MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

PerfSONAR in SIR

Service Integration through an Identity Hub

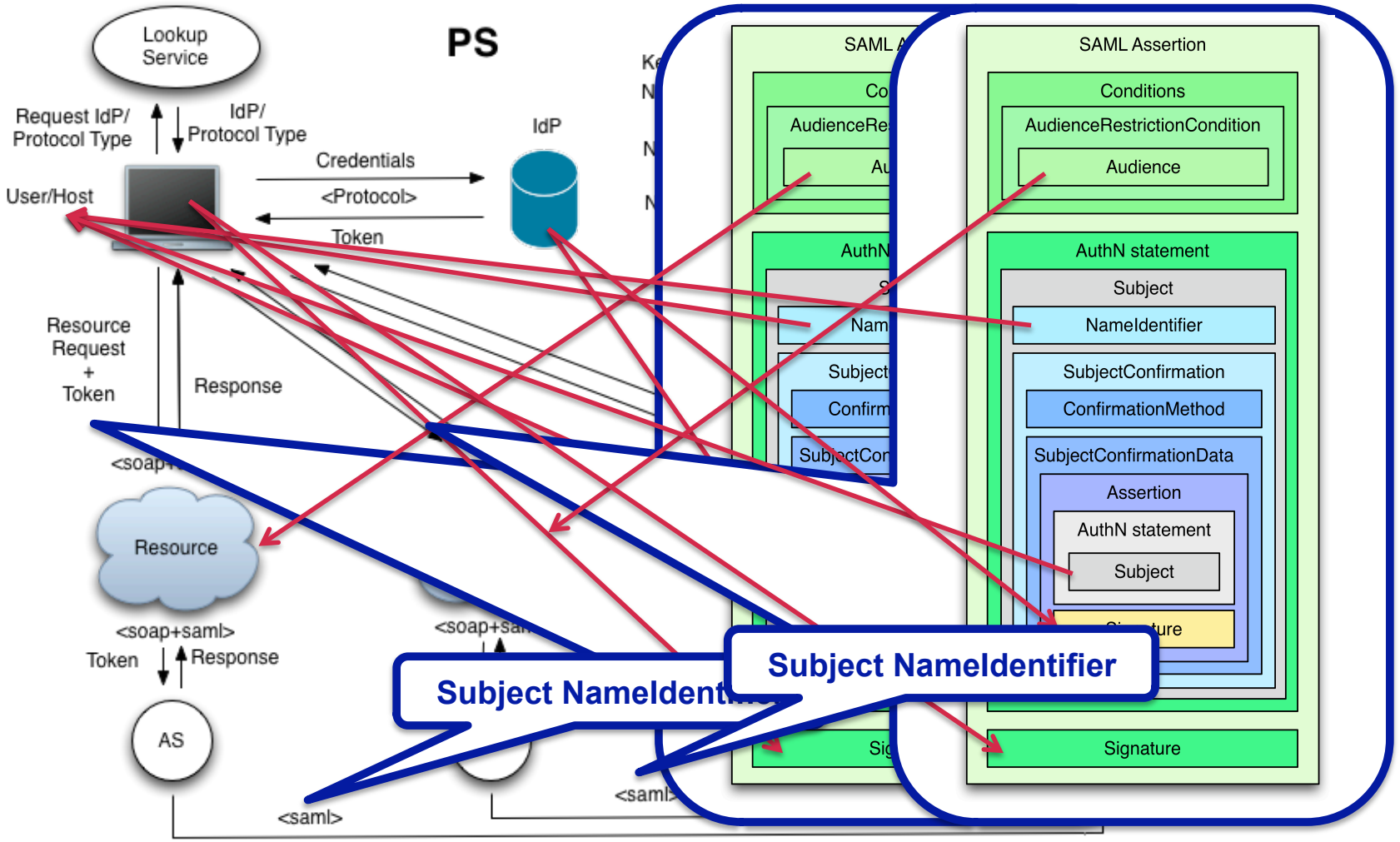
Diego R. Lopez, RedIRIS

RedIRIS

PerfSONAR AAI

- WS infrastructure
- Security based on tokens
  - Which component
  - On behalf of whom
  - Reference for additional attribute retrieval
- Two kind of tokens
  - X509 certificates
  - SAML assertions
- Converging to a STS
  - Both SOAP-oriented and RESTful

Using the PS Security Tokens



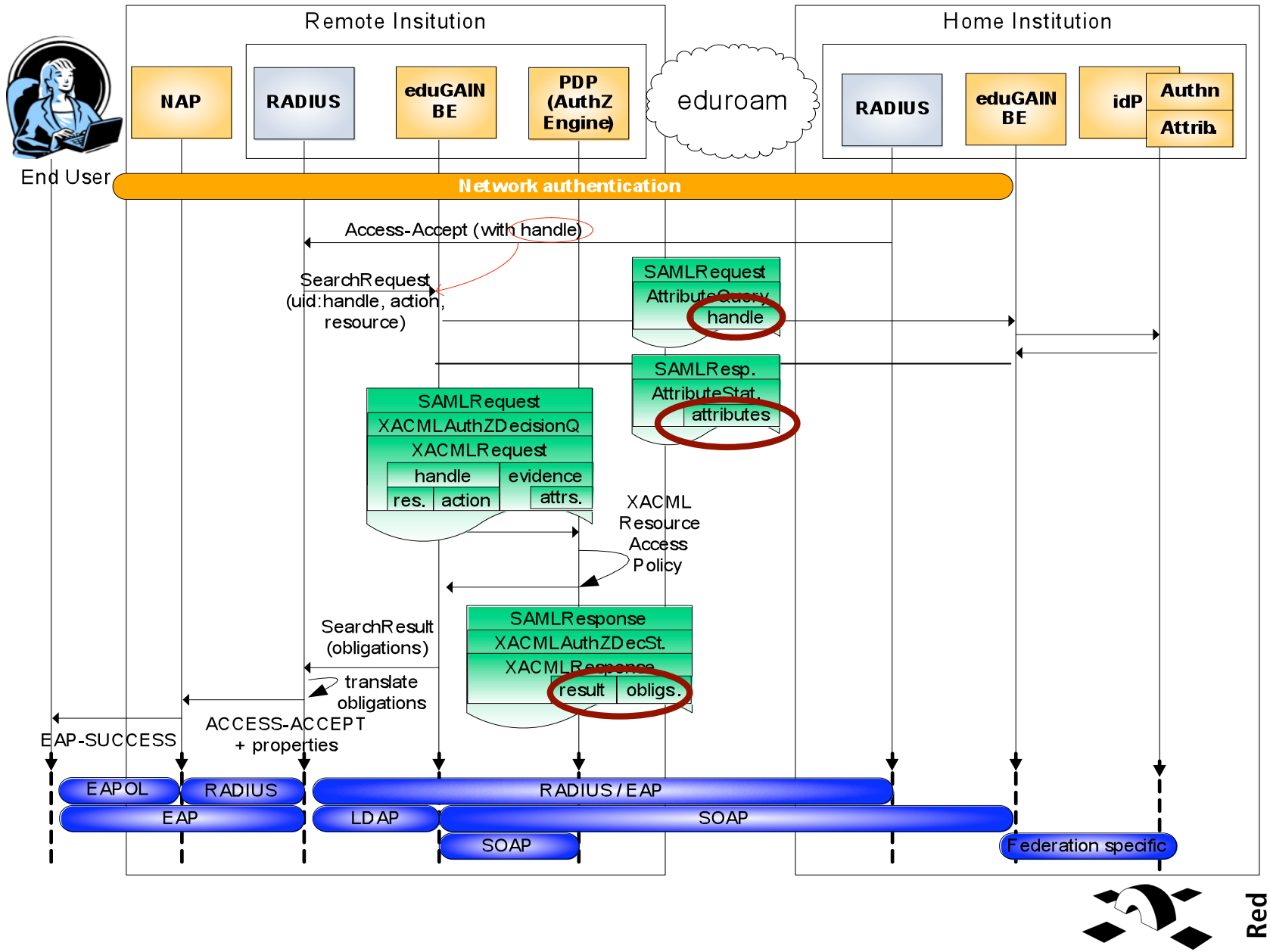
PerfSONAR AA Profiles

- AC
  - Autonomous components
  - Token (X.509) pre-installed in the component
- WE
  - Applications at web portals
  - SAML assertion derived from federated authentication
- UbC
  - Stand-alone client with a GUI
  - X.509 token dynamically built via SASL
  - New mechanisms under development

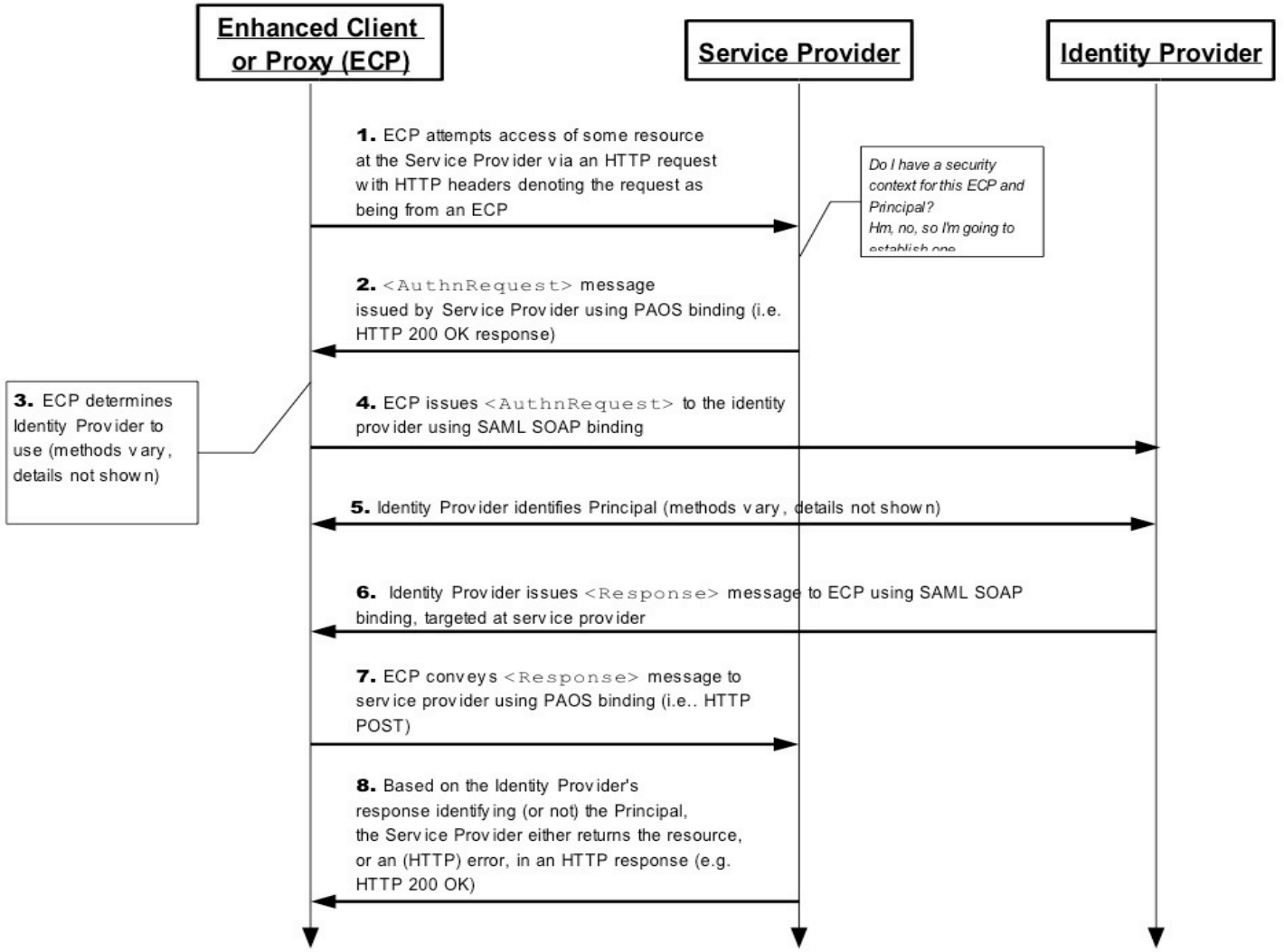
Struggling with UbC

- Deploy and configure a SASL online CA
  - Including a signing certificate
  - Direct access to user credentials
  - Able to provide a session to user attributes
- Deployment has been hampered because of this
  - Practically, a single SASLCA (at GIdP)
- New profile(s) to solve or alleviate this
  - Using SAML tokens
  - With a general STS as the long-term solution
- In the mid-term, make use of already existing identity exchange infrastructures
  - DAMe-based authentication
  - SAML ECP
  - Good-ole HTTP Auth

Applying DAMe



Applying ECP



- Provide a single entry point to digital identity services for the academic community
- Multiprotocol
  - Simplify management
  - Guarantee evolution
- Flexible
  - Compatible with any level of IdM deployment
  - Able to live in parallel with other infrastructures

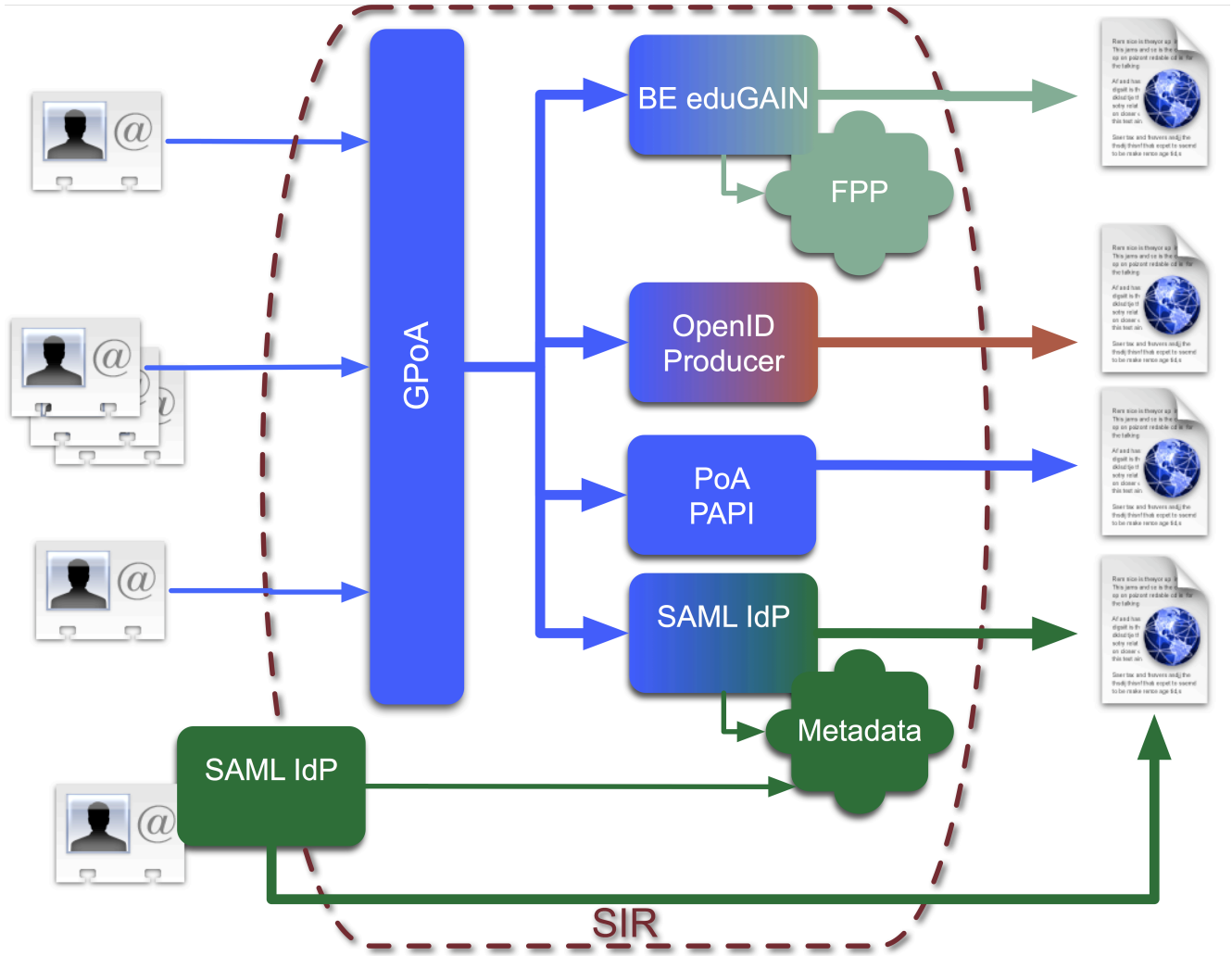
http://www.rediris.es/sir/

The SIR Model

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

One Ring to bring them all and in the darkness bind them
In the Land of Mordor where the Shadows lie.



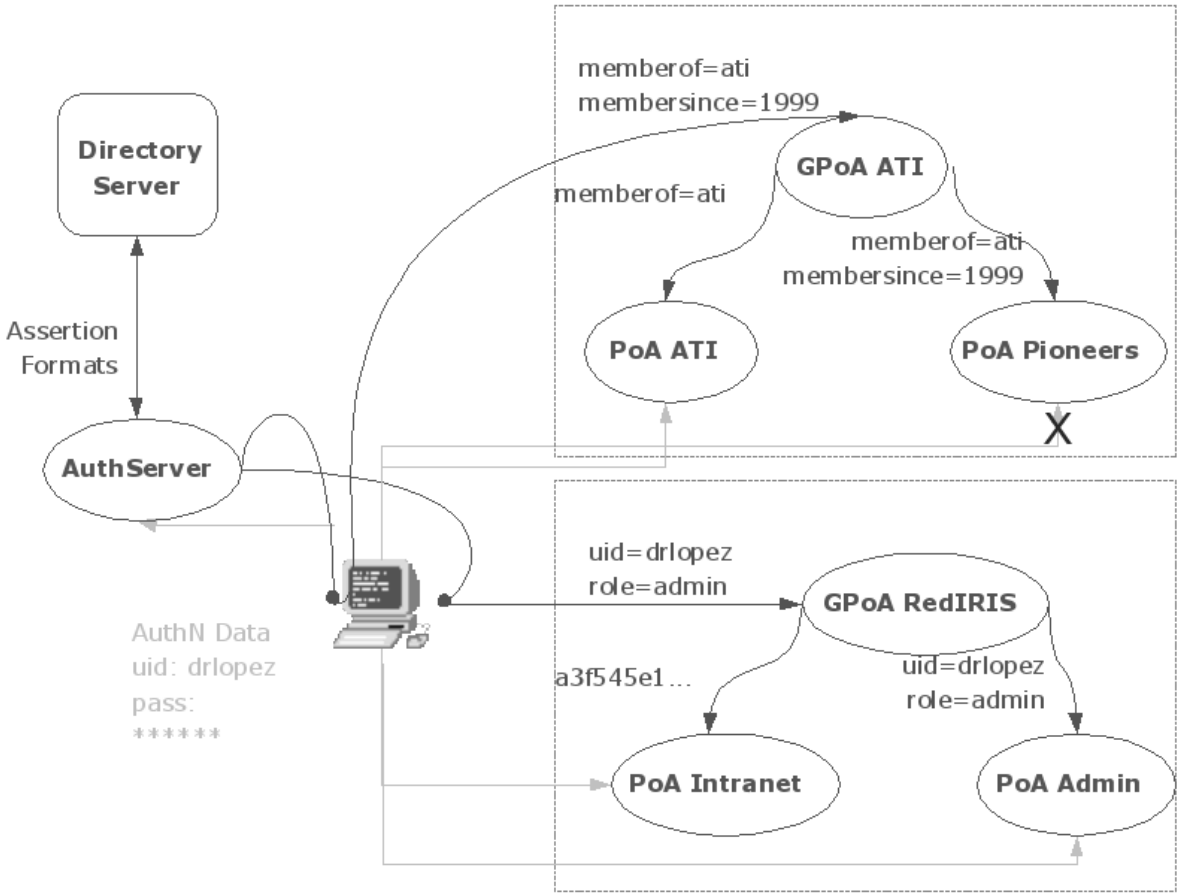
RedIRIS

The Hub Concept

- Simplifies initial adoption
  - Flattening the learning curve
- Provides additional services
  - Building the case for federated ID
- Offers a long-term solution
  - Easy management
  - Seamless evolution
  - Keeping the federation promise
- Adaptable to many kind of institutions
  - From well-staffed, big universities
  - To small-sized research institutes

Why the PAPI Protocol

- Painless trust model
- Lightweight transport
- Easy deployment
- Well-known by our community
- Installed base



IdPs in SIR

- Based on *connectors*
  - Associated to institutional access / SSO system
  - Able to produce assertions in the PAPI v1 protocol
  - PHP, Java (JSP & Filter), Apache mod_perl, ASP, Sun AM, OSSO and some specific ones
  - Community process for developing new ones
- Extensible attribute flow
  - Minimum set of attributes in the iris-* schema
  - Any other can be sent
  - Retrieved by the connector from the environment and/or Id repositories

SPs in SIR

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- PAPI PoAs using the SIR GPoA as authoritative source
  - GPoA metadata available at the SIR site
  - Connectors available in Perl, PHP, Java and ASP.Net
- SAML SPs of external providers
  - Metadata is internally used by SIR adaptation layer
- SAML SPs of participating institutions
  - Metadata integrated with the IdP SAML metadata set
- Any OpenID relying party
  - No metadata (for the moment…)

Red IRIS

The Policy

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- ASAP (The `S´ is for simple)
  - This is a data transport infrastructure
  - Signature of an agreement
  - Explicit liability disclaimer
- IdPs
  - Restricted to institutions in the RedIRIS constituency
  - PAPI trust material (public key)
  - Acknowledgement of the conditions of use
  - Explicit description of the data protection measures
- SPs
  - Acceptance of the metadata
  - Declaration of the endpoints and consumed attributes
  - Acknowledgement of the conditions of use

RedIRIS

Bringing PerfSONAR to SIR

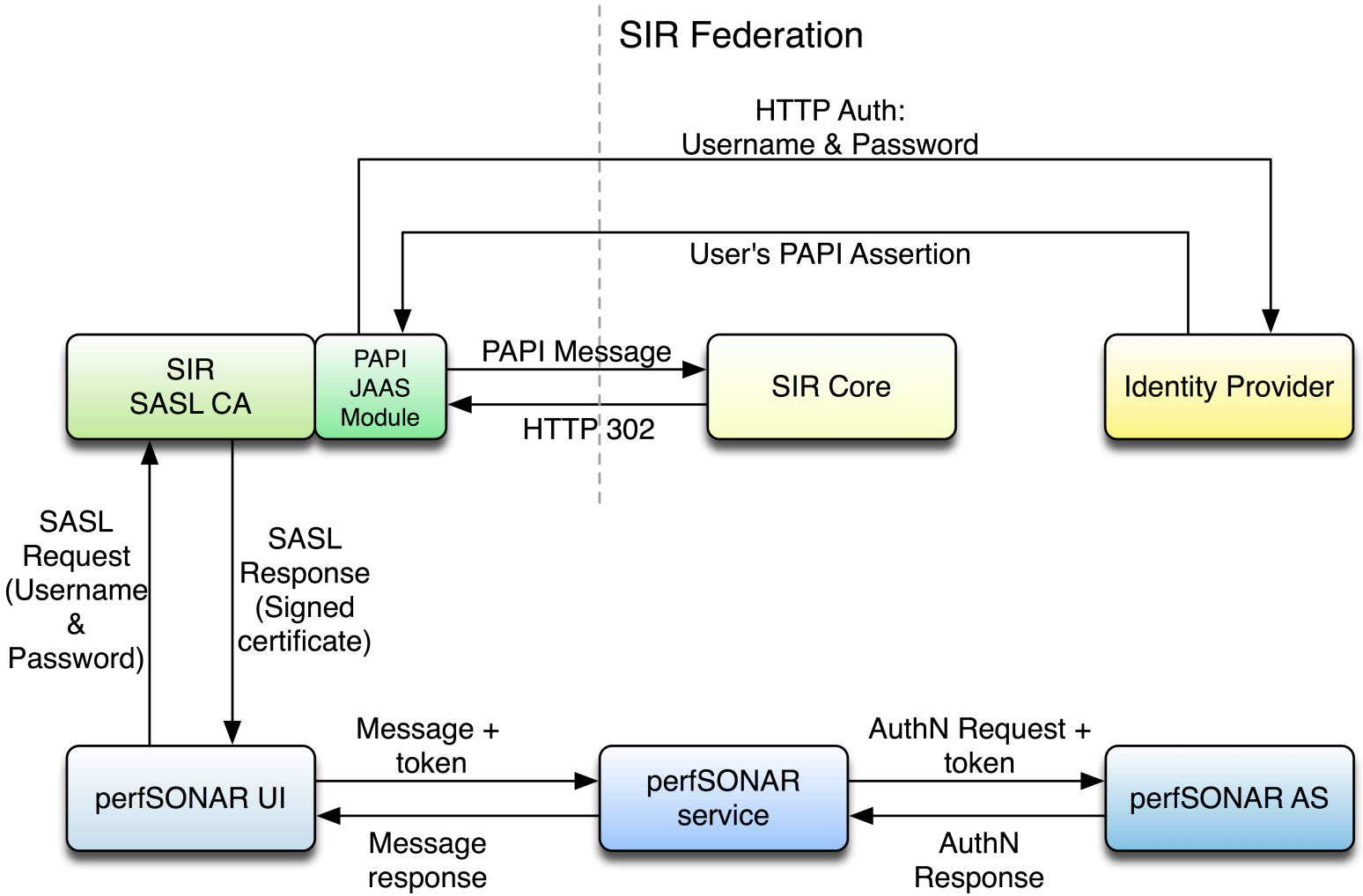
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Already implemented for other WS-based services
- Including support for a SASL CA in the SIR SP set
  - Deploy the SASL CA software
  - Extending the JAAS PAPI connector
- Deploying IdP connectors supporting HTTP Auth
  - Already existing ones
  - Lightweight PHP application
- Taking advantage of SIR location services
  - Local-username@Local-domain
  - Up to each domain whether usual passwords can be applied

Red IRIS

SIR-enabled PerfSONAR



As Conclusion

- PerfSONAR AA mechanisms still evolving
  - Identity federation integration not as easy as planned
  - Clear evolution path ahead
- Initial deployment for singular projects supported by the GÉANT infrastructure (GIdP)
- A wider deployment at the NREN level requires adapting federations to current AA profiles
- The hub approach simplifies adaptation
  - In depth, minimizing software changes
  - In breadth, allowing adoption by any kind of institution