



Authorisation in eduGAIN

Cándido Rodríguez, RedIRIS

7th NRENs and Grids

Dublin, 1st September 2008



Connect. Communicate. Collaborate

Outline

- **A brief overview of eduGAIN**
- Authorization in eduGAIN
- Future work for non-web applications

A brief overview of eduGAIN



Connect. Communicate. Collaborate

- Based on the national federations, operated by NRENs, but not limited to this technically
- eduGAIN is a confederation infrastructure
 - Federates federations (adding interfederation issues)
- SAML 1.1 (and soon SAML 2.0) is the lingua franca
- Specific software developed
 - eduGAIN base libraries (Java)
 - simpleSAMLphp (PHP)
 - eduGAINFilter (javax.servlet.filter)
- Direct use of Shibboleth 2.0 being investigated

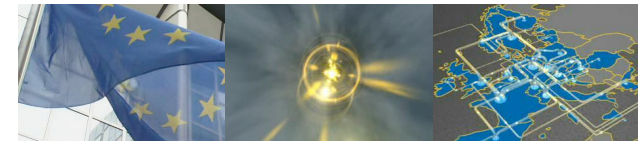
A brief overview of eduGAIN



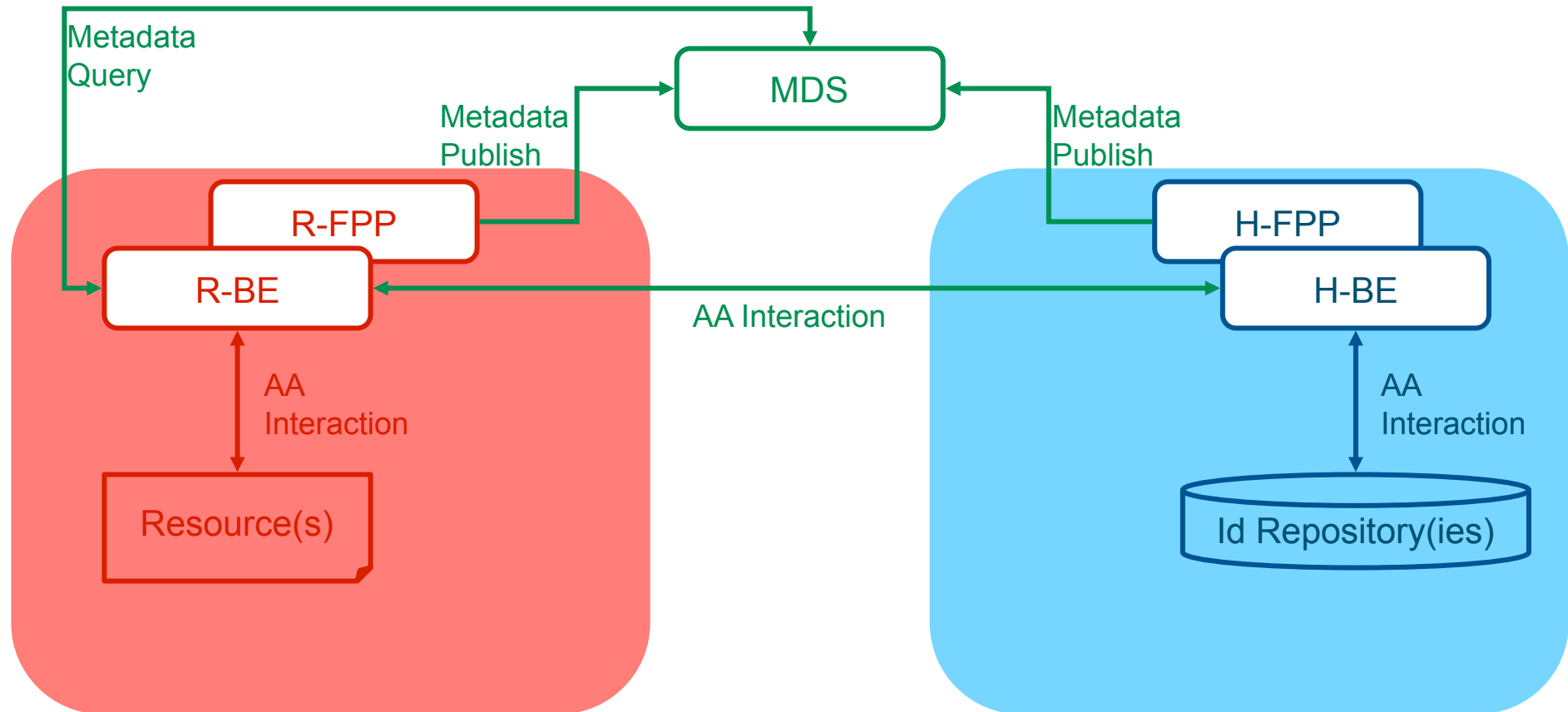
Connect. Communicate. Collaborate

- **Shibboleth**: InCommon (US), SWITCHaai, HAKA, Ukerna/JISC, DFN-AAI, GRNET, HUNGARNET, probably more
- **PAPI**: RedIRIS, EFDA federation
- **simpleSAMLphp**: Feide (under test), RESTENA, WAYF.dk, GIdP, a growing community world-wide
- **A-Select**: SURFfederatie
- **AAI@EduHr**: RADIUS-based
- Different technologies, even with identical technology different policy and purpose -> interfederation soup

A brief overview of eduGAIN



Connect. Communicate. Collaborate



A brief overview of eduGAIN



Connect. Communicate. Collaborate

- Metadata Service MDS
 - Repository of metadata of all connected IdP and SP
 - Upload by authorised components (FPP/BE)
 - Queries possible, WFAYF for user selection or automated
- PKI: component ID used in certificates, eduGAIN SCA (CSR, CRL, CP/CPS)
- URN: components names, protocols etc
- Web site: www.edugain.org portal and info (under reconstruction)
- Attribute mapping or Credential Conversion service (different schemas might be used)
- Other elements still under development!



Connect. Communicate. Collaborate

Outline

- A brief overview of eduGAIN
- **Authorization in eduGAIN**
- Future work for non-web applications



Connect. Communicate. Collaborate

Authorization in eduGAIN

- Two ways of doing the authorization
 - Send an Authorization request to the user's H-BE
 - It requires H-BE has implemented the authorization interface
 - AuthR policy is managed in the H-BE
 - Resources cannot manage it!
 - Send an Attribute request to the user's H-BE and implement a local authority engine
 - A Java library will be provided based on XACML 1.1

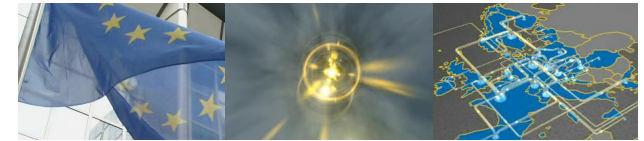


Connect. Communicate. Collaborate

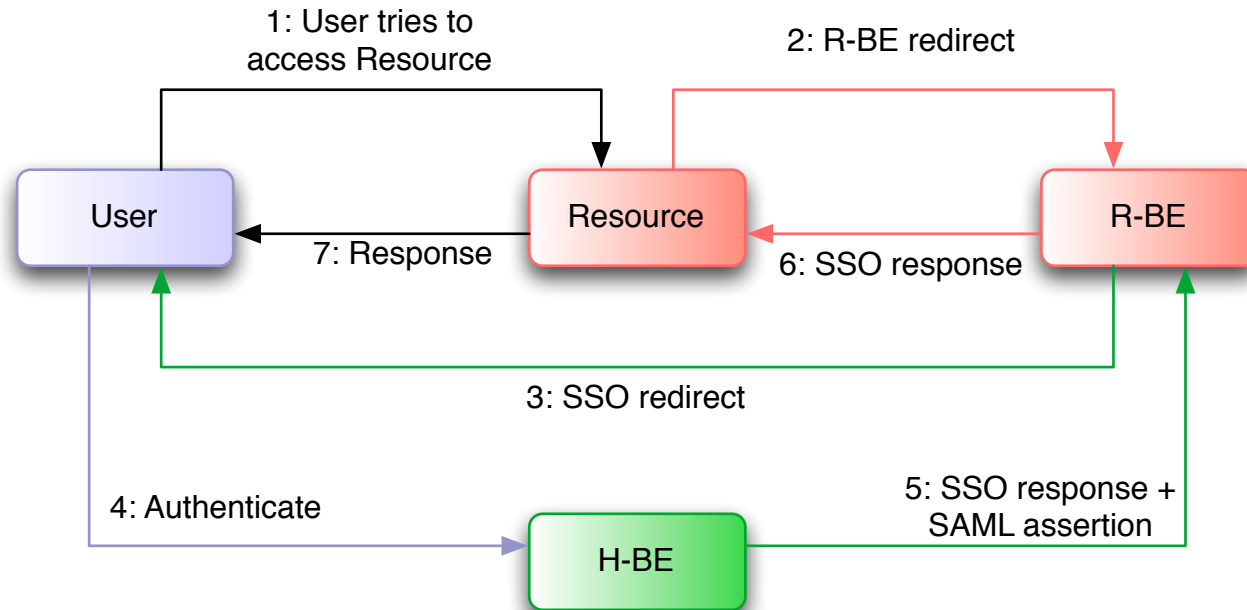
Authorization in eduGAIN

- Different clients - different profiles
 - Web SSO profile: stand-alone web-based application
 - *Automated Client (AC) profile*: client without human interaction
 - *Client in a Web containEr (WE) profile*: web-based applications
 - *User behind a Client (UbC) profile*: non web-based applications
- Transmission of credentials *except Web SSO profile*
 - Clients send security tokens representing themselves
 - Web Service Security (WS-SEC) standard

Authorization in eduGAIN: Web SSO profile

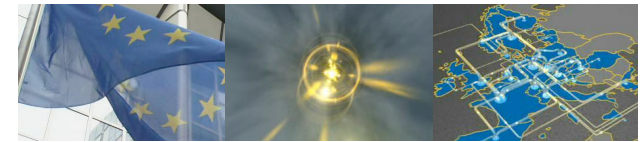


Connect. Communicate. Collaborate

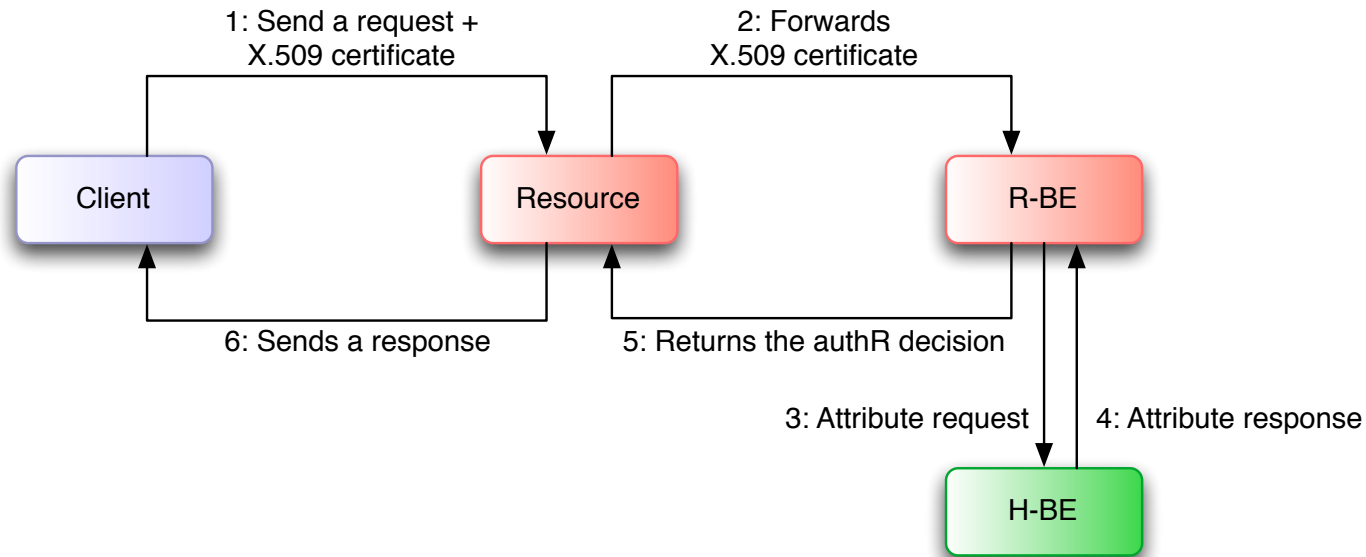


- Typical Web Single-Sign On scenario
 - Authorization could be done in both R-BE and Resource
- Behaviour 100% like a Service Provider protecting a resource

Authorization in eduGAIN: AC profile

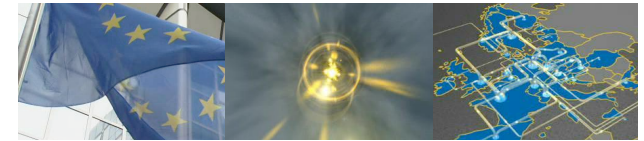


Connect. Communicate. Collaborate

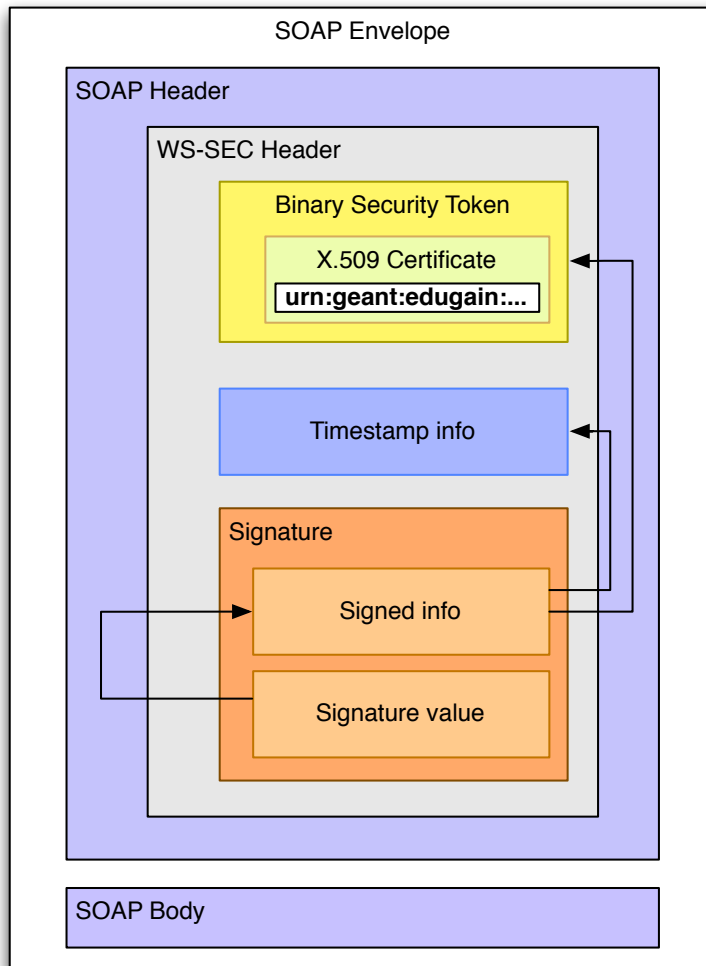


- Unique and non-transferable ID for each client
 - URN obtained from eduGAIN registry service
- Private and public key valid in the eduGAIN trust model
 - Subject Alternative Name of the cert contains the URN
 - Obtained from eduGAIN PKI
- Authentication information is based on the X.509 certificate

Authorization in eduGAIN: AC profile

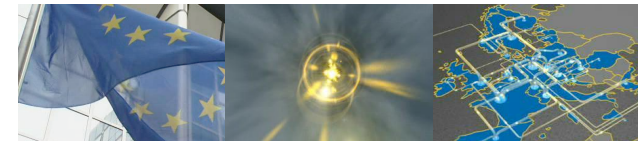


Connect. Communicate. Collaborate

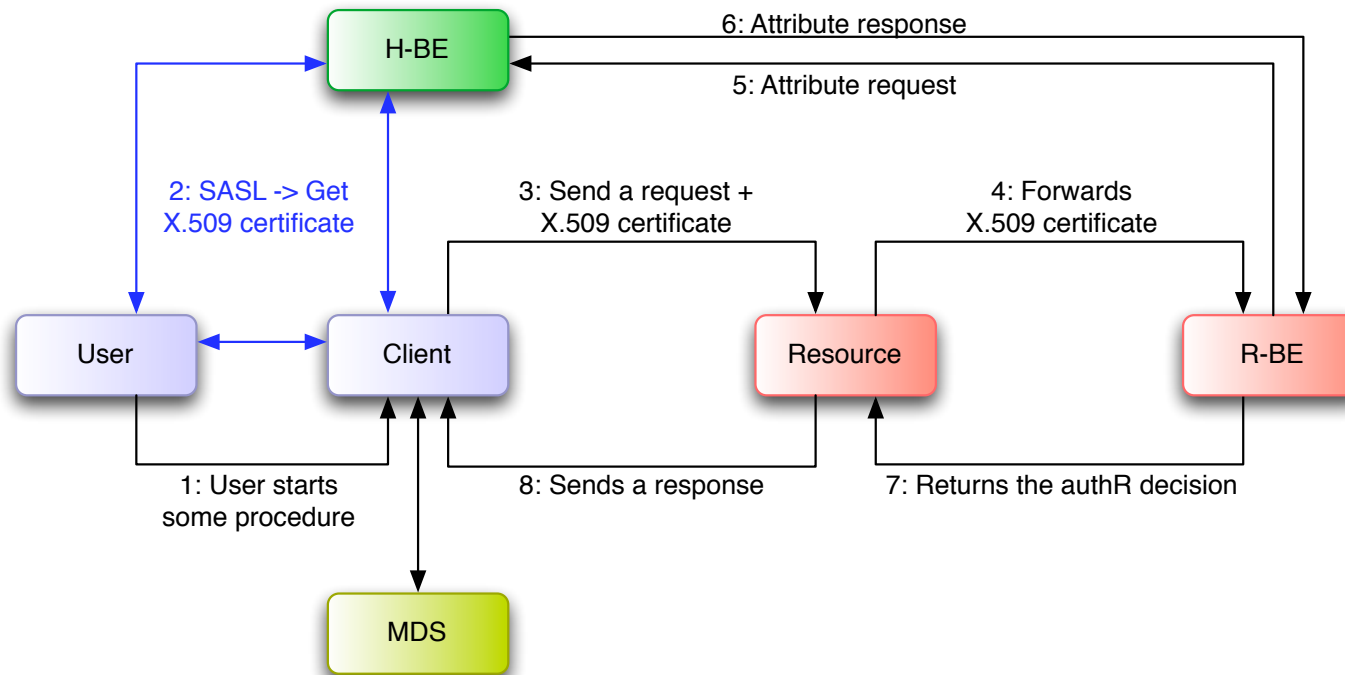


- Authentication data included in the SOAP header
 - Certificate of the client sent following the X.509 profile of WS-SEC
- Generation of the ws-sec element is a proof of the authenticity of the client
- Certificate contains the component ID
 - It is used for the Subject in the Attribute Request

Authorization in eduGAIN: UbC profile

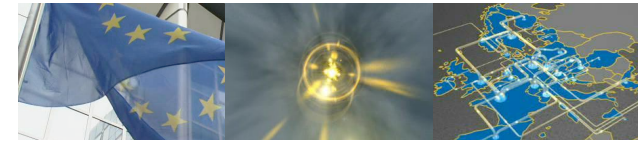


Connect. Communicate. Collaborate

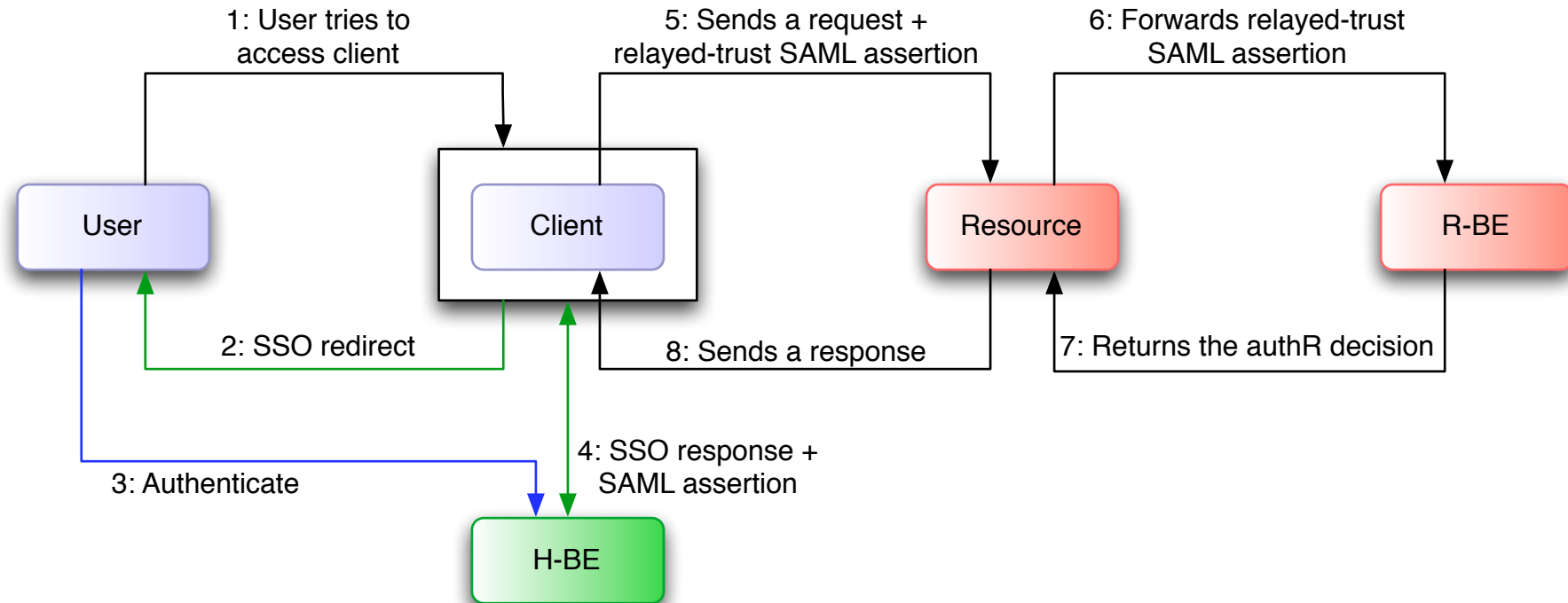


- A similar case than AC
 - Online CA for getting the certificate
 - SASL CA

Authorization in eduGAIN: WE profile

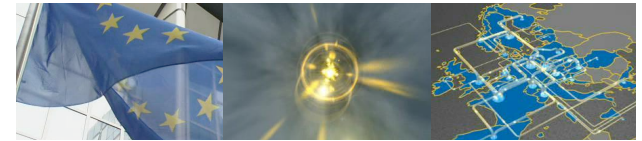


Connect. Communicate. Collaborate



- SAML assertions contain user's credentials
- Clients must have a pair of keys valid in the eduGAIN trust model

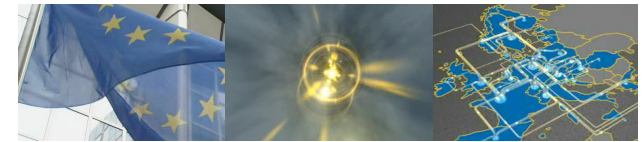
Authorization in eduGAIN: WE profile



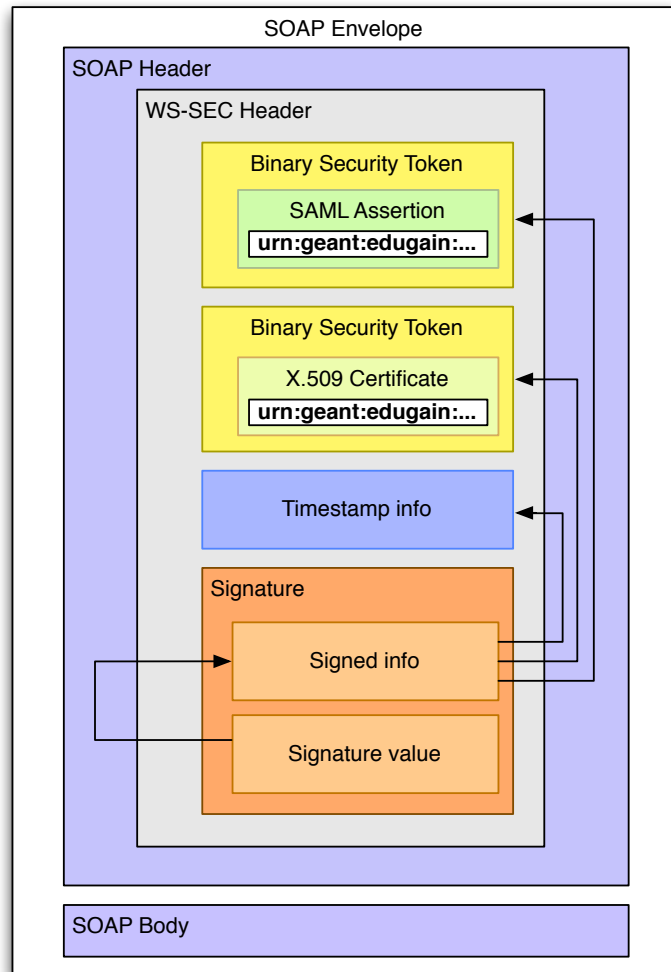
Connect. Communicate. Collaborate

- Constraints of the relayed-trust SAML assertion
 - It must be bound to the client by the H-BE
 - User's credentials legally obtained
 - It must be bound to the resource by the client
 - Malicious resource cannot re-use it
- This SAML assertion contains
 - `AudienceRestrictionCondition` element with the component ID of the resource
 - Authentication statement
 - `ConfirmationMethod` element containing the value `relayed-trust`
 - `SubjectConfirmationData` has the SAML assertion got from the H-BE

Authorization in eduGAIN: WE profile



Connect. Communicate. Collaborate



- Authentication data included in the SOAP header
 - Relayed-trust SAML assertion sent following the X.509 and SAML profiles of WS-SEC
- Certificate contains the component ID of the client
- Subject of the SAML assertion used for requesting its attributes



Connect. Communicate. Collaborate

Outline

- A brief overview of eduGAIN
- Authorization in eduGAIN
- **Future work for non-web applications**

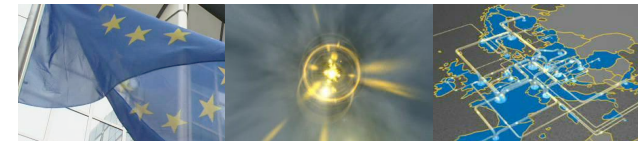
Future work for non-web applications



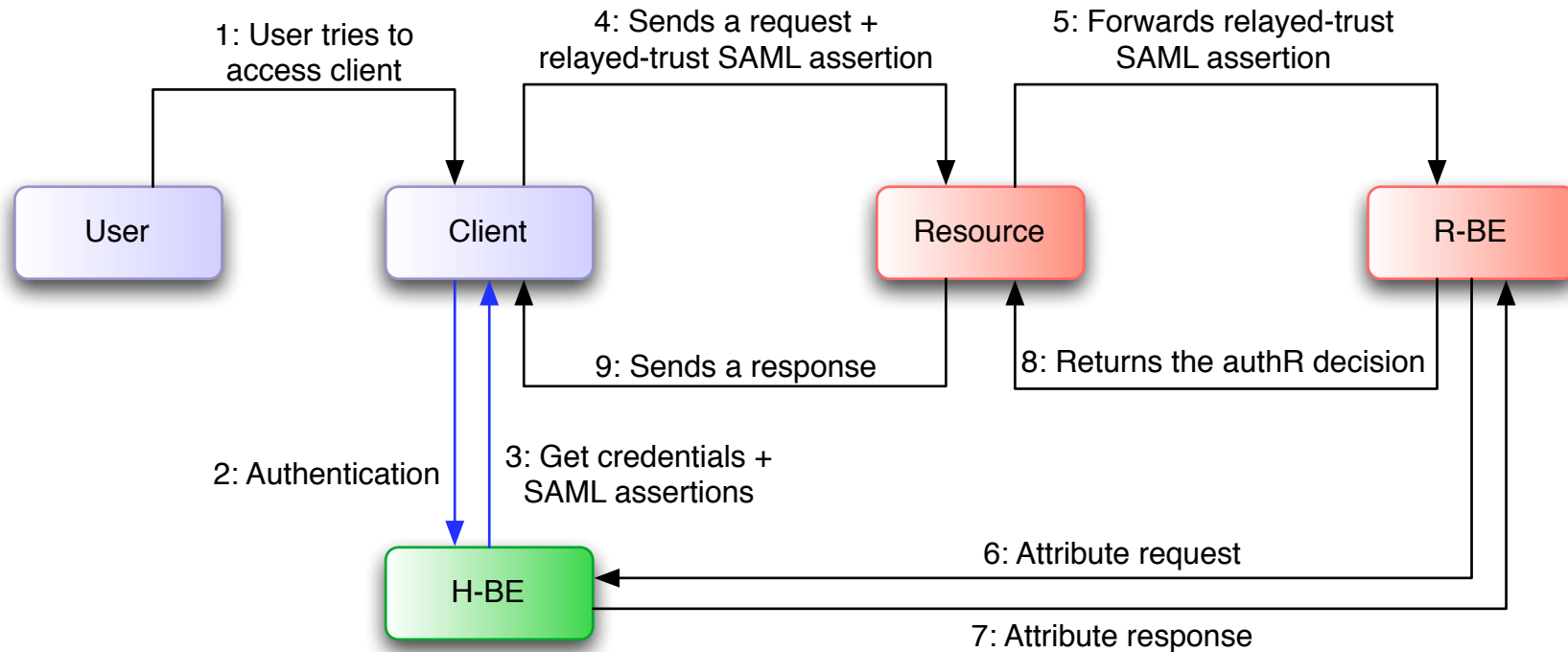
Connect. Communicate. Collaborate

- UbC profile isn't being adopted by organizations
 - Based on an online CA
 - They don't want it!
 - Technically, it doesn't fit very well
- A new profile is coming from DICE
 - It can cover the AC profile too
 - It is based on relayed-trust SAML assertions

Future work for non-web applications

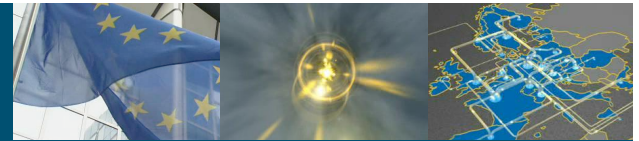


Connect. Communicate. Collaborate



- **Protocols of authentication**
 - RADIUS
 - DAME project
 - HTTP Auth

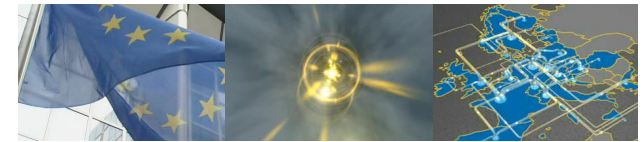
Future work for non-web applications



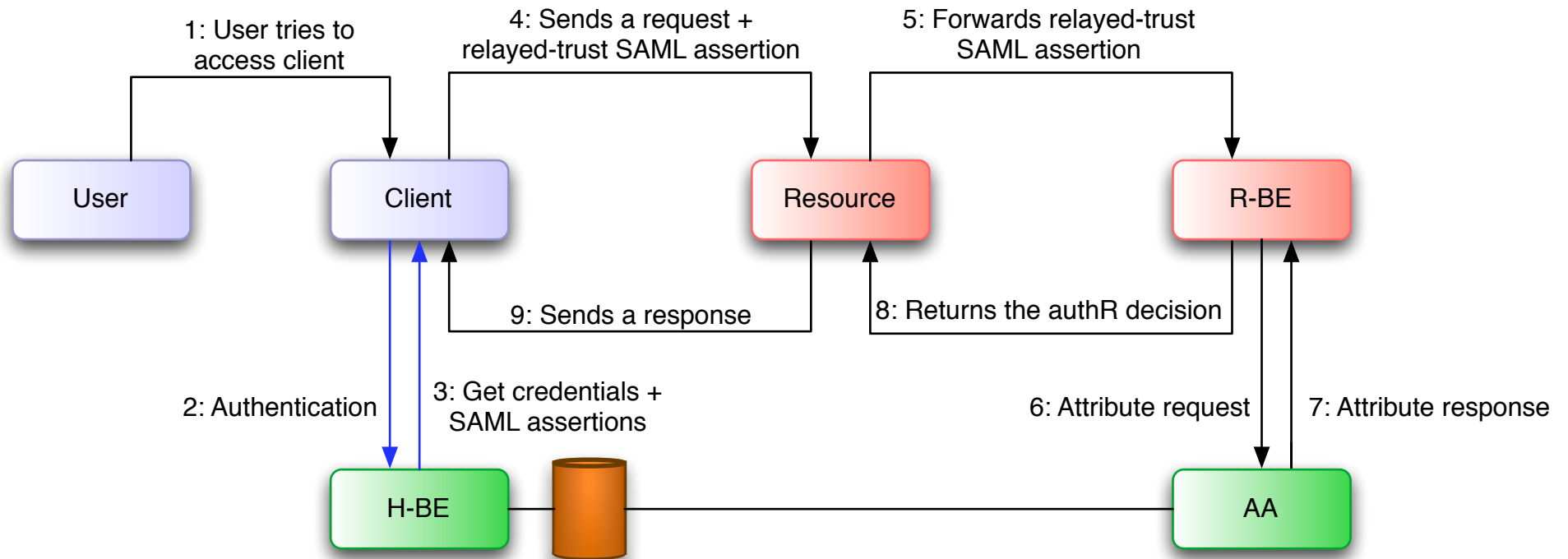
Connect. Communicate. Collaborate

- This new profile could find problems with the war between:
 - Attribute push VS Attribute pull
- Attribute authorities outside the IdP bring the solution
 - It allows attribute requests without starting an initial context

Future work for non-web applications



Connect. Communicate. Collaborate



- R-BE has configured a list of Attribute Authorities
- AA is connected to a set of Attribute Stores



Connect. Communicate. Collaborate

Thank you for your attention!

Any questions?