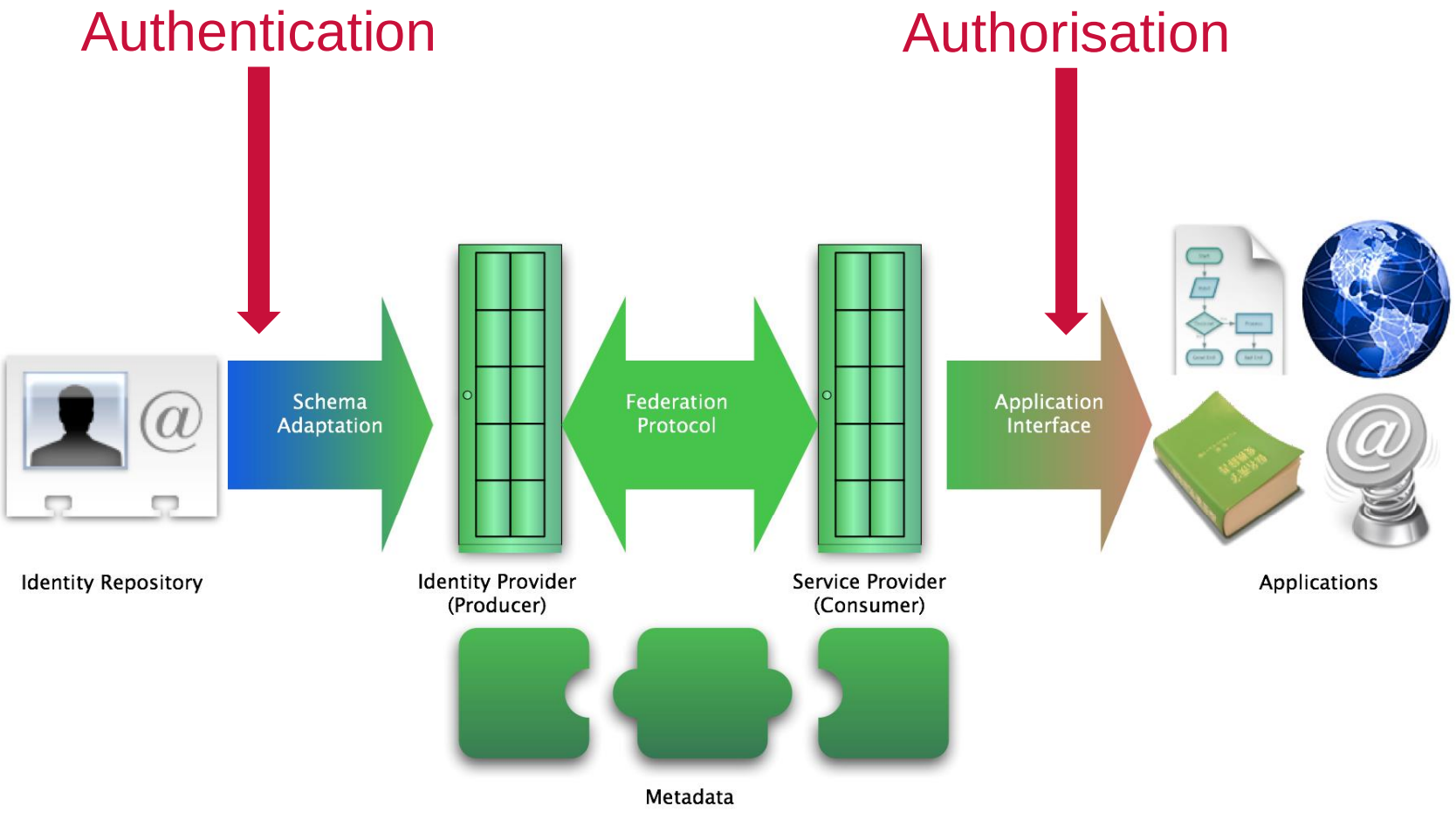
# Report on AAIs
## Convergence and Expansion of the Identity Spheres

e-IRG Workshop. Brussels, October 2010

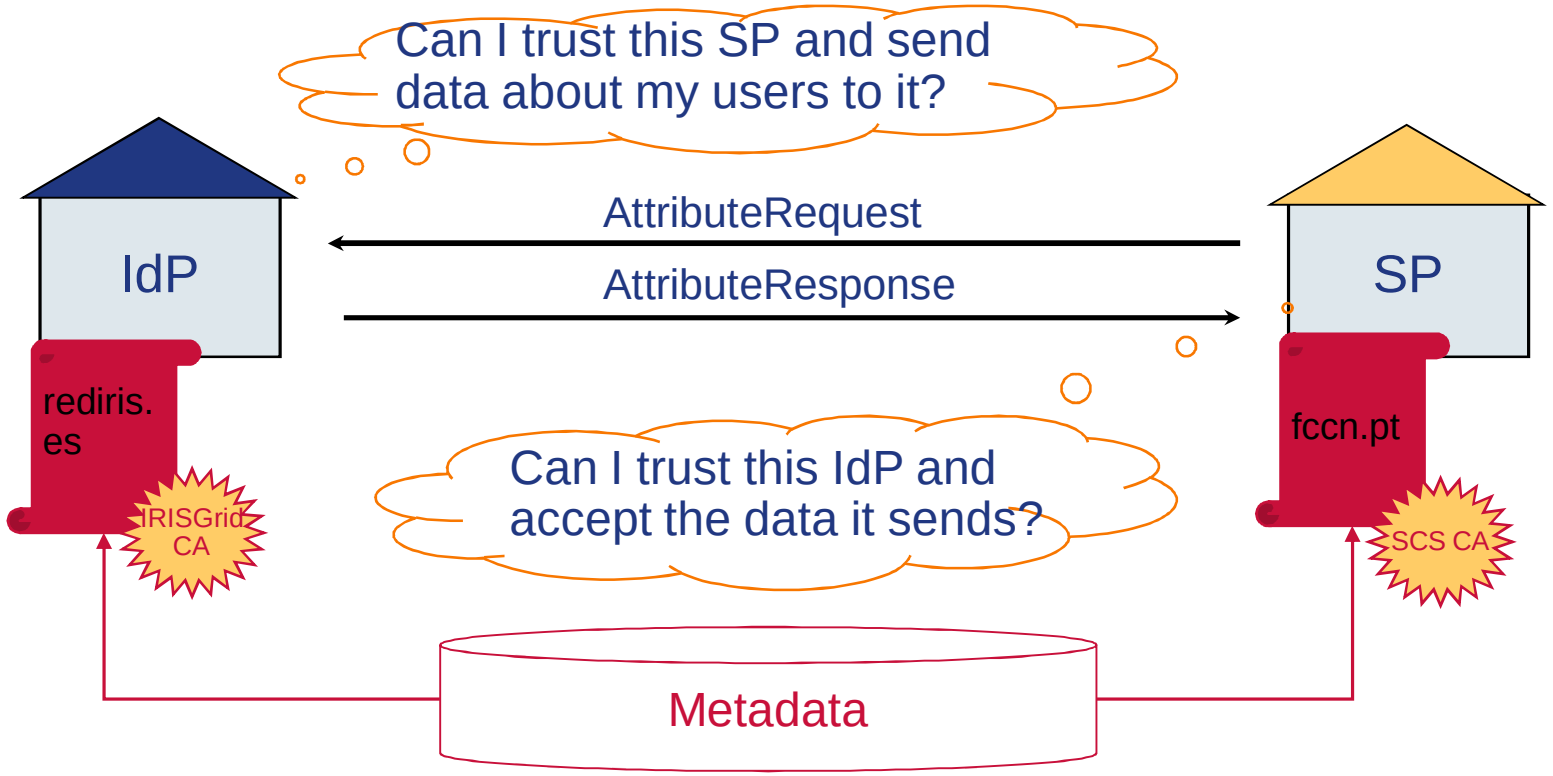
# The Identity Data Flow



# The Components

- An infrastructure supporting the trust fabric
  - Typically based on public keys
- A set of protocols for data exchange
  - SAML is the lingua franca
- A common schema for syntax and semantics
  - eduPerson + SCHAC
- An agreement among participants
  - Bi- or multi-lateral
  - Through a unilateral declaration (affiliation)

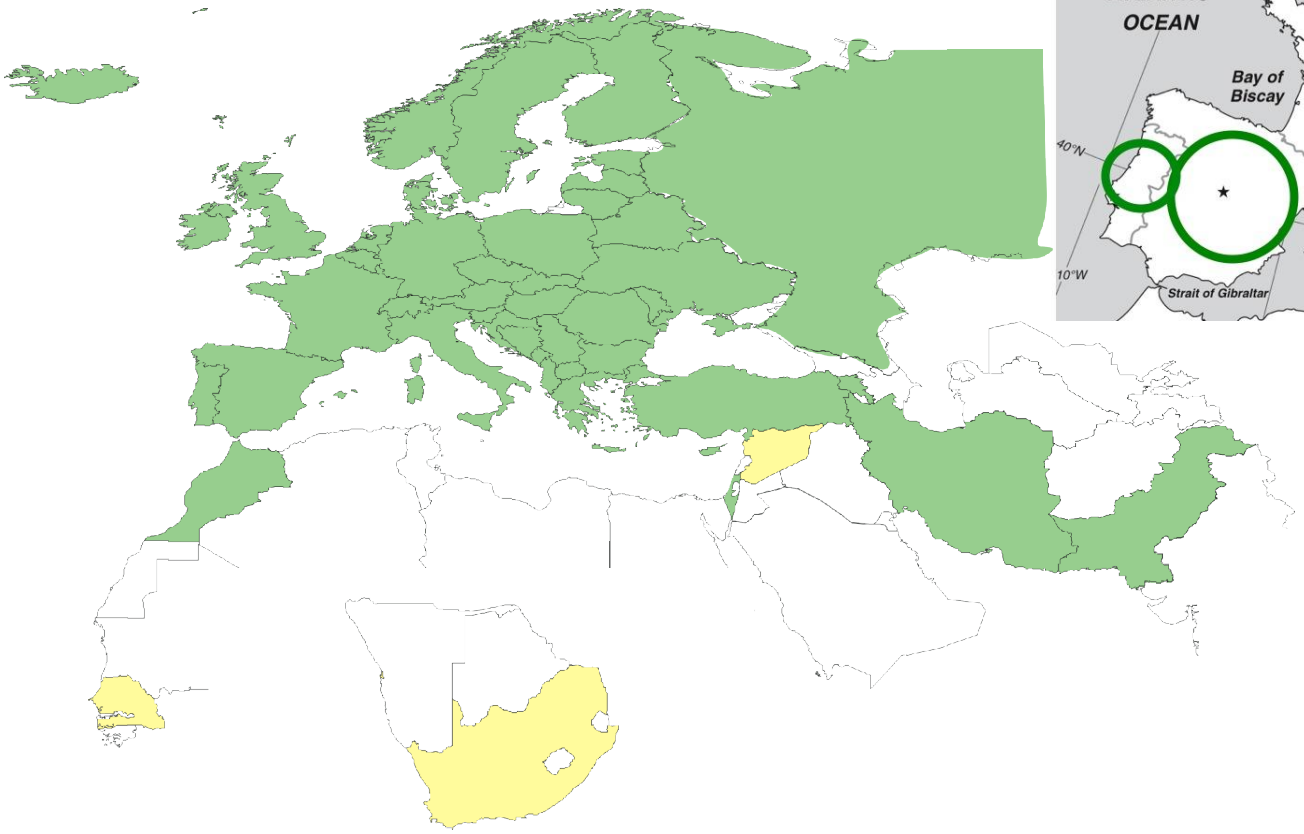
# The Trust Issue

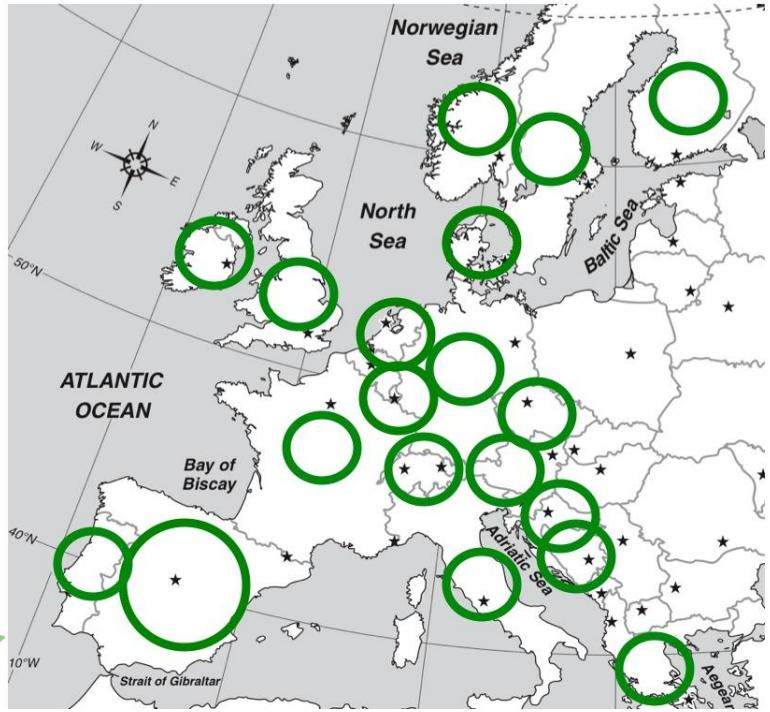



- Trust is established through different metadata

# All Around the Map

EUGridPMA






eduGAIN

# Actual Convergence

- Essentially, NREN-operated identity federations and Grid identity infrastructures are interoperable
- Convergence as use cases appear
  - SAML profiles
  - MICS and SLCS
  - edGAIN and metadata coordination services
  - VASH and attribute provision
  - TCS e-Science
- Security Token Service in EMI and GN3
- Toolbox model
  - Compatible rather than unique

# Expansion Axes

- Going beyond current silos
  - Web SSO and Grid applications are not enough
- *User-centric* protocols and services
  - Learning to live in the “wider Internet”
- Governmental identity infrastructures
  - Taking advantage of higher levels of assurance
- Seamless integration
  - Multiple identity sources
- Building a reputation
  - The  identity *prosumer* model

# Adding Application Domains

- Exploring protocols
- And trying to solve other issues
  - Trust transitivity
  - Attribute and rights mapping
  - Policy matching
- Work already started
  - DAMe
  - FedSSH
  - Moonshot
  - GEMBus

# Becoming More User-centric

- Better usability
  - Adapted to customary Web access flows
- Additional use cases
  - Mostly,  RESTful services
- Technology already implemented
  - SIROPE, SimpleSAMLPHP, PAPOID, IdPProxy, Logins4Life,…
- Policy challenges
  - Big guys play here
  - Keep the hard-won achievements on privacy and security

# Supporting Higher LoAs

- Governmental identity infrastructures already available in many countries
  - Smart-card and other identification technologies
  - Legal support where deployed
- Interconnection already demonstrated: STORK
  - Among them and with academic federations
- Enhance vetting processes
- Additional assurance to subject identifiers
- Authoritative source of specific attributes
- Consume identity data from the academic side

# Integrating Identity Sources

- Acknowledge the fact that no single source of identity data exists
  - The federation promise must be kept
  - And there is no upper limit in the general case
- Experiments already done
  - Different aggregation models
- Trust issues still open
  - Current LoA models only deal with identity vetting and identification mechanisms
- And policy matters become even more crucial

# Reputation: The Next Frontier

- The social part of identity
  - Users as (dynamic) producers and consumers of identity
  - Support for the next generation of e-infrastructures, especially in aspects related to data
- First experimental models
  - P2P networks
  - Domain assessments
- Protocol, trust and policy challenges extended to network-wide scale
  - Not intended to replace current AAIs, but to take advantage of them

# The Domestication Concept

- Re-factoring applications to use the emergent identity services infrastructure
- Externalize authentication
- Externalize group management
- Needs a fine grain set of authorization tools down the road
- Domesticated applications can receive attributes via a multitude of standards

# The REFEDs Group

- The purpose of REFEDs is to serve the needs of the worldwide community of R&E Identity Federations
  - To align policies to facilitate inter-federation
  - To create community best-practices and promote them within our community and beyond
  - To become the interface of the R&E community when talking to other communities
- Under the auspices of TERENA
  - Sponsored by AAF, CESNET, GARR, Internet2, JISC, NORDUNET, RedIRIS and SURFnet
  - Participants from identity federations worldwide (NRENs and Grids)

http://refeds.terena.org/

# As a Conclusion

- Accelerate the process of the continued convergence of different identity infrastructures, and contribute to their improvement at the national and community levels
- Require that future pan-European e-infrastructures and ESFRI projects define their access control policies and mechanisms from the beginning, and promote the application them of standards methods for identity data integration with their services

- Support REFEDs as a global, open group for collaboration in identity technologies, within the research networking communities and even beyond