



# Federation Interoperability Made Possible By Design: eduGAIN

Diego R. Lopez (RedIRIS)



Connect. Communicate. Collaborate

# The Goal of AAI within GN2

- To build an interoperable authentication and authorisation infrastructure that will be used all over Europe enabling seamless sharing of e-science resources
- We started from
  - Scattered AAI (pilot) implementations in the EU and abroad
  - The basic idea of federating them, preserving hard-won achievements



Connect. Communicate. Collaborate

# The eduGAIN Model

- Use a set of interconnection points (Bridging Element, BE) at each federation
- Announce BE metadata through the FPP (Federation Peering Point)
- Distribute these metadata through the Metadata Service (MDS)
- Metadata is retrieved through the eduGAINMetaQuery API and delivered to the requesting BE
- BEs exchange data using the eduGAIN SAML-based profiles
- Interactions are based upon the eduGAIN trust model



Connect. Communicate. Collaborate

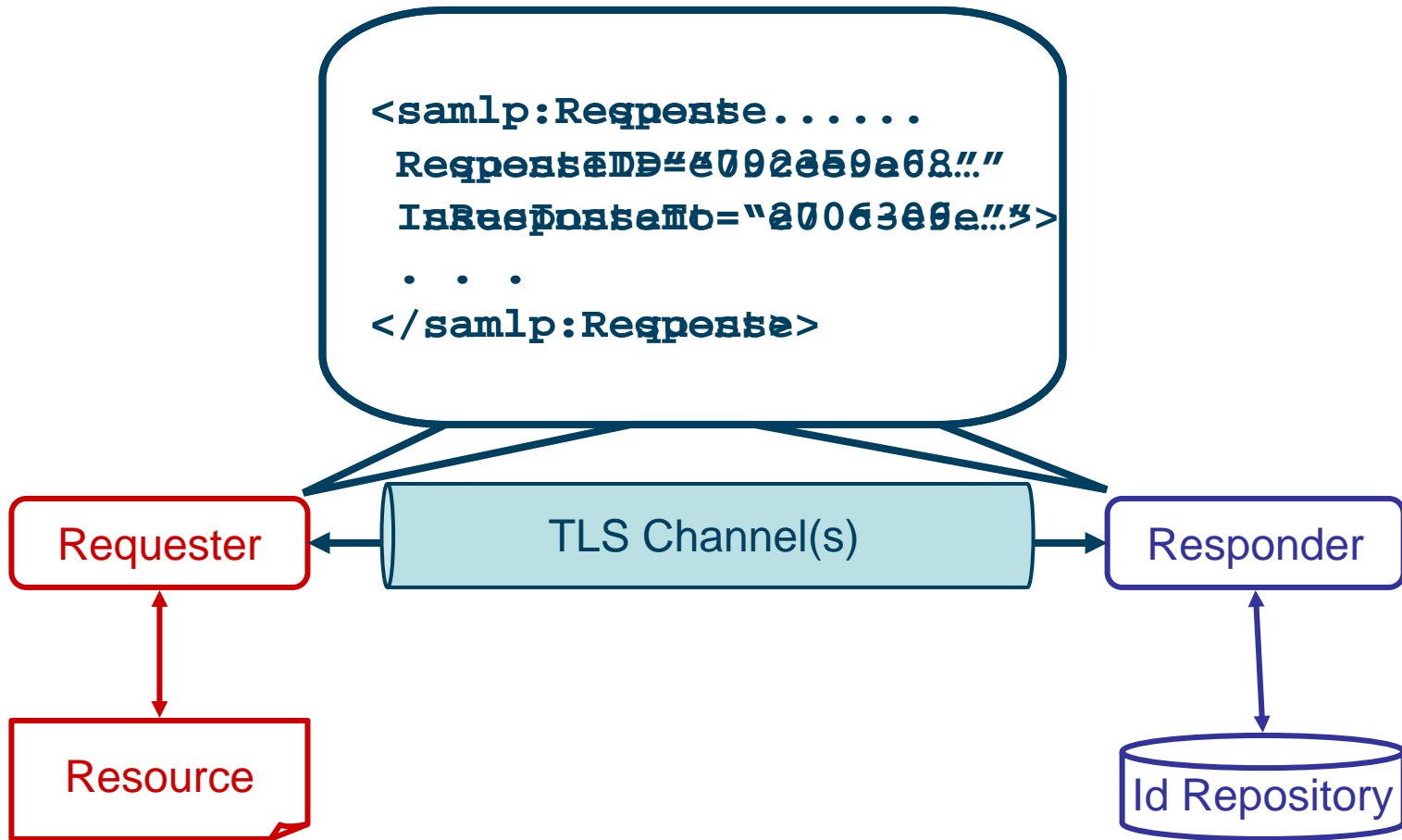
# eduGAIN Operations

- Defined in abstract terms, following the SOA paradigm
  - Metadata Service (MDS)
  - Authentication Service (AuthN)
  - Attribute Exchange Service (Attr)
  - Authorisation Service (AuthZ)
- Formally defined parameters for each operation
- Bindings defined for SAML 1.1 and part of SAML 2.0
  - Plans for evolving these bindings as required

# A general model for eduGAIN interactions



Connect. Communicate. Collaborate





Connect. Communicate. Collaborate

# Component Identifiers

- eduGAIN operations strongly depend on having unique, structured and well-defined component identifiers
- Based on URNs delegated by the eduGAIN registry to the participating federation
- Identifiers establish the kind of component they apply to by means of normalized prefixes
- Identifiers follow the hierarchy of the trust establishing process
  - Including the identifiers of the federation (and BE) the component is using to connect to eduGAIN



Connect. Communicate. Collaborate

# Some identifier examples

- A typical FPP identifier

```
urn:geant:edugain:component:fpp:starfleet
```

- A typical BE identifier

```
urn:geant:edugain:component:be:starfleet:enterprise
```

- A typical SP identifier

```
urn:geant:edugain:component:sp:starfleet:enterprise:  
captainlog:http://enterprise.starfleet.sf/logs/cap  
tain/
```

- A typical IdP identifier

```
urn:geant:edugain:component:idp:starfleet:enterprise  
:roll
```



Connect. Communicate. Collaborate

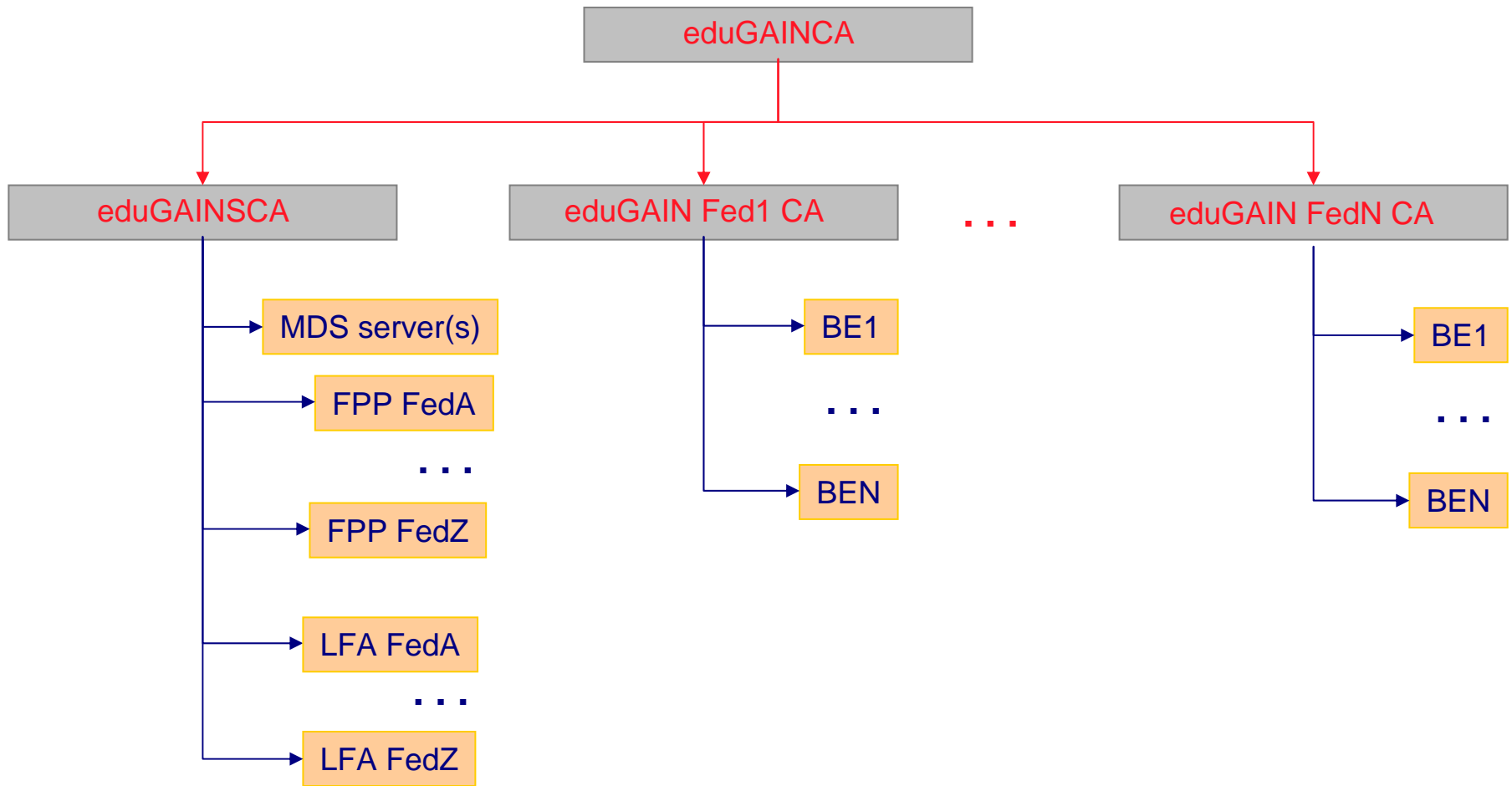
# eduGAIN Trust Fabric

- Based on a PKI
- Validation procedures include
  - Normal certificate validation
    - Trust path evaluation, signatures, revocation,...
  - Peer identification
    - Certificates hold the component identifier
    - It must match the appropriate metadata
- Applicable to
  - TLS connections between components
    - Two-way validation is mandatory
  - Verification of signed XML assertions



# eduGAIN CA Hierarchy

Connect. Communicate. Collaborate





Connect. Communicate. Collaborate

# Metadata Service

- Based on REST interfaces transporting SAML 2.0 metadata
- Metadata are published through POST operations
- Metadata are retrieved through GET operations

- URLs are built as

`MDSBaseURL/FederationID/entityID?queryString`

- Using component names
- The `queryString` transports data intended to locate the appropriate home BE (Home Locators)
  - Usually, coming from hints provided by the user

# General eduGAIN Operation Mapping



Connect. Communicate. Collaborate

- Current version is based on SAML 1.1
  - Profiling the standard to fit abstract parameters
  - Component identifiers play their role again
- A SAML 2.0 implementation will be available along the lifetime of the project
  - The abstract service specification protects components and applications from these changes
- Authentication assertions and attribute exchange mechanisms are designed to be Shibboleth 1.x compatible
  - And Shibboleth 2.0 in the future



Connect. Communicate. Collaborate

# eduGAIN API Structure

- The eduGAIN APIs are the common libraries for all eduGAIN components
  - Direct implementation of the eduGAIN service definition
  - And also available to local requesters and responders
- Building blocks:
  - eduGAINVal: Validation procedures
  - eduGAINBase: Adapt the abstract service definition
  - eduGAINMetaQuery: Queries to the Metadata Service
  - eduGAINMetaPub: Publication at the Metadata Service

# A layered Model for Implementation



Connect. Communicate. Collaborate

Component logic

eduGAINBase + eduGAINVal + eduGAINMeta\*

SAML library ▲ OpenSAML

SOAP/TLS/XMLSig libraries ▲ Shibboleth components whenever possible



Connect. Communicate. Collaborate

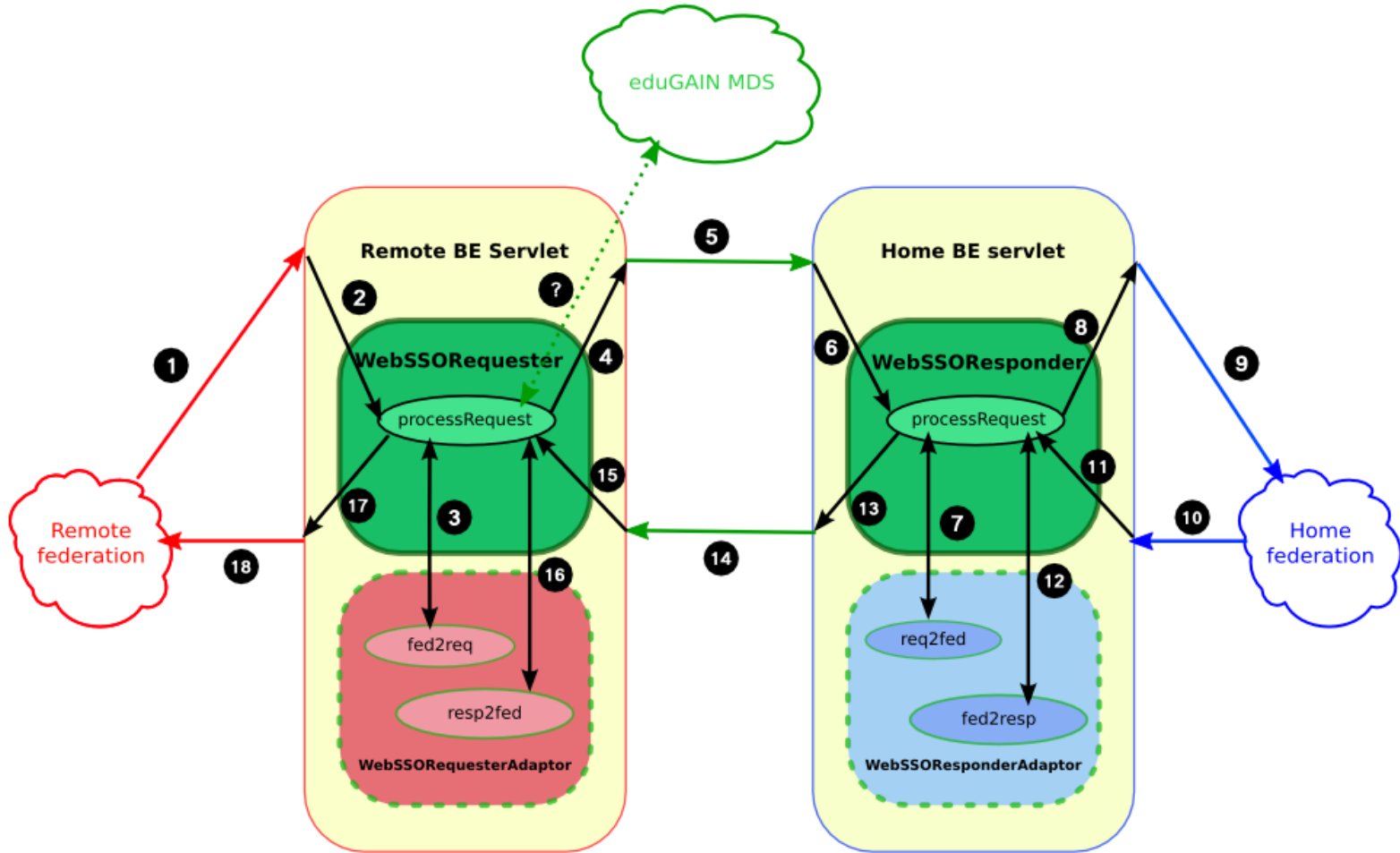
# eduGAIN Profiles

- Define the precise exchange of messages and the processing rules for these messages in particular use cases
- Two profiles defined so far
  - Web SSO (Shibboleth compatible)
  - Automated client (no human interaction)
- Others envisaged
  - Extended Web SSO (allowing the send of POST data)
  - Non-web applications (based on Web SSO)
  - eduGAIN usage from roaming clients (DAMe)



# eduGAIN Profiles: Web SSO

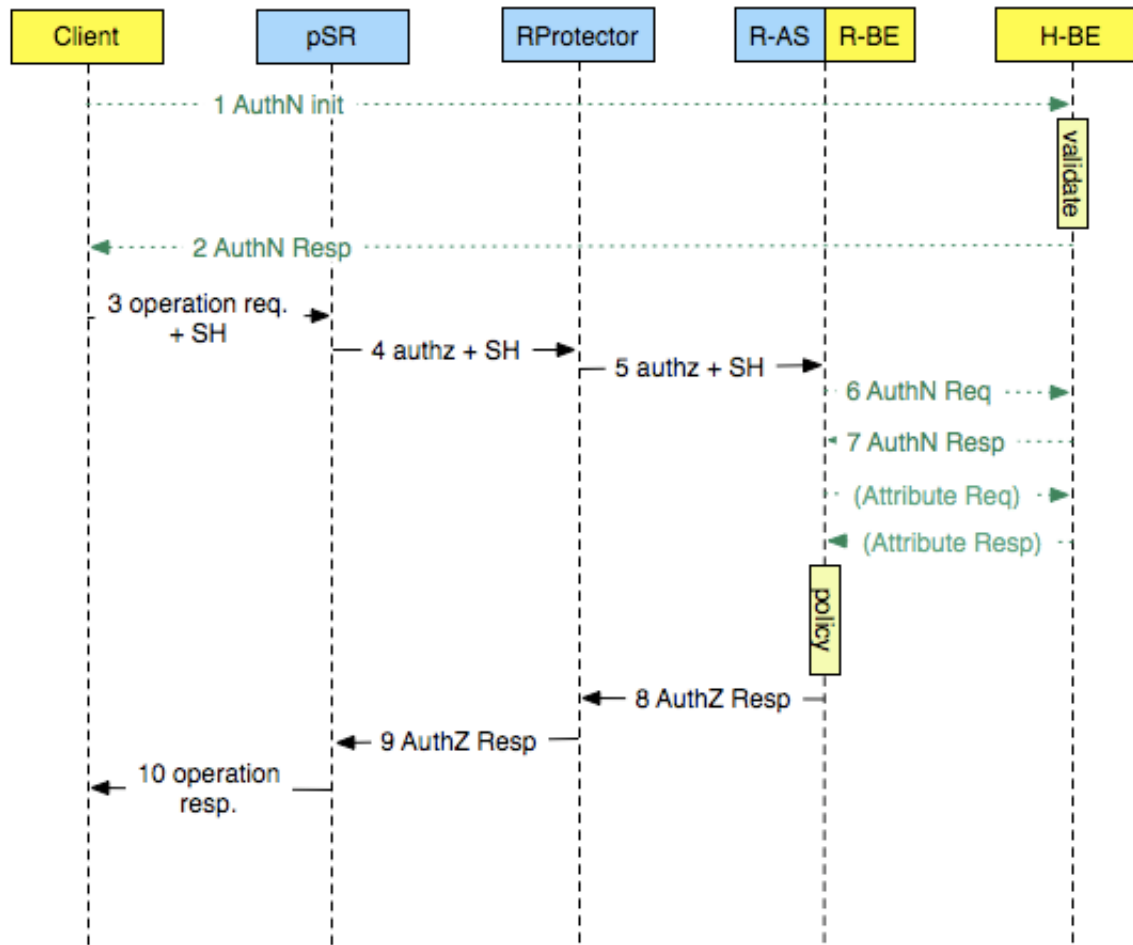
Connect. Communicate. Collaborate



# eduGAIN Profiles: Automated Client



Connect. Communicate. Collaborate





Connect. Communicate. Collaborate

# Where We Are

- Implementing the eduGAIN APIs
- Polishing profiles
  - Through interaction with user activities
- Preparing the first version of a cookbook
  - Deployment and component implementation guidelines
- First pilot to be run around 4th quarter of this year
- Establishing links with other potential user communities beyond the GN2 project
- Policy is on its way