SIR and Identity Hubs

Diego R. Lopez, RedIRIS
• 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/](http://www.rediris.es/sir/)

TF-EMC2. Utrecht, December 2008
The Basic SIR Model

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

- **Bases 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
SIR Services

- Interconnection with SAML infrastructures
- Access to PAPI-based services
- eduGAIN BE
- OpenID producer
SAML Services

- Taking full advantage of simpleSAMLphp flexibility
- Virtual* SAML IdP(s) per SIR IdP
  - SAML 1.1 (Shib 1.3) by default
  - Additional SAML 2 by request
- Individual ARP and mappings
  - GPoA applies its own initial filters
  - SAML IdPs apply theirs per SPs
- User consent can be defined at either the inner or the outer level

* external, managed, outer, outsourced,…
The Extended SIR Model

- SAML-based IdPs
- Region- or community-based federations
- SIR acts as a metadata aggregator
SIR: OpenID

- Specific producer rules per institution
- Additional controls
  - Match URL with attribute values
  - Specify acceptable RPs
  - Explicit user consent for extensions related to personal data
- Simplified identifiers in whatever Spanish language
  - yo.rediris.es
  - jo.rediris.es
  - eu.rediris.es
  - ni.rediris.es
  - Explicit translation for limited consumers
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
  - Keeping the federation promise
  - Specially for small-sized institutions