red.es

RedIRIS

European Efforts towards a Global AAI Infrastructure

Diego R. Lopez
RedIRIS

red.es

Where We Are Aiming at

- An infrastructure to allow users establish their digital identity and rights inside the European research and academic networks. And beyond
  - Europe is a *little world* by itself
- The three (Spanish) Bs:
  - *Bueno* (Good)
    - Secure, in both user and provider senses
    - Dependable
    - Open
    - Scalable
  - *Bonito* (Nice)
    - Essentially, as seamless as possible
  - *Barato* (Cheap)
    - Do not impose additional burdens on campus/site/network admins
    - Rely on already deployed infrastructures

Where We Start from

- Several operating infrastructures in many countries
  - Home-grown software and policies oriented to solve specific problems, albeit based in the same principles
    - Finland -> HAKA
    - Netherlands -> A-Select
    - Norway -> FEIDE
    - Spain -> PAPI
    - Sweden -> SWAMI
    - Switzerland -> SWITCH-AAI
    - UK -> Athens + …
  - P2P compatibility already demonstrated several times
- General consensus on protocols and models
  - Federated solutions
  - SAML and related protocols
- The will of seeking a global solution (worldwide)

The Confederation Idea

- A loosely-coupled set of cooperating identity federations
  - Subject to less restrictive policies
- Identity management and AuthN/AuthZ must be properly handled by the participating federations
  - Though last-resort elements could be provided by the confederation itself
- Dynamical establishment of trust links
  - Metadata publication and retrieval plays a key role
  - Trust links are necessarily weaker than inside participating federations

- The TERENA Academic CA Repository
- A PKI-based web of trust among the global academic and research community
  - Built and maintained by *out-of-band* methods
- Without the technical and administrative burdens of a common root CA or a bridge
  - Lighter than a hierarchy, simpler than a bridge
- Adopted by the Grid community
  - Trust repository for the EUGridPMA and the IGTF
  - Endorsed by the eIRG
- Direct application to the establishment of confederated trust links

TACAR: The Basic Principles

- Keep it simple
  - Do not require extra developments
  - Make the whole system sustainable
- Let it happen
  - Follow a very pragmatic approach
  - Gain critical mass
  - Act according to user organization demands
- The better illustration is the original evolution
  - TACAR was conceived as a simple bundle of certificates to be distributed via a trusted site
  - Policy issues came into play and the TACAR policy was created

TACAR: What Does It Offer

- A single authoritative source for certificates and policies
  - Able to simplify maintenance procedures
- Mechanisms to extend (and strengthen) trust links
  - Grid communities
  - Geographical areas
- Running for two years
  - http://www.tacar.org/
  - 31 root CA available through the repository
- The team is working in a new set of services
  - Trusted introducers to reduce administrative overhead
  - Enhanced back-end
  - Certificate set selection and certificate tagging

TACAR: What Can It Offer

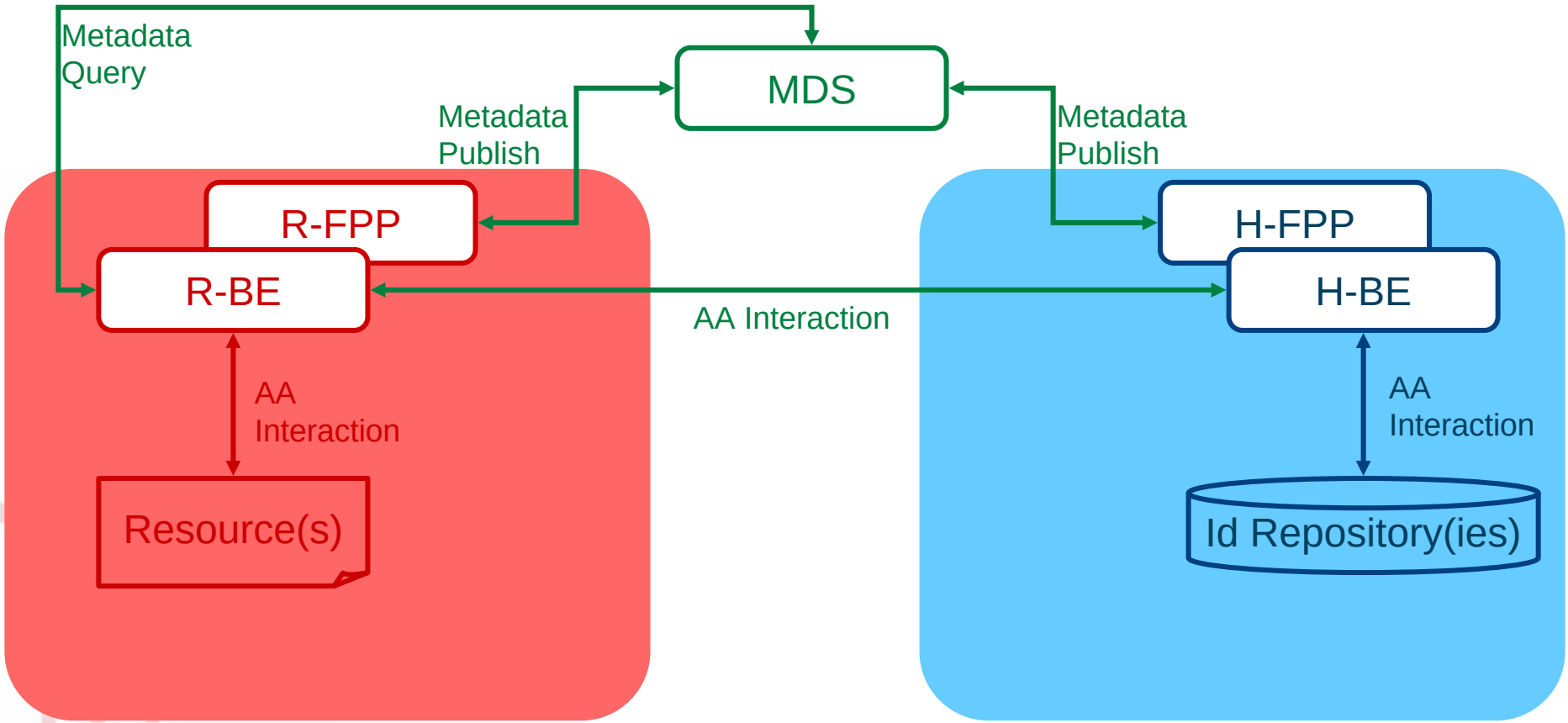
- Extend the use of models based on peer-review
  - Qualified or not
- Support for PKI operation servers
  - OCSP and more
- Simplified trust exchange
  - The (multiple) root(s) for confederations
- Automated policy matching
  - Following 1SCP (One Statement Certificate Policies)

- A model to experiment with
  - Lighter than a common root, simpler than a bridge

eduGAIN: The AAI for GÉANT2

- 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 used by the requesting BE to establish the trust links
- BEs exchange data using the eduGAIN SAML-based profiles

red.es The eduGAIN Model



The 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
  - 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

The eduGAIN Trust Fabric

- Based on PKI and component identifiers
  - 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
  - Verification of signed XML messages
- Identifiers are based on URNs
  - Delegated by the eduGAIN registry to the participating federation
  - Following the hierarchy of the trust establishing process
    - Including the identifiers of the federation (and BE) the component is using to connect to eduGAIN

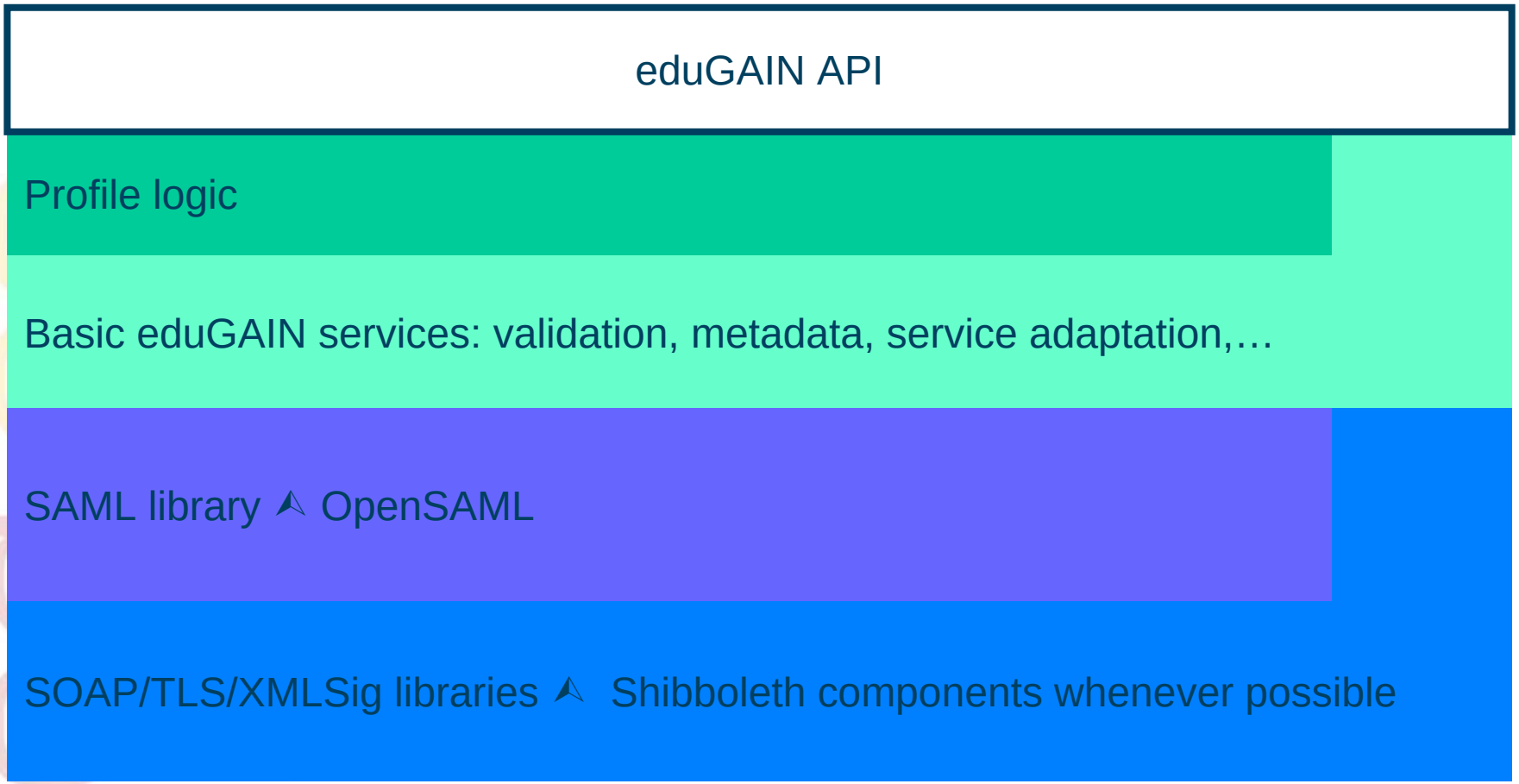
The euGAIN API

- Common libraries for all eduGAIN components
- Implementation of the eduGAIN service definition, metadata access and validation procedures
  - The interface is based on specific classes modeling the abstract definition
    - `AuthNReq` + `AuthNResp`
    - …
- Provides a general abstraction layer for AuthN/AuthZ operations
  - Applicable to components directly woven in the eduGAIN trust fabric
  - And to other elements for interactions within their internal trust zones

The eduGAIN Profiles

- Define the precise exchange of messages and the processing rules for these messages in particular use cases
  - A specific eduGAIN document
  - Joint specification documents for application areas
- Three profiles defined so far
  - Web SSO (current federation interoperability)
  - Automated WS client (no human interaction)
  - Non-web WS client (derived from Web SSO)
- The eduGAIN API provides specific access to elements implementing the profile logic
  - Simpler usage
  - Easier interoperability

A Layered Approach



red.es Where We Are

- Implementing the eduGAIN APIs
- Polishing profiles
- First pilot to be run around 4th quarter of this year
- Establishing links with user communities
  - Inside GÉANT2:
    - JRA1, network monitoring
    - JRA2, security
    - JRA3, bandwidth on demand
  - And beyond
    - The LOBSTER project
    - Grids
- Starting an initiative to connect network access and AAI
  - DAMe = eduroam + eduGAIN