

**Deploying Authorization Mechanisms for  
Federated Services in the eduroam  
Architecture (DAMe)**

Kick-off

*University of Murcia*

6th September, Madrid (Spain)

# Overview

---

- ✓ **Introduction**
- ✓ **Main goals and current status**

# Introduction

- ✓ **DAMe** is a project that builds upon previous TERENA, Internet2, and University of Murcia work:
  - ✓ **eduroam**, a result of TERENA Mobility Task Force, which defines an inter-NREN roaming architecture based on AAA servers (RADIUS) and the 802.1X standard,
  - ✓ **Shibboleth**, a widely deployed federation mechanism.
  - ✓ **eduGAIN**, the AAI of GN2
  - ✓ **NAS-SAML**, a network access control approach for AAA environments, developed by the University of Murcia (Spain), based on the SAML (Security Assertion Markup Language) and the XACML (eXtensible Access Control Markup Language) standards.

# Introduction

- ✓ EDUROAM allows users of participating institutions to access the **Internet** at other participants **using their home institution's credentials**.
  - ✓ It would be desirable to **extend** the EDUROAM architecture with authentication and authorization mechanisms.
  - ✓ **NAS-SAML** is an access control proposal for AAA environments which can be used to extend EDUROAM to exchange existing credentials.
  - ✓ Credentials can be **expressed in several forms**, ranging from Shibboleth statements to X.509 Attribute certificates
  - ✓ Integration of **eduGAIN** in order to obtain the authentication and authorization credentials
- ✓ Additionally, this authorization mechanism might be **used at service-level**, for example for Grid Computing purposes.
- ✓ EDUROAM constitutes an **exceptional starting point** to offer a full and integrated network access experience to the users.

# Overview

---

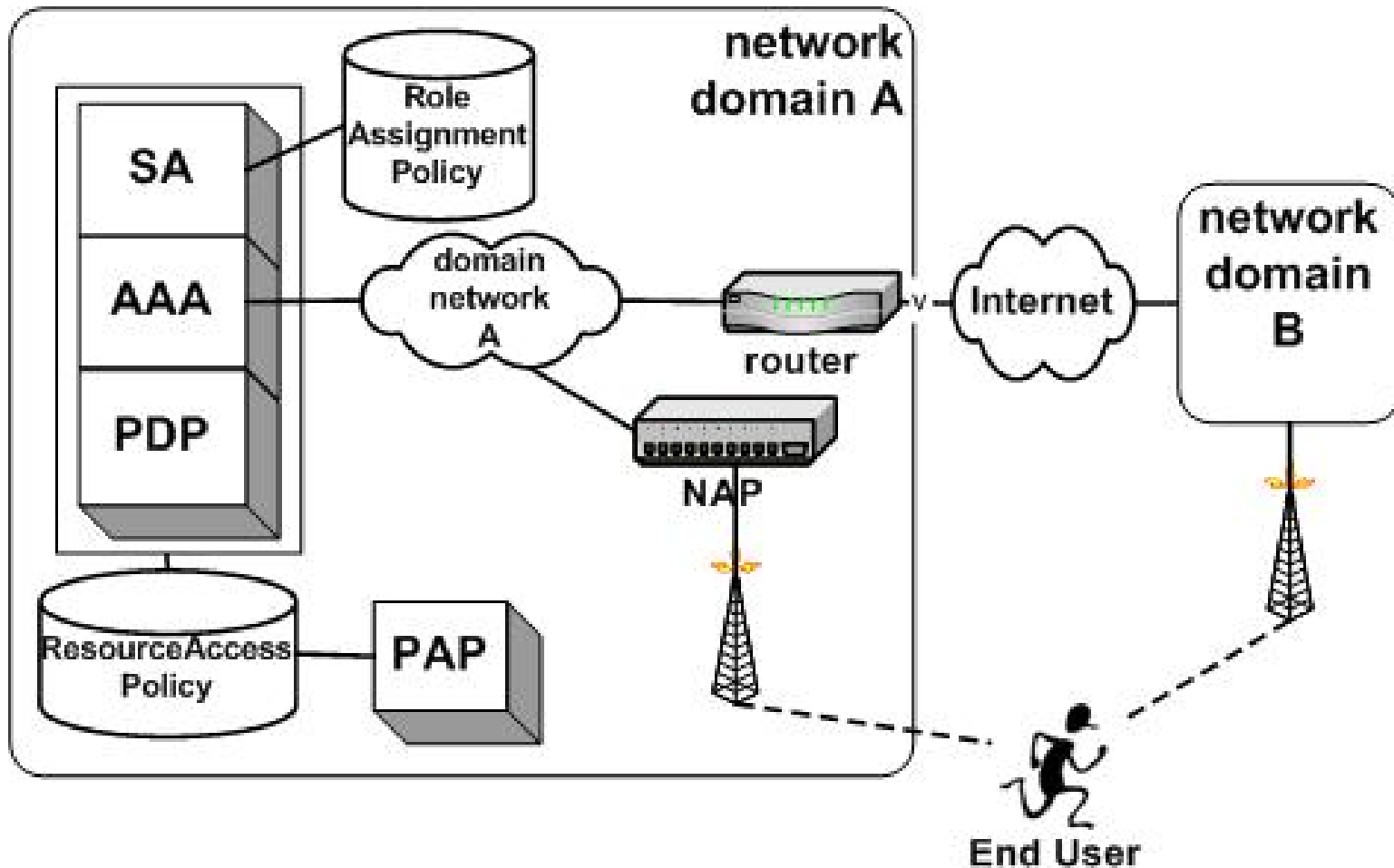
- ✓ Introduction
- ✓ **Main goals and current status**

# NAS-SAML

- ✓ Main objectives:
  - ✓ To define a network access control approach based on:
    - X.509 PKC authentication
    - User attributes (roles)
    - Authorization policies. Rules stating the permissions give to each system role.
  - ✓ Use of XML to express:
    - access control policies (XACML)
    - authorization statements (SAML)
    - authorization protocols (SAML)
  - ✓ The scenario should be integrated in the AAA architecture.

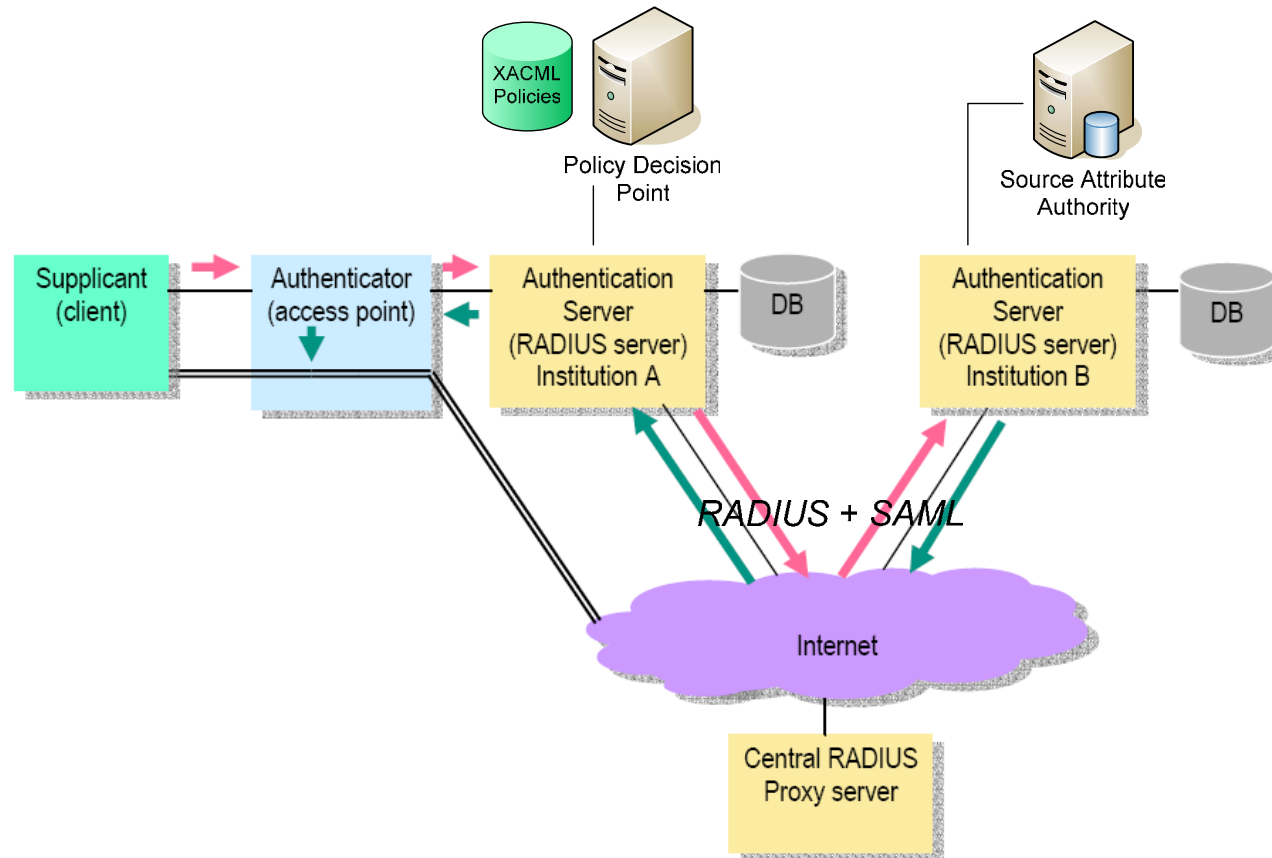
# NAS-SAML

## ✓ Architectural elements



# Main goals

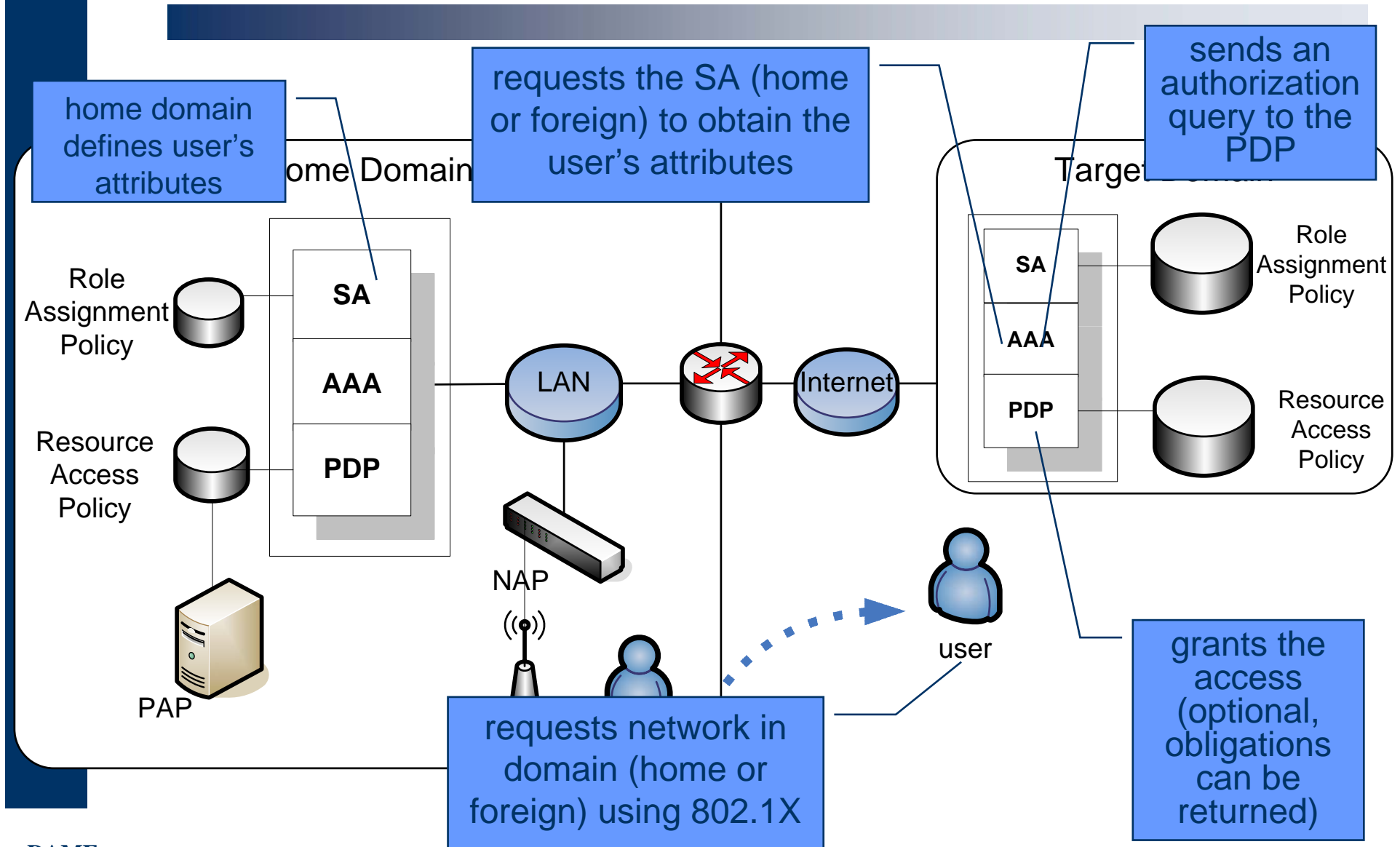
- ✓ First Goal: Extension of eduroam using NAS-SAML
  - ✓ User mobility controlled by assertions and policies expressed in SAML and XACML.
  - ✓ Enhanced interoperability among organizations (common language)



# Main goals

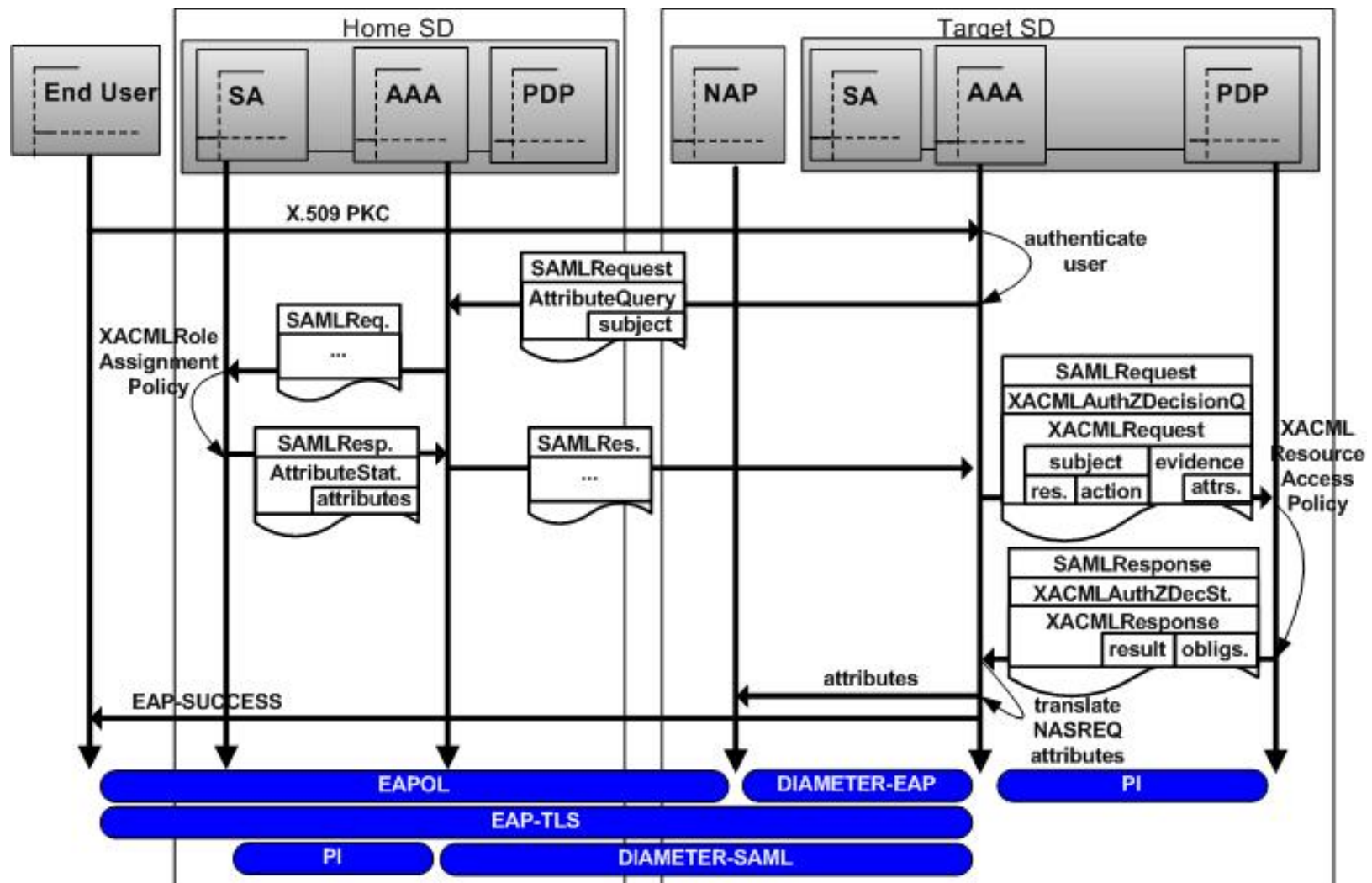
- ✓ **First Goal: Extension of eduroam using NAS-SAML**
- ✓ **RELATED ACTIVITIES:**
  - ✓ **Activity 1. Integration of the NAS-SAML architecture in the eduroam network.**
    - Task 1. Analysis of the current status of the eduroam network.
    - Task 2. Analysis of the required user attributes and policies for roaming.
    - Task 3. Analysis of the different Grid platforms that are being currently used in the different European initiatives.
    - Task 4. Development of the Source Authority and Policy Decision Points.
    - Task 5. Development a custom SAML module for RADIUS and DIAMETER servers.
    - Task 6. Create a translator to convert RADIUS messages into DIAMETER and vice versa.
    - Task 7. Validate the resulting architecture for mobility purposes.
  - ✓ **Activity 2. Development of a user-friendly management interface for authorization policies.**
    - Task 1. Analysis of the different existing proposals for privilege administration.
    - Task 2. Development of a high level interface able to be integrated with common office applications.
    - Task 3. Creation of interpreters and translators able to convert policies into XACML.
    - Task 4. Validate the resulting interface.

# Current Work (Activity 1)



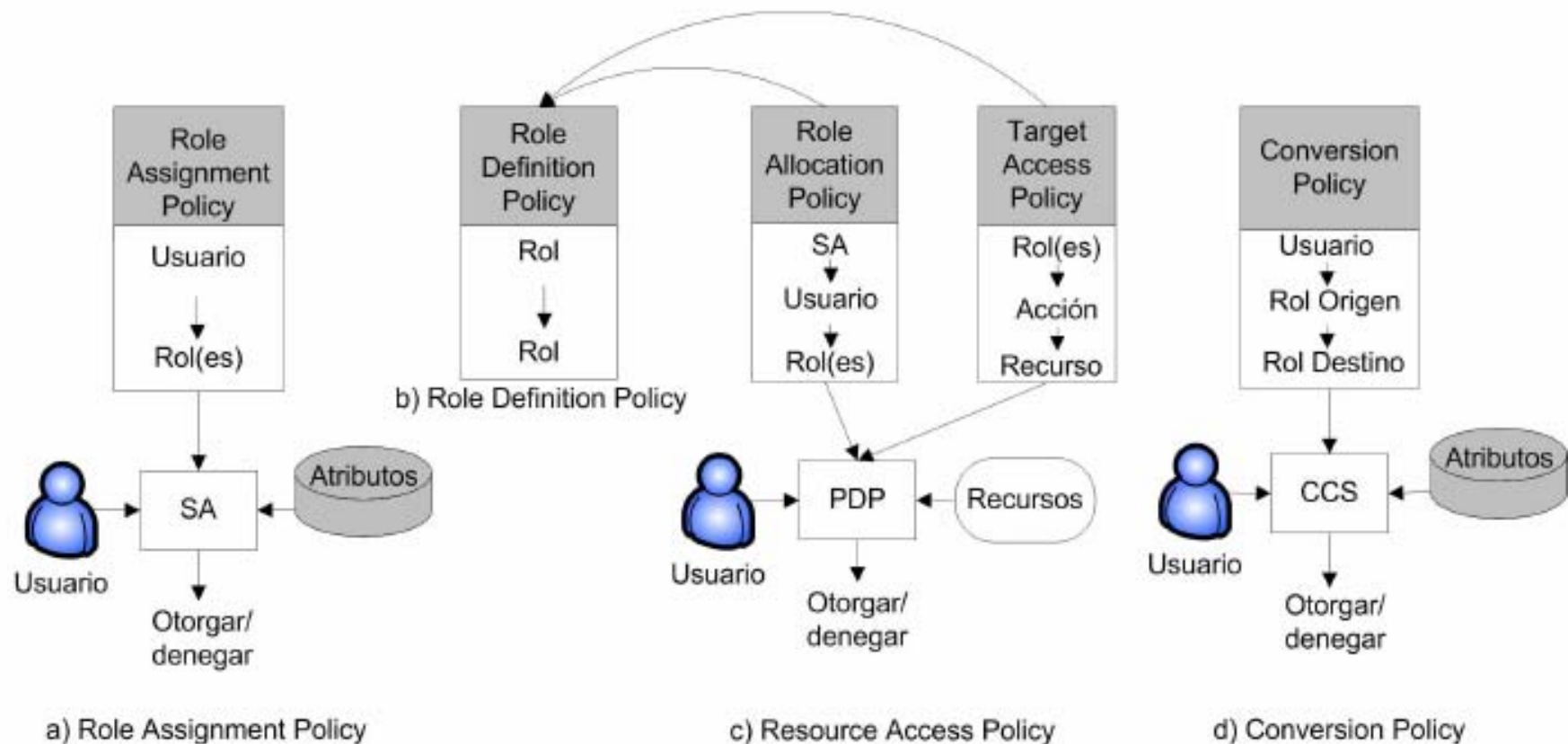
# Current Work (Activity 1)

- ✓ NAS-SAML. Inter-domain pull model



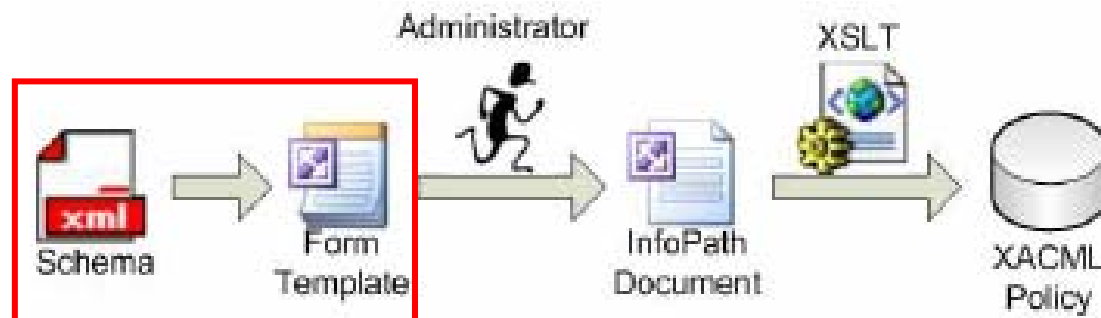
# Current Work (Activity 1)

- ✓ Set of policies used in NAS-SAML



# Current Work (Activity 2)

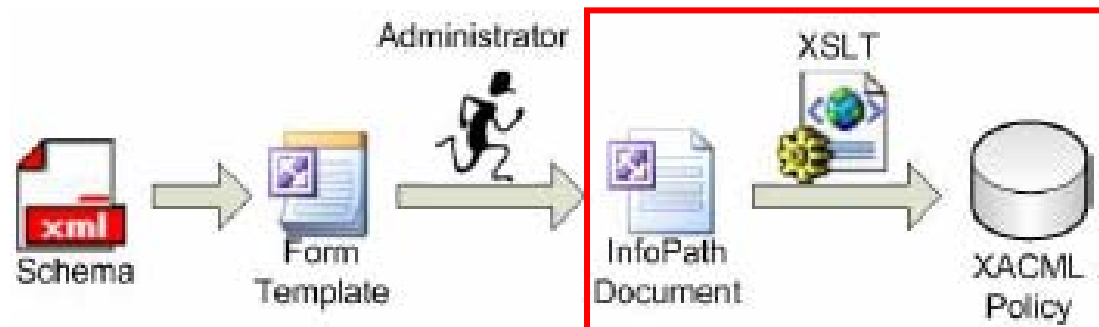
- ✓ User friendly interface. Main idea:



- ✓ Initial XSD:
  - ✓ The "security expert" (XACML aware) is responsible for developing the schema
  - ✓ That **schema depends on the specific XACML policy** to be generated
  - ✓ Using the schema (and an optional XSL transformation) a form is presented to the administrator to be filled in.
  - ✓ A **set of templates** are available to the system administrator, each one for every specific policy existing in the system.

# Current Work (Activity 2)

- ✓ User friendly interface. Main idea:



- ✓ XACML transformation:
  - ✓ Once the initial document is written, a XSL transformation must be applied to transform it into the final XACML policy.
  - ✓ This can be done either using a XSLT compiler, such as XALAN, or some XML editor implementing the XSLT standard.
  - ✓ The XSL transform generates the XACML policy completing the required sections using the information from the initial document.

# Current Work (Activity 2)

## ✓ Resource Access Policy



### TARGET ACCESS POLICY

The attribute  grants access over the following resources/actions:

- /

Under the following conditions:

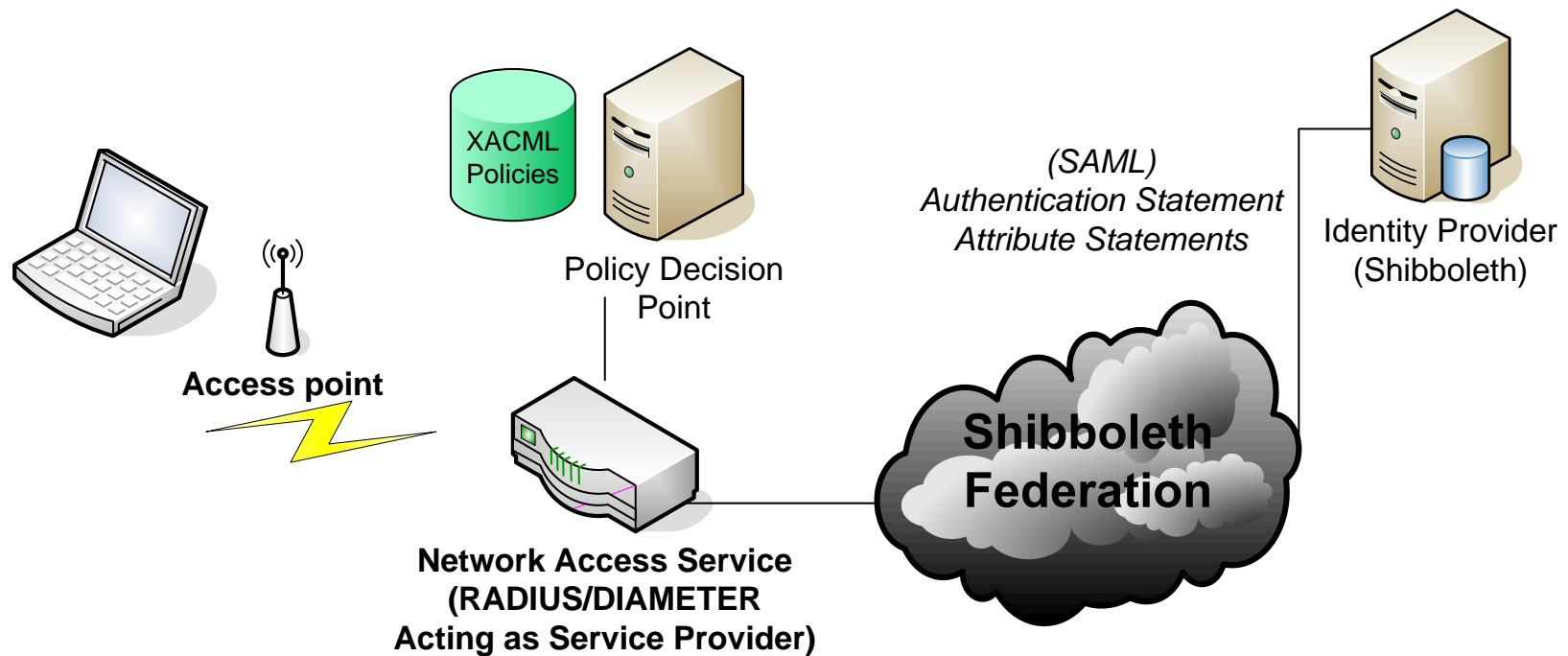
and

And these obligations must be enforced:

- =
- =

# Main goals

- ✓ Second Goal: Use of eduGAIN as authn and authz backend
  - ✓ NAS-SAML has been already integrated with other proposals (X.509 AC)
  - ✓ Link between the AAA servers (now acting as Service Providers) and the AAI of eduGAIN or Shibboleth.

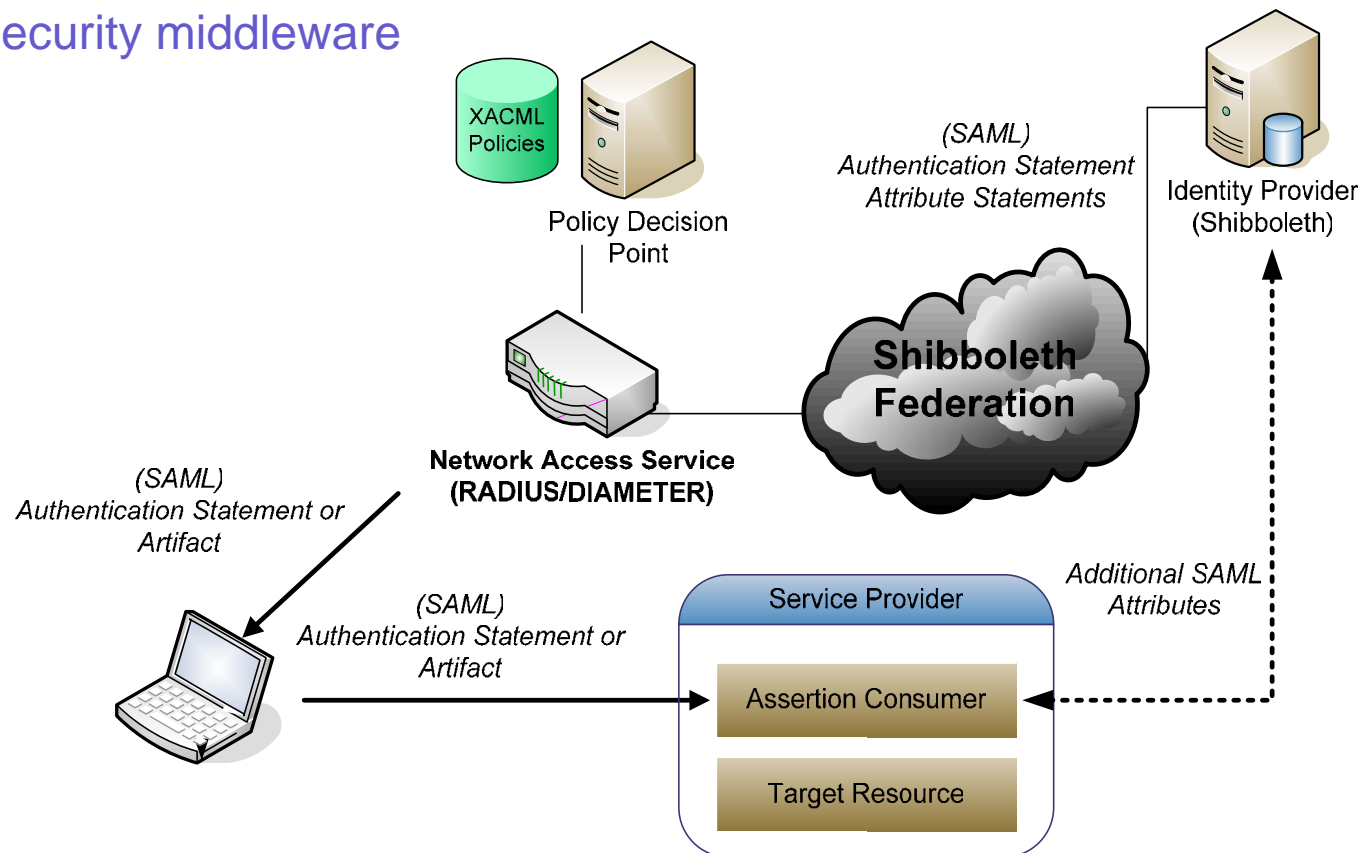


# Main goals

- ✓ Second Goal: Use of Shibboleth as authn and authz backend
- ✓ RELATED ACTIVITIES:
  - ✓ **Activity 3. Use of eduGAIN as authentication back-end for NAS-SAML**
    - Task 1. Analysis of the proposed eduGAIN/Shibboleth profiles for SSO. Identification of the possible modifications that would require some of those profiles.
    - Task 2. Development of a Service Provider module responsible for the creation and exchange of eduGAIN/Shibboleth authentication and attribute requests.
    - Task 3. Definition of the authentication methods to be used by the end users in order to demonstrate their digital identity.
    - Task 4. Extension of the existing XACML context manager in order to interpret the eduGAIN/Shibboleth SAML credentials.
    - Task 5. Validate the resulting architecture.

# Main goals

- ✓ Third Goal: Global Single Sign On (SSO)
  - ✓ Users will be authenticated once, during the network access control phase
  - ✓ The eduGAIN authentication would be bootstrapped from the NAS-SAML
  - ✓ New PEAP method for delivering authentication credentials and new security middleware

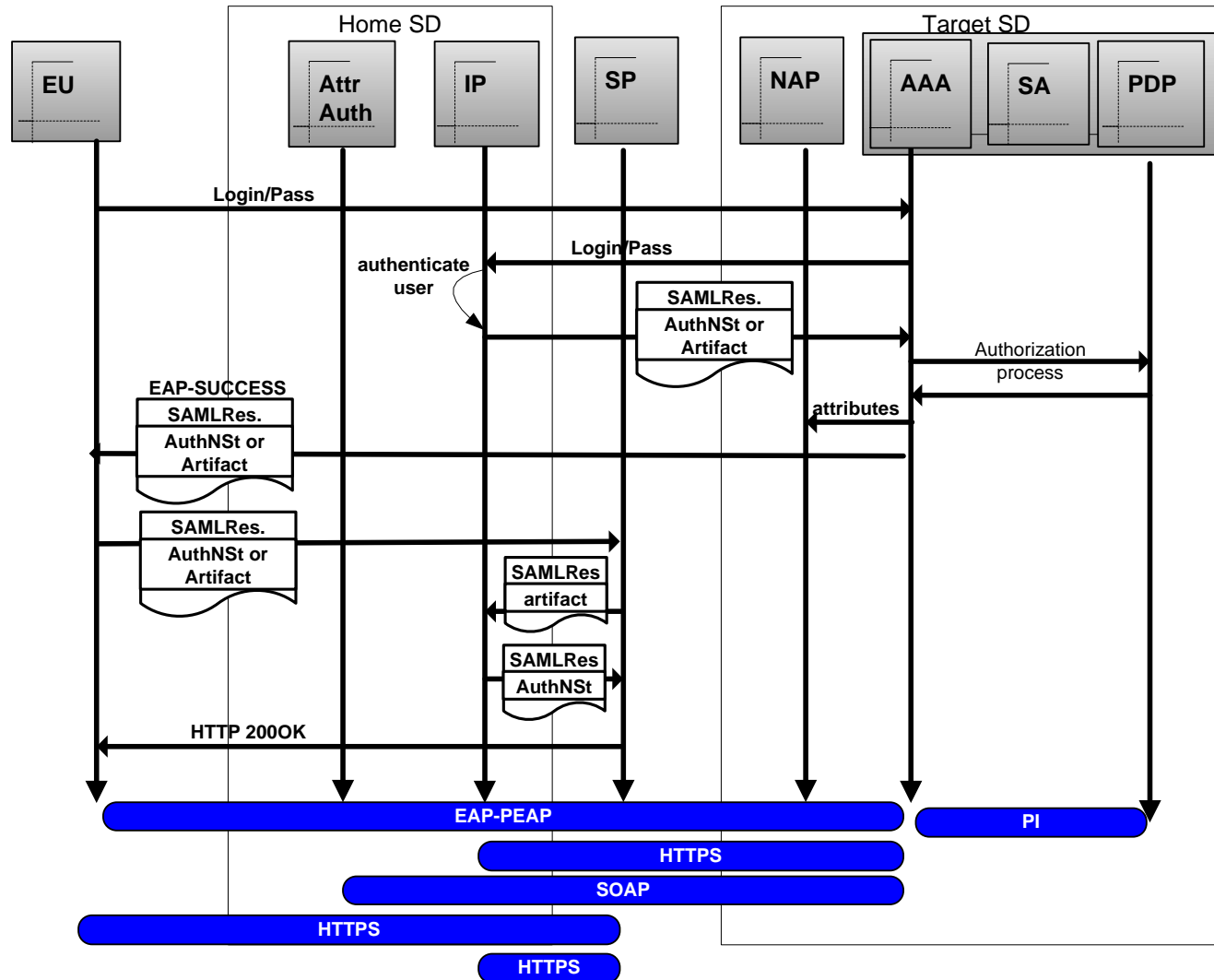


# Main goals

- ✓ Third Goal: Global Single Sign On (SSO)
- ✓ RELATED ACTIVITIES:
  - ✓ **Activity 4. Development of a global SSO**
    - Task 1. Analysis of the requirements of a new PEAP authentication method able to exchange the necessary eduGAIN signed tokens.
    - Task 2. Development of the client and server software modules implementing the specified PEAP method..
    - Task 3. Design and develop the middleware able to manage the signed Shibboleth tokens that will be then provided to the resource providers
    - Task 4. Modify the existing service providers in order to include a custom SSO profile based on a push method, that is, a method where the end users are able to provide the required authentication credentials.
    - Task 5. Validate the resulting system.

# Main goals

- ✓ Third Goal: Preliminary design.



# Main goals

- ✓ **Fourth Goal: Authorization mechanisms for application-level services**
  - ✓ Mainly focused on Grid Computing
  - ✓ Grid Services have specific components for authorization purposes
  - ✓ We plan to link that components with the existing authorization infrastructure, using standard extension points:
    - OGSA-Authz
    - MyProxy
    - GridShib
- ✓ **RELATED ACTIVITIES:**
  - ✓ **Activity 5. Deployment of an authorization mechanism for an application-level service: Grid Computing.**
    - Task 2. Analysis of the GridShib tool as starting point to provide authorization services to Grids.
    - Task 3. Definition of the set of attributes used to describe grid-relevant properties.
    - Task 4. Modify the existing network of AAA servers in order to add the Grid-related policies and attributes.
    - Task 5. Validate the resulting authorization services.

# First draft of the Grid Architecture

