

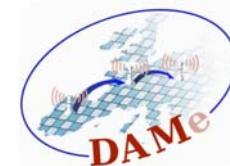
RUS

DAMe

Deploying Authorization Mechanisms for Federated Services in the eduroam Architecture

Sascha Neinert

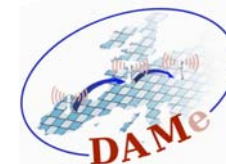
Marseille, 06.02.2008



RUS

Overview

- **Project Goals**
- **Partners**
- **Network Authorization**
- **Unified Single Sign On**



Project Goals

1. Network Authorization

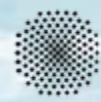
- Further development of eduroam, the Europe-wide NREN roaming federation
- Fine-grained network access control based on attributes
- For properties of the network

2. Unified Single Sign On

- Using eduGAIN, the European AAI confederation architecture
- Interoperability with existing AAIs based on Shibboleth, PAPI, ...
- Token-based authentication for web services
- Unified Single Sign On for network, web- and Grid services



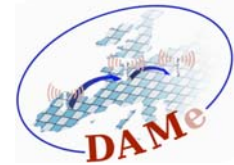
RUS



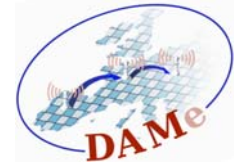
Universität Stuttgart

Kommunikationssysteme
Rechenzentrum

Partners

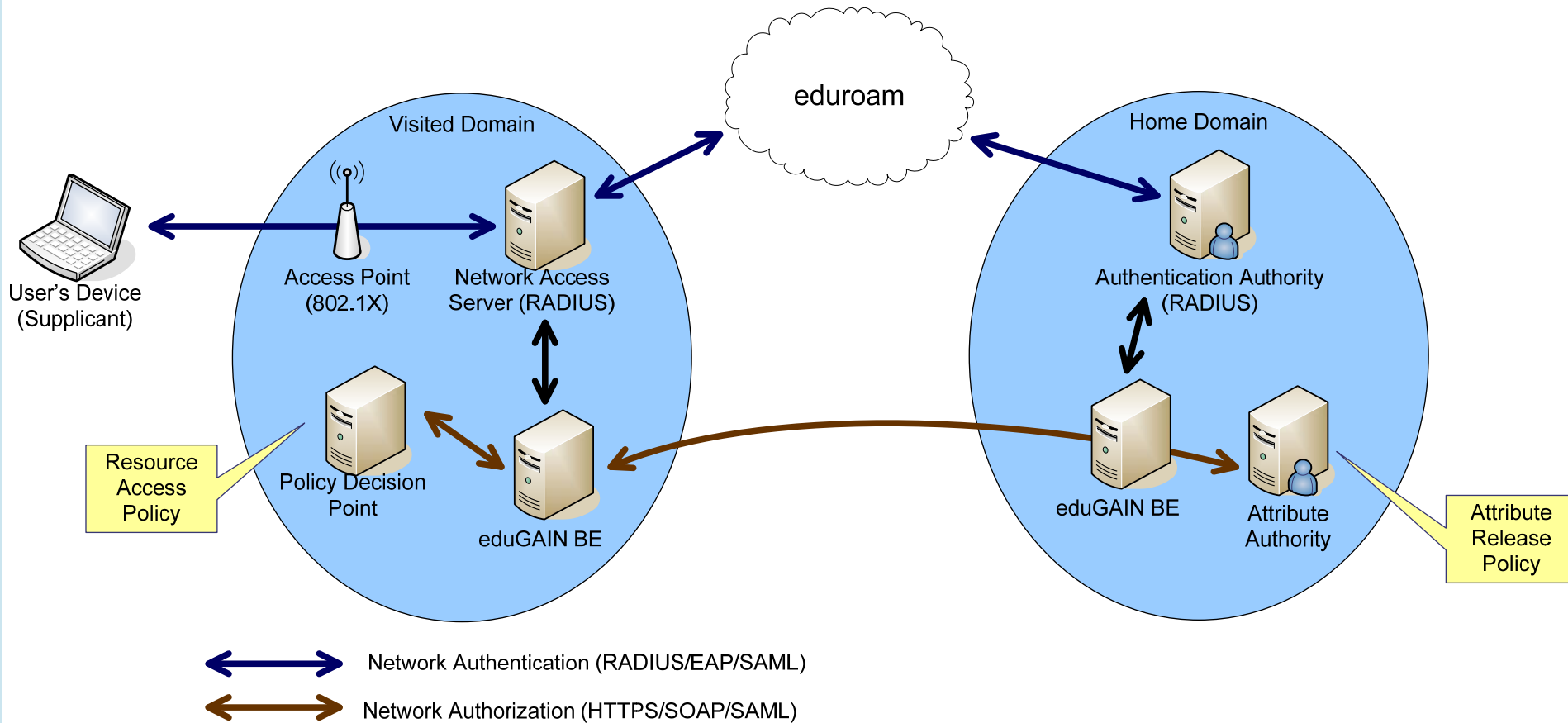


DAMe Project

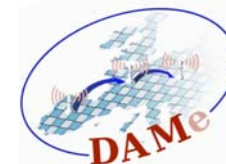


RUS

Goal 1: Network Authorization

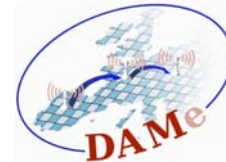


DAME Project



Network AuthZ Components

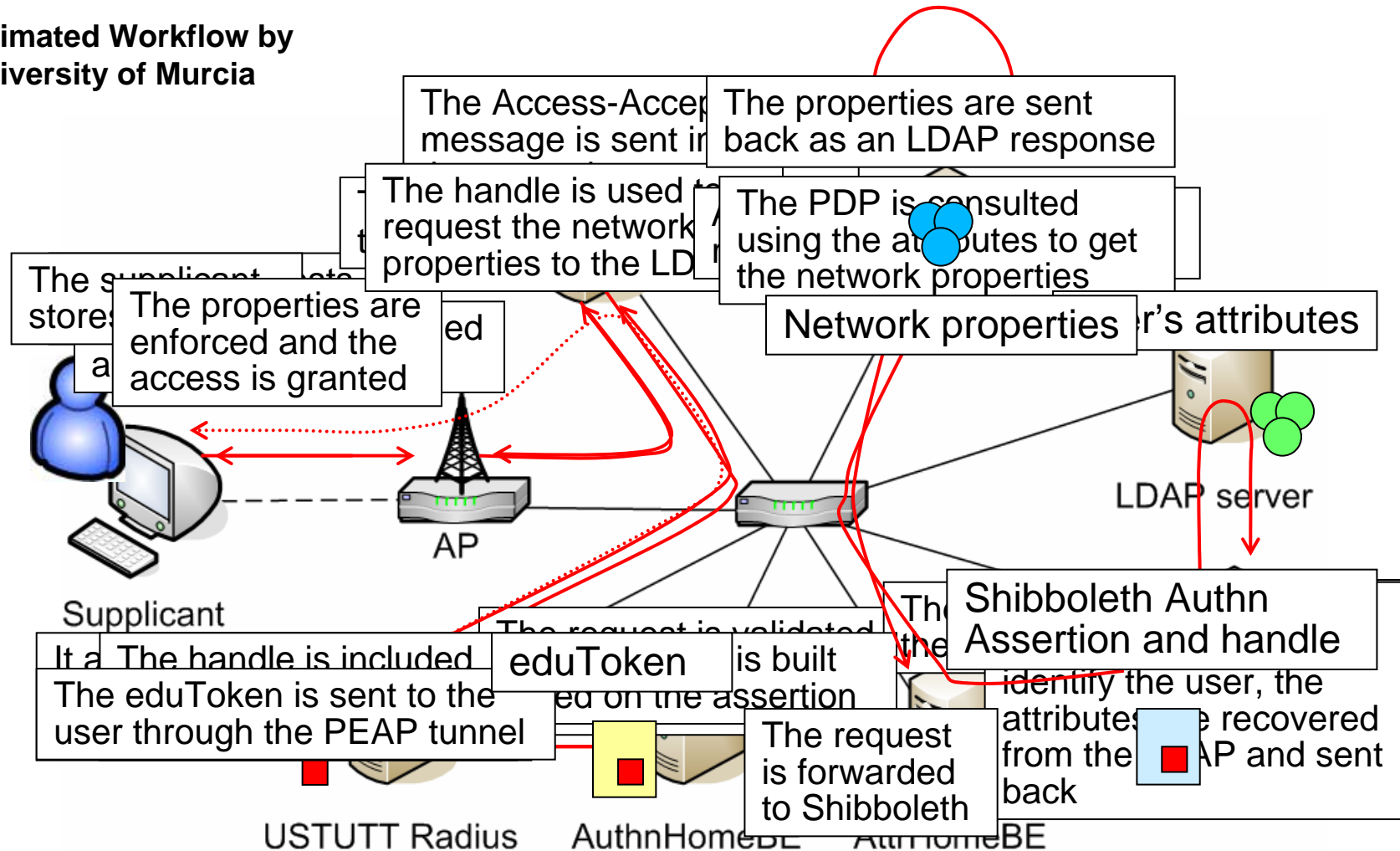
- XSupplicant
 - Recovery and storage of the eduToken
- FreeRadius
 - Request of the eduToken from the HomeBE
 - Delivery of the eduToken using a TLV in the tunneled success message
 - New RADIUS attribute in the response with the user's handle
- LDAP_RemoteBE
 - Receives the user's handle via LDAP
 - Requests the user's attributes using eduGAIN
 - Consults the PDP to get the user's network properties
- PDP
 - Implemented as a servlet and using the XACML library
 - Using the XACML policies, decides the network properties based on the user's attributes
- ...



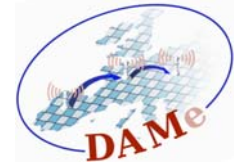
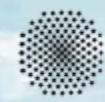
RUS

Network AuthZ Workflow

Animated Workflow by
 University of Murcia

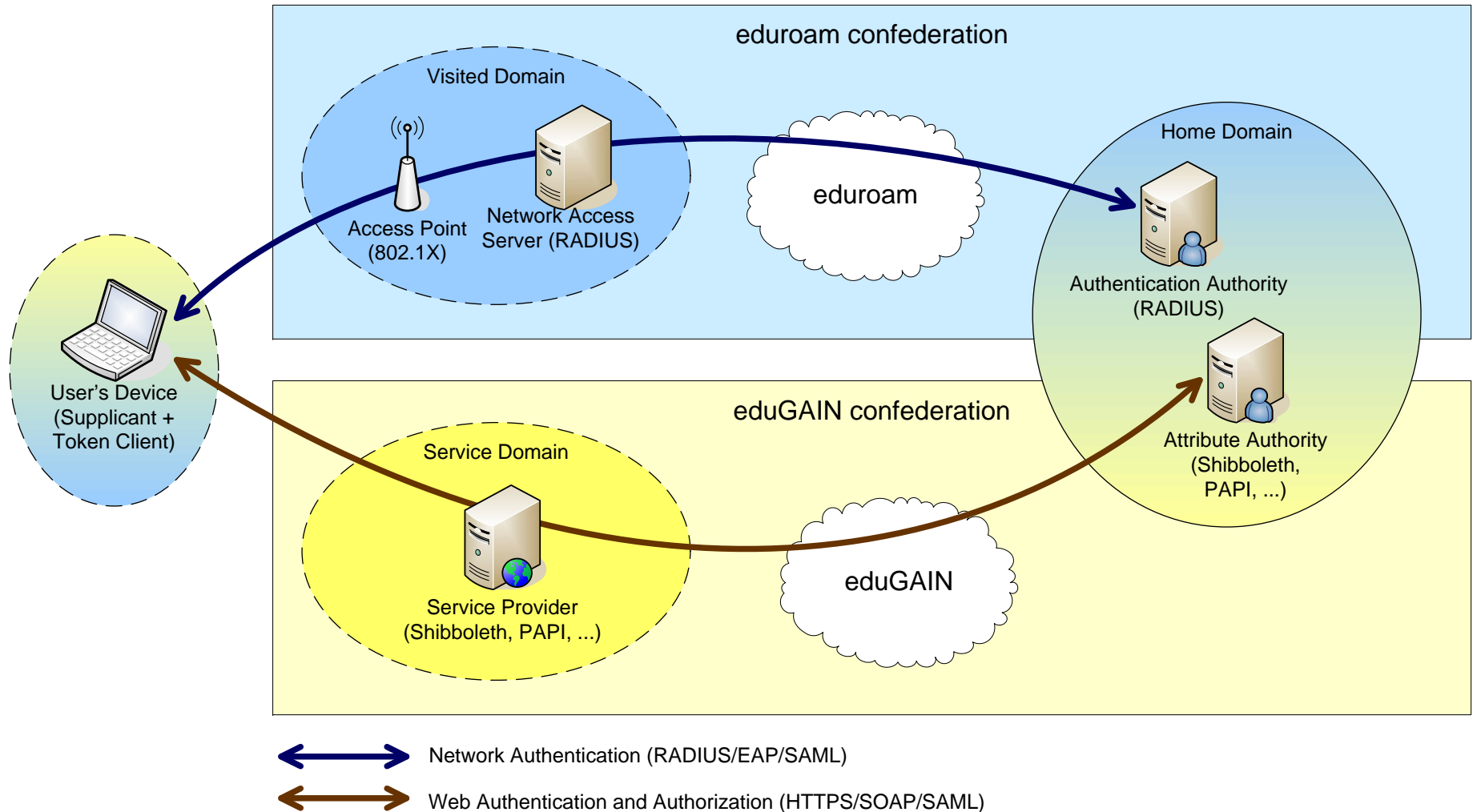


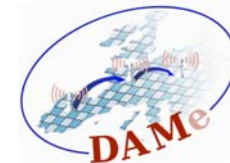
DAME Project



RUS

Goal 2: unified SSO





uSSO Components

■ DameTokenManager

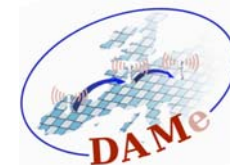
- Java **Client** Application (eduGAIN + openSAML libraries)
- Receives eduToken from supplicant
- Provides eduToken to DameTokenFetcher

■ DameTokenFetcher

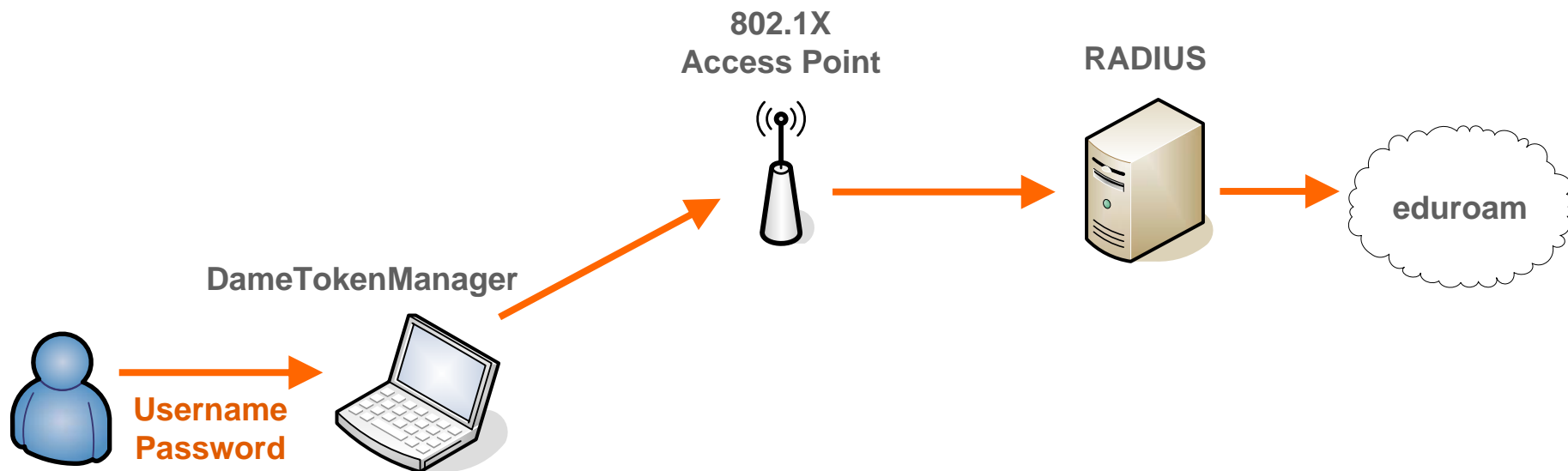
- Signed Java **Applet**
- Fetches eduToken from DameTokenManager
- Sends eduToken to DameTokenServlet

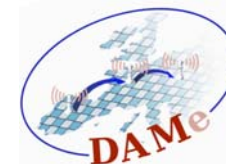
■ DameTokenServlet

- Java **HttpServlet** (eduGAIN + openSAML libraries)
- Receives eduToken from DameTokenFetcher
- Create Shibboleth assertions and send to Service Provider
- Using fromSAML and toShibbolethSAML of Shibboleth remote Bridging Element



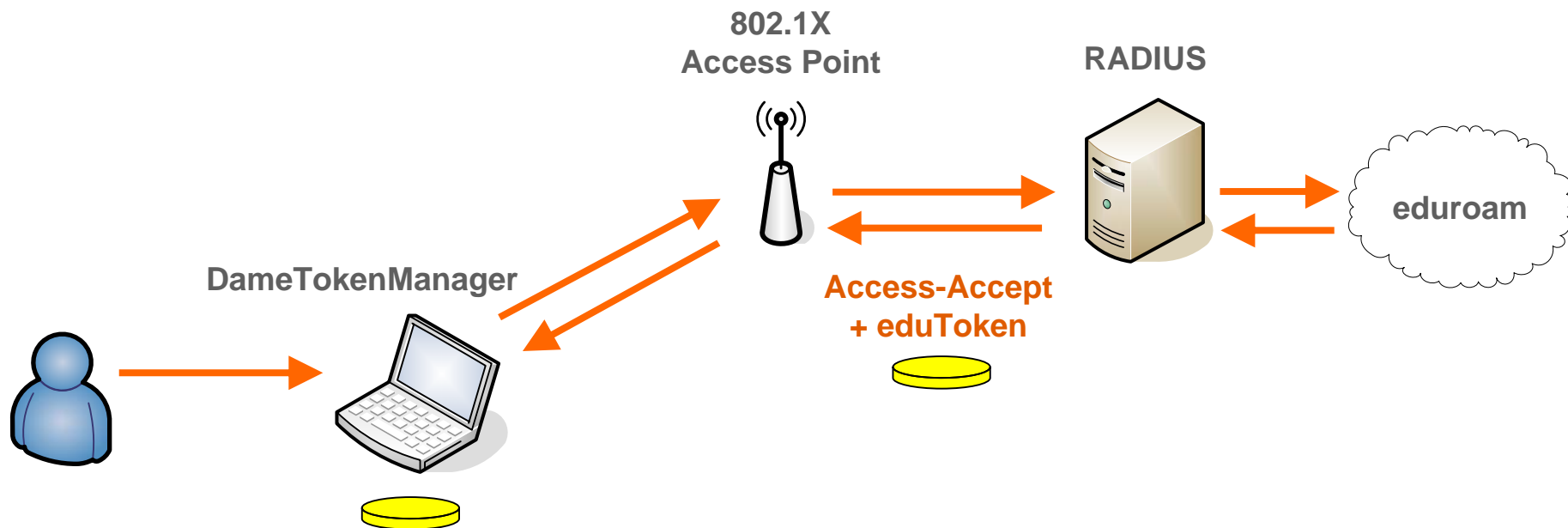
uSSO Workflow



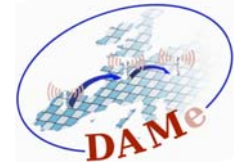
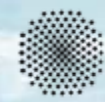


RUS

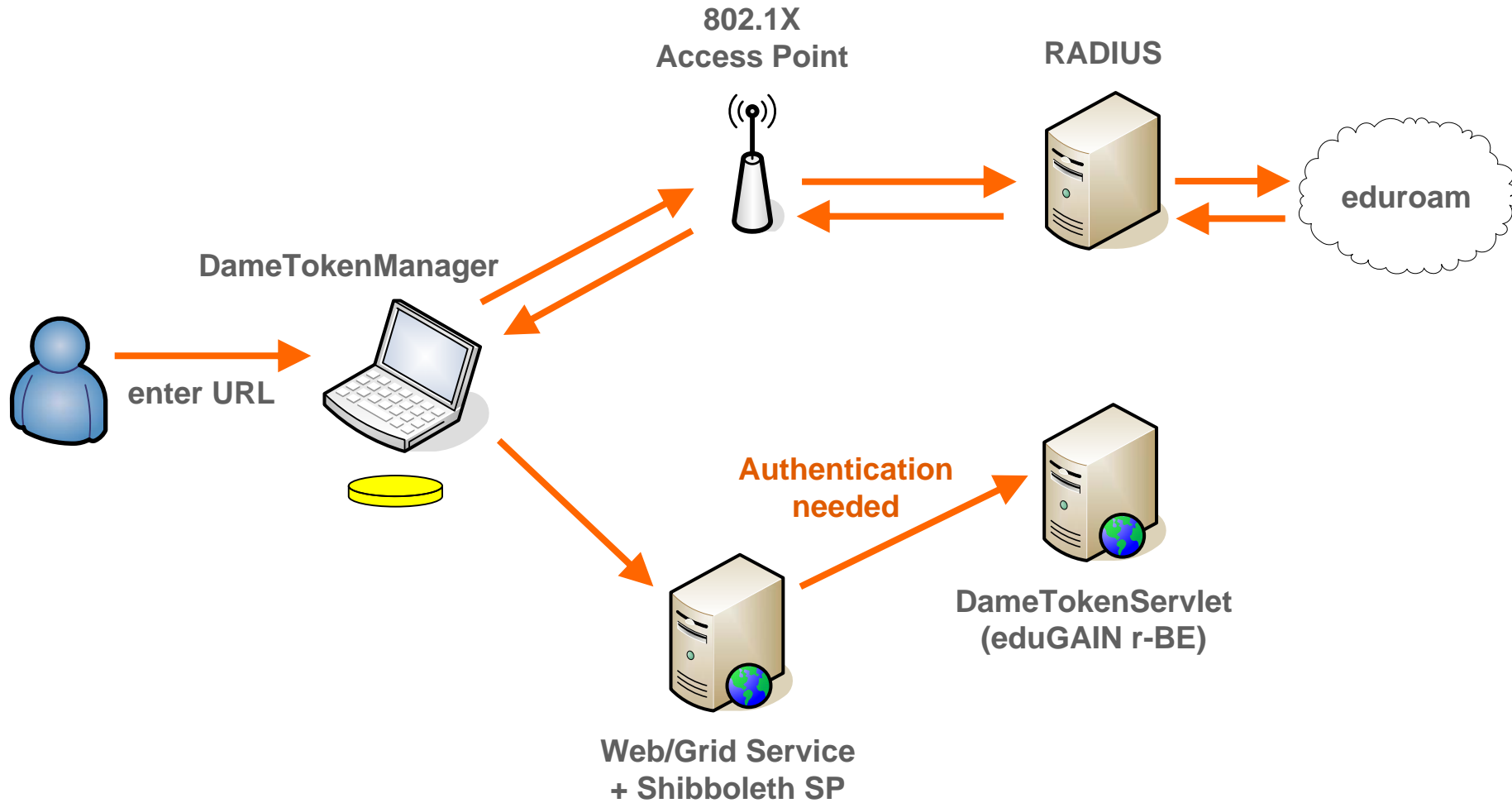
uSSO Workflow

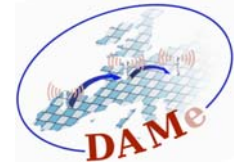
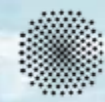


DAME Project

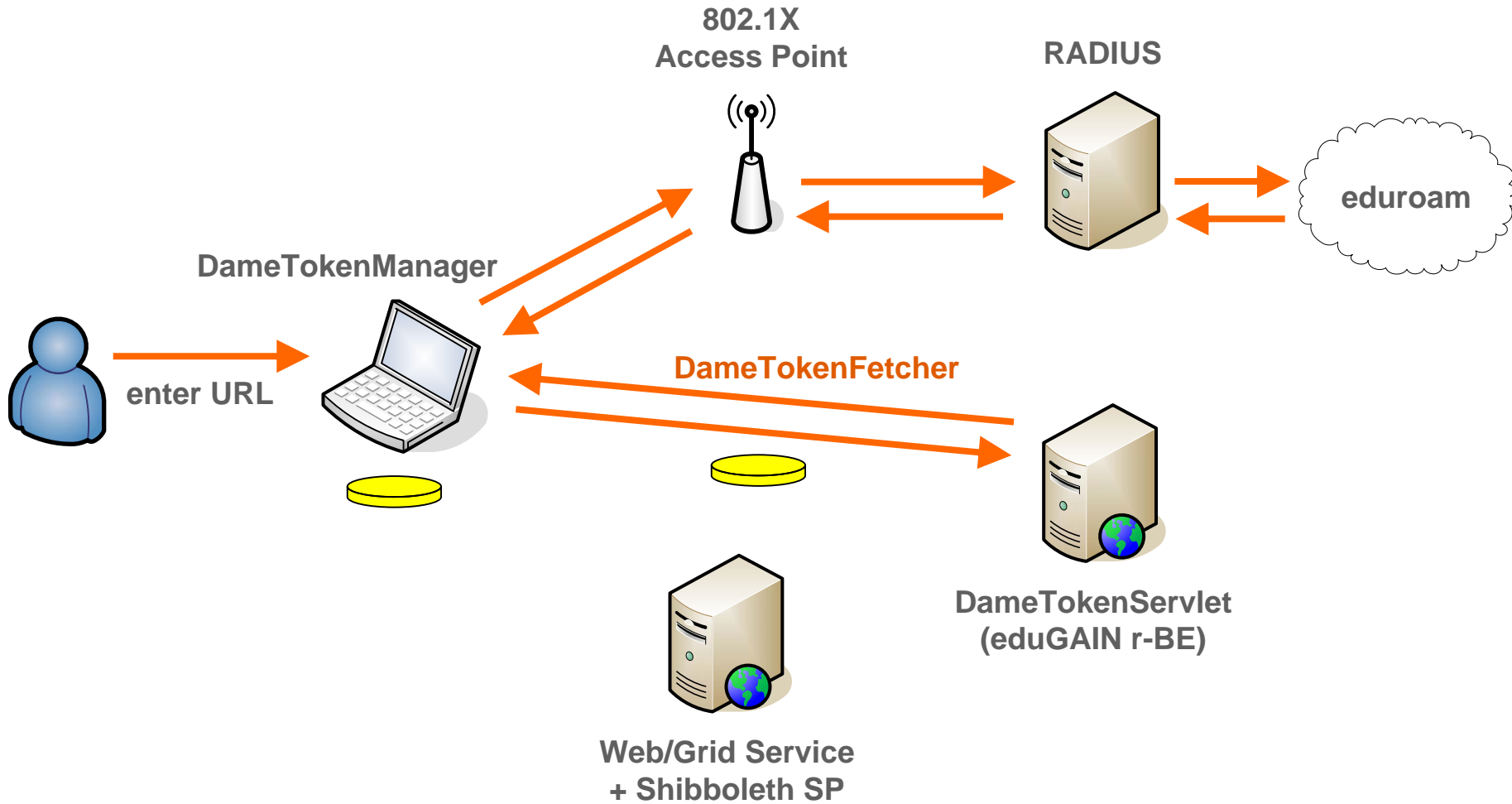


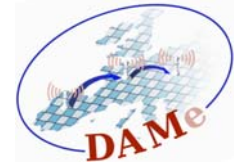
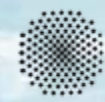
uSSO Workflow





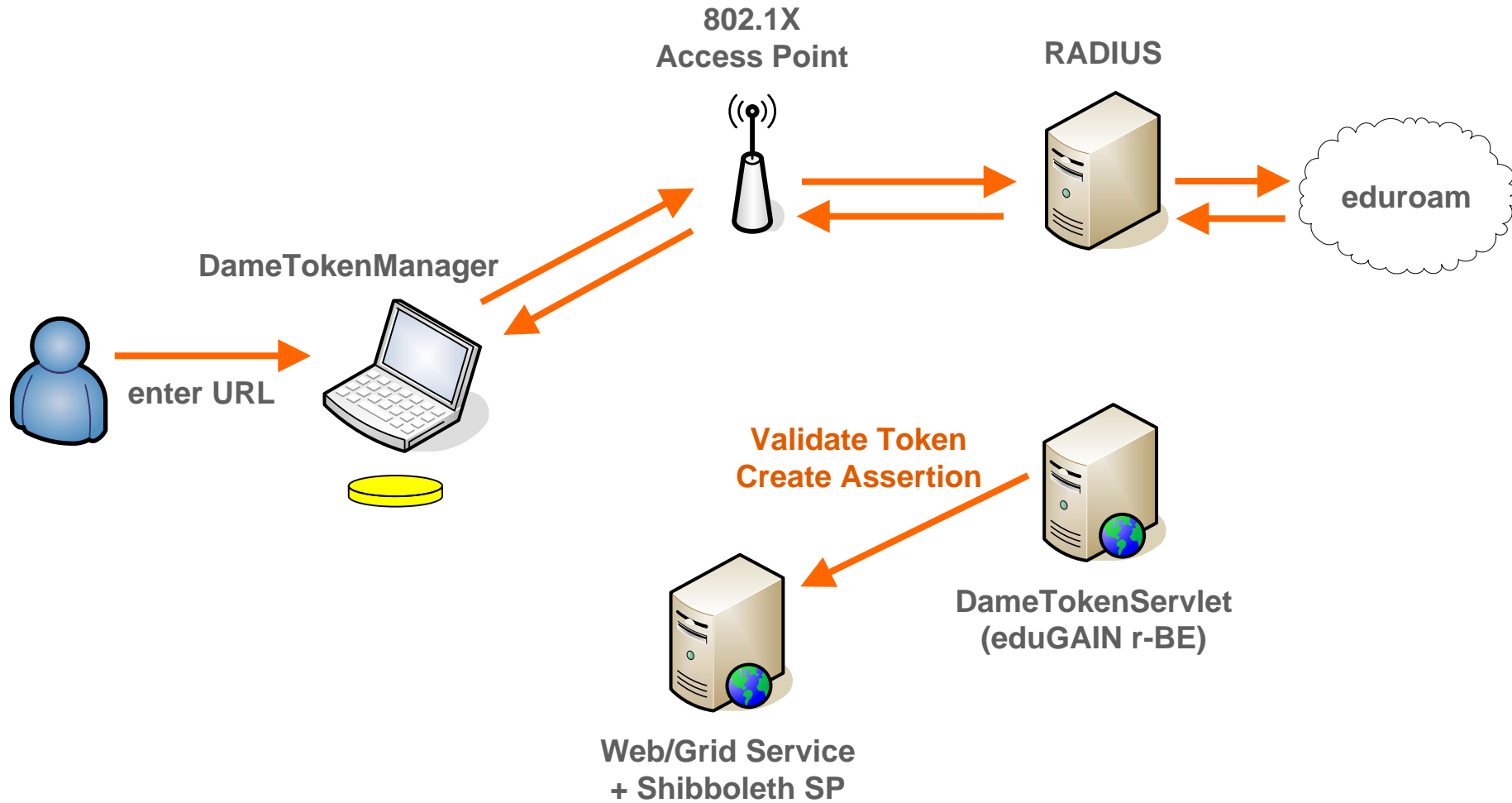
uSSO Workflow

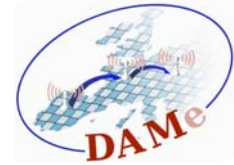
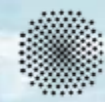




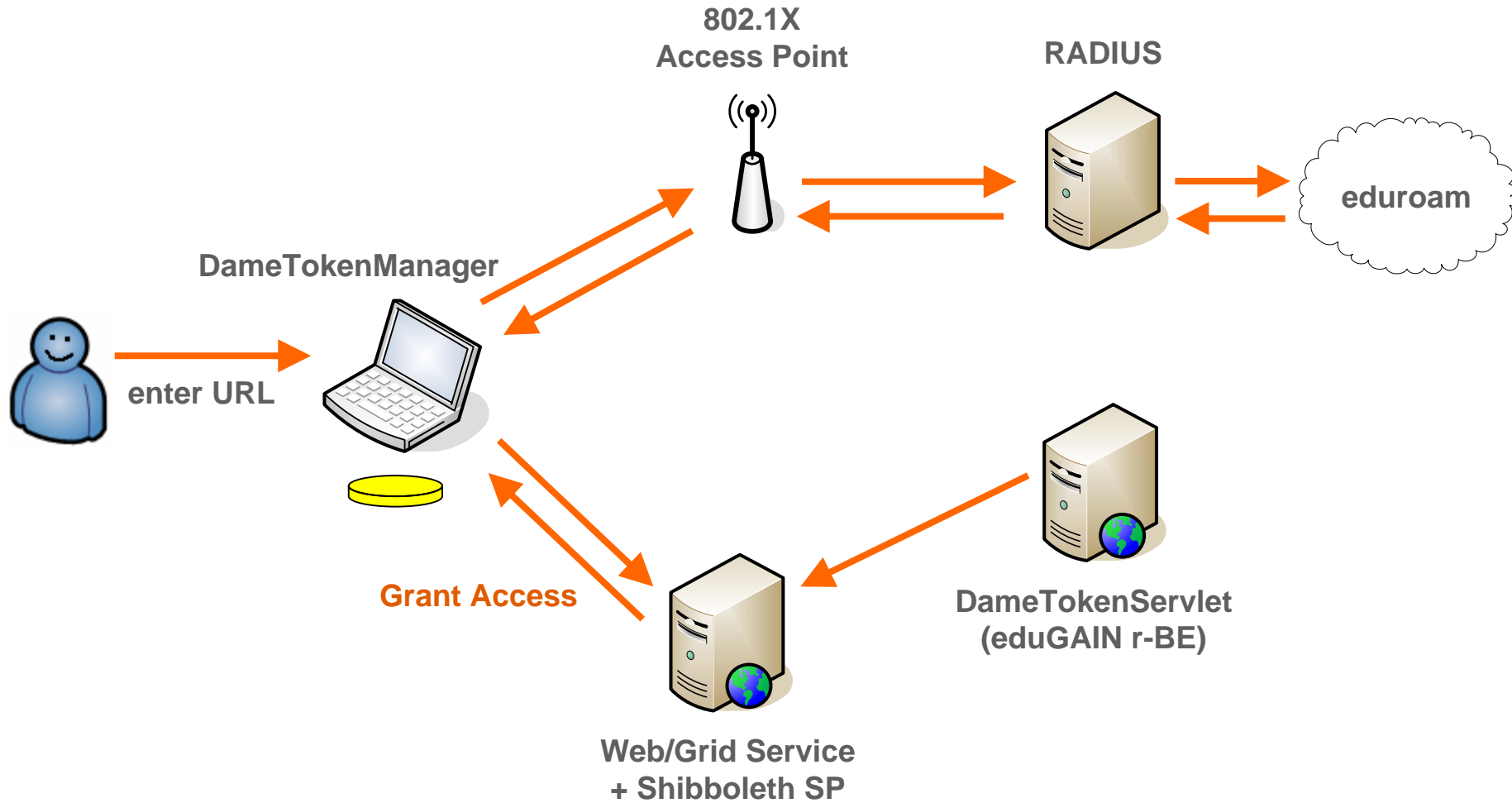
RUS

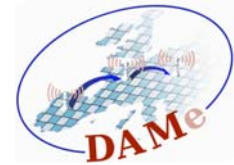
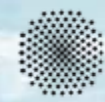
uSSO Workflow





uSSO Workflow





Questions?

Any questions or comments?



Visit the DAMe website: <http://dame.inf.um.es/>

... see you @ DAMe-2 ☺