri

➔ Alex Egner

SAFAX

Authorization as a Service

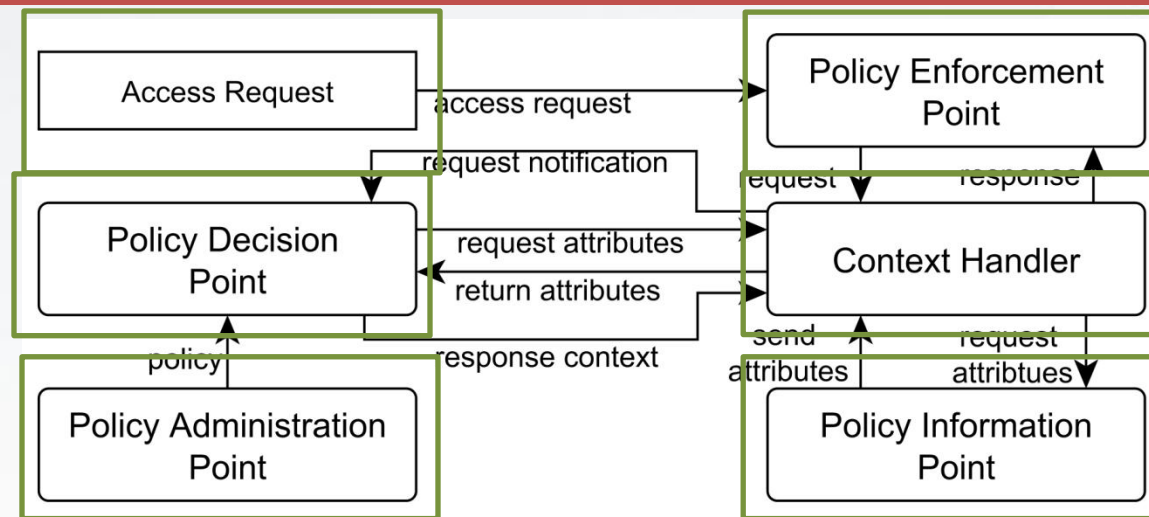
- ➔ SAFAX Overview
- ➔ SAFAX Architecture
- ➔ SAFAX Features

AGENDA

SAFAX Overview

- ➔ SAFAX is an eXtensible Authorization Service
- ➔ XACML Compliant
- ➔ Tailored specifically for cloud environments
- ➔ Can consume information from additional trust sources during policy evaluation – *extensible*
- ➔ Includes a User Interface for Policy Administration

XACML Reference Architecture



- ⊕ XACML provides extensibility points through the use of “User Defined Functions”
- ⊕ There are many different implementations of XACML available
- ⊕ XACML standard is underspecified – and it does not pose too many constraints on the implementations

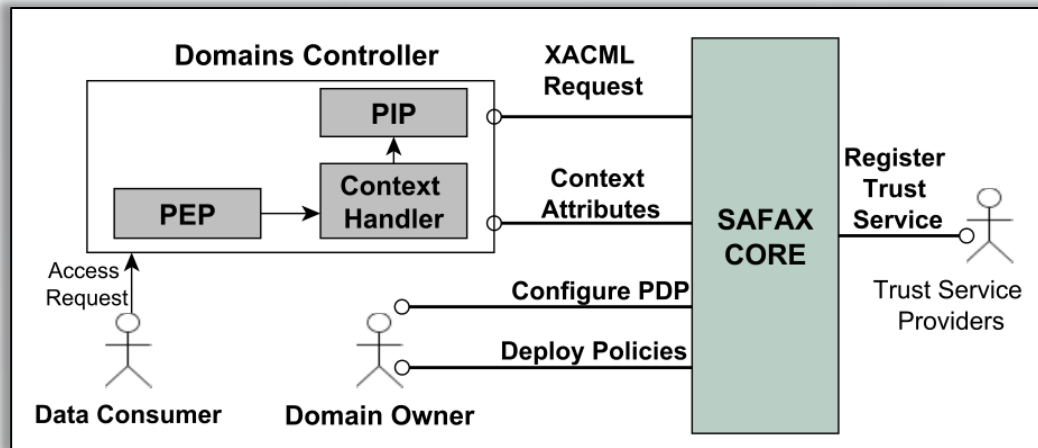
XACML Implementations - Limitations

- ④ Current XACML Implementations – based on SUN XACML, HERAS-AF or Balana are implemented as **Monolithic Components**
- ④ Extensions are typically bundled with the Implementation
- ④ They cannot consume external information during policy evaluation
- ④ ***Major stumbling blocks – when applied in cloud environments***

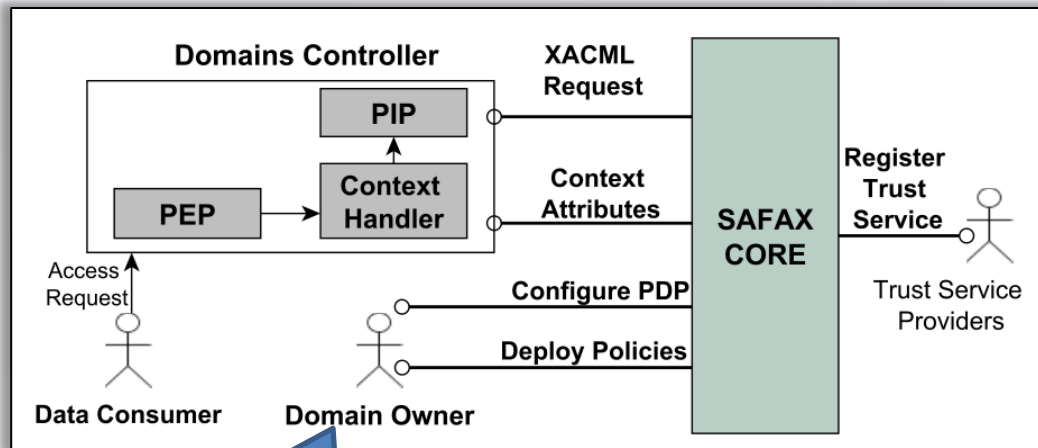
SAFAX - AZaaS

- ⊕ XACML compliant policy evaluation engine
- ⊕ Can cater to traditional and cloud provisioning models
- ⊕ Modular, Extensible, Flexible, Scalable and Interoperable
- ⊕ Offers Authorization As A Service (AZaaS)

SAFAX Architecture

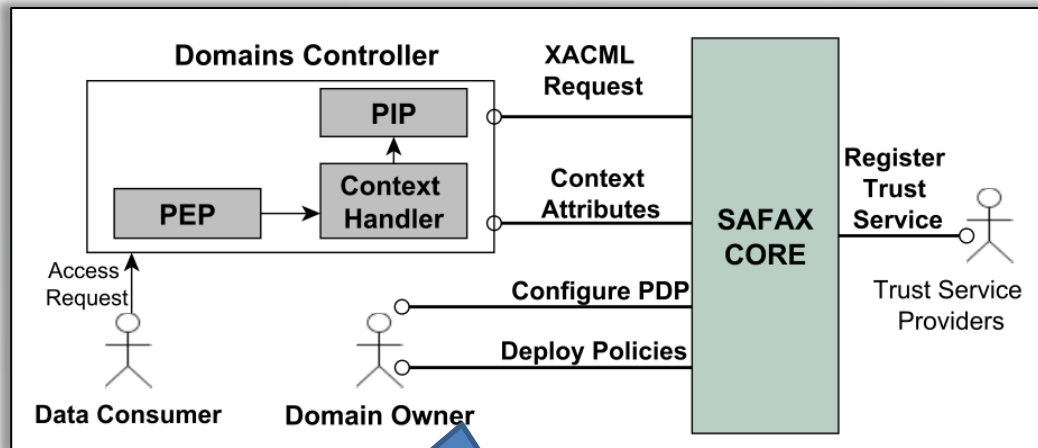


SAFAX Architecture



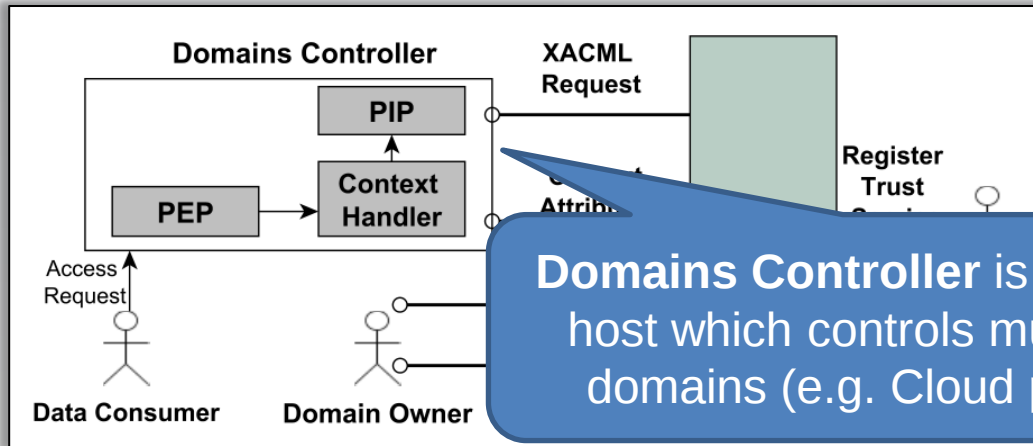
Domain specifies a data set managed by a user

SAFAX Architecture

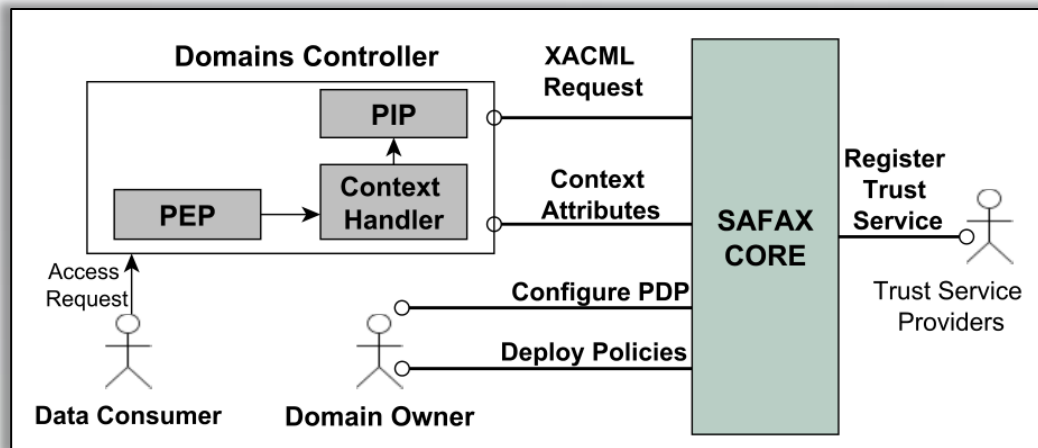


Domain Owner is a user to whom the domain belongs

SAFAX Architecture

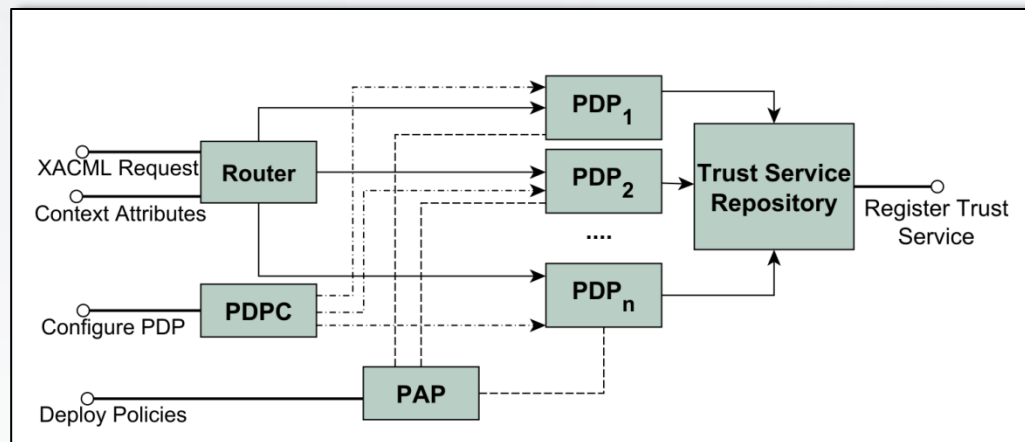


SAFAX Architecture



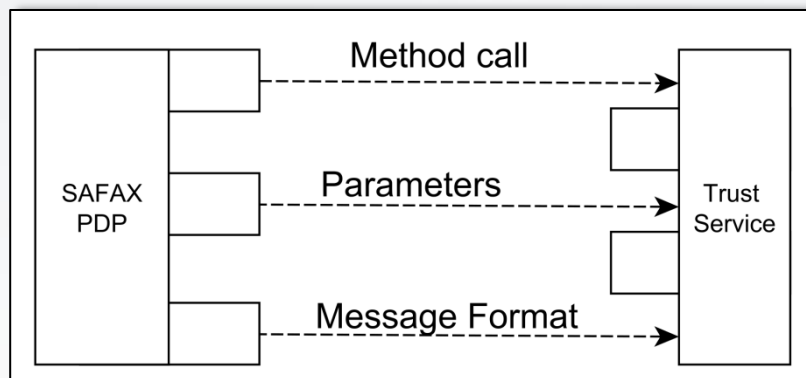
- ➞ Provides different users a single point to deploy their access control policies
- ➞ Provides flexibility to users to configure their PDPs and trust services
- ➞ Relieves domain controllers from custom solutions
- ➞ Developers can extend the PDP by registering new trust services
 - ➞ Reputation scores, Credentials etc.

SAFAX Architecture



- ➞ Router directs the request from DC to the PDP assigned to the user
- ➞ PDPC allows users to configure their PDPs
 - ➞ version, implementation, external trust services
- ➞ PAP allows Domain Owners to deploy their policies
- ➞ PDP uses the trust service repository to make service invocations

SAFAX Architecture



- ➞ External Services must conform to API specifications
 - ➞ RESTFul
 - ➞ JSON/XML
- ➞ Services must be registered with SAFAX
 - ➞ Unique Function Identifier (URN)
 - ➞ Service Endpoint (URI)
 - ➞ Method call type (POST/GET)
 - ➞ Input parameters number
 - ➞ Output Parameter type
 - ➞ Message format

SAFAX Implementation

- ⊕ Developed in JAVA
- ⊕ Jersey as Service Framework
- ⊕ Tomcat as Application Server
- ⊕ MySQL for persistence
- ⊕ JSON and XML for messaging
- ⊕ Browser based GUI for demonstration purposes
 - ⊕ HTML
 - ⊕ CSS
 - ⊕ JS
 - ⊕ AJAX
- ⊕ PDP Implementation
 - ⊕ HERAS-AF

USING SAFAX

- Users can create PROJECTS
 - Each project contains DEMOS
 - Each demo contains POLICIES
 - Demos can be configured according to user preferences
- Users can evaluate their policies against access requests
- Users can review their actions and analyze the logs generated by SAFAX
- SAFAX comes with an integrated Issue Reporting tool
 - Users can report bugs or request for new features

SAFAX Tutorial – Creating Projects

[Home](#) [Policy Evaluation](#) [Service Registry](#) [Account Activity](#) [Issue Tracker](#) [About](#) [Settings](#) [Logout](#)

SAFAX

A Flexible and Extensible Authorization Service

Projects +

Start a new Project +

mickey
mouse



testpr



Project Name

Unique Project Name

Project Description

Project Homepage

Project Homepage

Make Private

☒

Assign members to project

Find Users

Users

+

-

Assigned Users

Create Project

TU/e - Security Group

SAFAX Tutorial – Creating Projects

Home Policy Evaluation Service Registry Account Activity Issue Tracker About Settings Logout

SAFAX

A Flexible and Extensible Authorization Service

Projects **+** Start a new Project **+**

mickey mouse

Project Name

testpr

Project Description

Project Homepage

Make Private ☒

Assign members to project

Find Users

Assigned Users

Create Project

TU/e - Security Group

SAFAX Tutorial – Creating Projects

Home Policy Evaluation Service Registry Account Activity Issue Tracker About Settings Logout

SAFAX

A Flexible and Extensible Authorization Service

Projects + Start a new Project +

mickey mouse mickey mouse

testpr testpr

Project Name Unique Project Name

Project Description

Project Homepage Project Homepage

Make Private ☒

Assign members to project

Find Users Users

Assigned Users

TU/e - Security Group

You can keep your projects **private**

SAFAX Tutorial – Creating Projects

Home Policy Evaluation Service Registry Account Activity Issue Tracker About Settings Logout

SAFAX

A Flexible and Extensible Authorization Service

Projects + [Start a new Project](#) +

mickey mouse ✎ 🗑 Project Name

testpr ✎ 🗑 Project Description

Project Homepage

Make Private ☒

Assign members to project

Find Users 🔍 + -

Assigned Users

TU/e - Security Group

You can share your project with other users

SAFAX Tutorial – Creating Demos

SAFAX

A Flexible and Extensible Authorization Service

Projects

+

No Demos

+

mickey
mouse

Demo Name

Unique Demo Name

Sample
Project

Demo Description

Create Demo

SAFAX Tutorial – Creating Demos

SAFAX

A Flexible and Extensible Authorization Service

Projects

No Demos

mickey mouse

Demo Name

Unique Demo Name

Demo Description

Create Demo

SAFAX Tutorial – Creating Demos

SAFAX

A Flexible and Extensible Authorization Service

Projects

+

Edit Demo

+

mickey mouse



Back

Run

Sample Project



XACML

Credential

Reputation

Similarity



XACML

No policies have been deployed, You better upload atleast one!



SAFAX Tutorial – Creating Demos

The screenshot displays the SAFAX web application interface. At the top, the title 'SAFAX' is followed by the subtitle 'A Flexible and Extensible Authorization Service'. Below this, a 'Projects' section shows a list with 'mickey mouse' and a 'Sample Project' button. A 'Back' button and a 'Run' button are visible. The main content area is titled 'XACML' and contains a message: 'No policies have been deployed, You better upload atleast one!'. A green circle highlights an upload icon (a document with a plus sign) in the bottom right corner of the XACML section.

Upload XACML Policies

SAFAX Tutorial – Creating Demos

⬅ Back Run ▶

XACML Credential Reputation Similarity ⚙

Demo Name

Demo Description

Move Demo

PDP Code
http://localhost/pdp/65

Persistent ☐

PEP

Context Handler

PIP

PDP

PAP

Configure your demos

SAFAX Tutorial – Creating Demos

⬅ Back Run ▶

XACML Credential Reputation Similarity ⚙

Demo Name

Demo Description

Move Demo

PDP Code
http://localhost/pdp/65

Persistent ☒

PEP

Context Handler

PIP

PDP

PAP

Save Settings

Run the Demos

SAFAX Tutorial – Evaluating Policies

[Activity](#) [Issue Tracker](#) [About](#) [Settings](#) [Logout](#)

SAFAX

A Flexible and Extensible Authorization Service

DEMOS

test9

test2

test1

in4stars test1231

in4stars test1231

Sample Demo

Request

Response

TU/e - Security Group

SAFAX Tutorial – Evaluating Policies

The screenshot shows the SAFAX web application interface. At the top, there is a navigation bar with links: Activity, Issue Tracker, About, Settings, and Logout. Below this, the header displays 'SAFAX' and 'A Flexible and Extensible Authorization Service'. The main content area is divided into two columns. The left column, titled 'DEMOS', contains a list of demo names: test9, test2, test1, in4stars test1231, and in4stars test1231. The 'in4stars test1231' option is highlighted with a green oval, and a blue callout box with the text 'Choose Your Demo' points to it. Below the list, there is a 'Sample Demo' button. The right column has a 'Request' input field and a 'Response' output area. At the bottom left, the text 'TU/e - Security Group' is visible.

SAFAX A Flexible and Extensible Authorization Service

Activity Issue Tracker About Settings Logout

DEMOS

test9

test2

test1

in4stars test1231

in4stars test1231

Sample Demo

TU/e - Security Group

Request

Response

Choose Your Demo

SAFAX Tutorial – Evaluating Policies

The screenshot shows the SAFAX web application interface. At the top, there is a navigation bar with links: Activity, Issue Tracker, About, Settings, and Logout. Below this, the header displays 'SAFAX' and 'A Flexible and Extensible Authorization Service'. On the left side, there is a 'DEMOS' section with a list of test cases: test9, test2, test1, in4stars test1231, and in4stars test1231. The 'Sample Demo' option is highlighted. The main area contains a 'Request' input field and a 'Response' output area. A green circle highlights a file upload icon in the 'Request' field. A blue callout box with the text 'Upload XACML Requests' points to this icon. At the bottom left, the footer indicates 'TU/e - Security Group'.

SAFAX A Flexible and Extensible Authorization Service

Activity Issue Tracker About Settings Logout

DEMOS

- test9
- test2
- test1
- in4stars test1231
- in4stars test1231
- Sample Demo

Request

Response

Upload XACML Requests

TU/e - Security Group

SAFAX Tutorial – Evaluating Policies

SAFAX

A Flexible and Extensible Authorization Service

DEMOS

test9

test2

test1

in4stars test1231

in4stars test1231

Sample Demo

Request

Response

```
<Response xmlns:ns2="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os">
  <Result>
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
</Response>
```

Analyze Trace

TU/e - Security Group

SAFAX Tutorial – Evaluating Policies

SAFAX

A Flexible and Extensible Authorization Service

DEMOS

test9

test2

test1

in4stars test1231

in4stars test1231

Sample Demo

Request

Response

```
<Response xmlns:ns2="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os">
  <Result>
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
</Response>
```

Analyze Trace

TU/e - Security Group

You can see detailed logs using Analyze Trace

SAFAX Tutorial – Analyzing Trace

SAFAX

A Flexible and Extensible Authorization Service

Options

- Current Session Transactions
 - evaluate_ad2b3270187e41a996b2b9800d39188b
 - evaluate_e863dbf4528947b6b0ab20f0e6d3713e
- Past 20 Transactions
 - evaluate_e860bcc1c9694c6dbaffd4e9ecec218
 - evaluate_e6c287f1fd644a8828c9bf30beb83a
 - evaluate_a37f79d51e464779a5aac4e1aadde70f
 - evaluate_307958452dd64ab7978d0c9f10b6604a
 - evaluate_8fe9a0e7093c4edbbe687d4aa0561c62
- Restore Deleted Items

Activity

```
<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>
<Environment />
</Request>
nl.tue.sec.safax.ch: Sending Request to PDP at http://localhost/pdp/evaluate
nl.tue.sec.safax.pdp: Received Request From CH
nl.tue.sec.safax.pdp: Sending Response to CH
nl.tue.sec.safax.ch: Received Response From PDP
nl.tue.sec.safax.ch: Sending response to PEP
nl.tue.sec.safax.pep: Received response from nl.tue.sec.safax.contexthandler.evaluate
nl.tue.sec.safax.pep: <Response xmlns:sa2="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os">
  <Result>
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Status>
  </Result>
</Response>
```

TU/e - Security Group

SAFAX Tutorial – Analyzing Trace

SAFAX

A Flexible and Extensible Authorization Service

Options

Current Session Transactions

evaluate_ad2b3270187e41a996b2b9800d39188b
evaluate_e863dbf4528947b6b0ab20f0e6d3713e

Past 20 Transactions

evaluate_e860bcc1c9694c6dbaffd4e9ecce218
evaluate_e6c287f1fd644a8828c9bf30beb83a
evaluate_a37f79d51e464779a5aac4e1aadde70f
evaluate_307958452dd64ab7978d0c9f10b6604a
evaluate_8fe9a0e7093c4edbbe687d4aa0561c62

Restore Deleted Items

Activity

```
<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>
<Environment />
</Request>
nl.tue.sec.safax.ch: Sending Request to PDP at http://localhost/pdp/evaluate
nl.tue.sec.safax.pdp:Received Request From CH
nl.tue.sec.safax.pdp:Sending Response to CH
nl.tue.sec.safax.ch: Received Response From PDP
nl.tue.sec.safax.ch:Sending response to PEP
nl.tue.sec.safax.pep:Received response from nl.tue.sec.safax.contexthandler.evaluate
nl.tue.sec.safax.pep:Response xmlns:ns2="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
<Result>
  <Decision>
    <Result>
      <Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
    </Value>
  </Decision>
</Result>
```

Choose a request to
view the detailed log