Federated IdM Workshop
CERN, 10 June 2011

David Kelsey
STFC-RAL
david dot kelsey at stfc dot ac dot uk
(personal views – not on behalf of any Grid)

Key Issues for federated IdM

- Many good technologies to choose from!
  - Must of course satisfy technical and security requirements
  - E.g. “Delegation”, LoA, ...
- Impossible that one size will fit all
- Avoid special one-off solutions - Use common framework
- Interoperability is important
  - must use standards
  - Single electronic identity usable everywhere
- Keep AuthN and AuthZ separate
- Scaling and Ease of Use
  - E.g. Do identity vetting just once
- Very important that we work with REFEDS, NRENs, academic federations
  - Scientific collaborations are excellent use case for inter-federation

Issues (2)

- Single sign-on very attractive – what about single sign-off?
- Levels of Assurance are now more important
  - To meet range of security requirements
  - User may wish to use different credentials for different purposes
- Attribute aggregation/linking important
  - Multiple sources of authority
- Privacy, Data Protection, Attribute release, User consent
- Do we need more formal auditing?
- The technology is the easy bit!
- MUST establish and maintain TRUST (independent of technology)
  - Policy standards very important

Input for Roadmap – federated IdM

- Levels of Assurance (technology **and** policy issues)
- *Developers* :
  - Address Ease of Use (hide complexity)
  - Credential translation (e.g. EMI STS)
  - Interoperability
  - Attribute aggregation
- *Policy bodies* (e.g. IGTF)
  - Building TRUST is essential
  - IGTF should cover wider range of services
    - e.g. LoA, STS, Attribute Authority operations
  - Scaling: involve others (NGIs?) in accreditation/audit
  - Aim should be to define interoperable and scalable TRUST