Lessons from SDSS/UK federations

Ian A. Young

SDSS, Edina, University of Edinburgh
ian@iay.org.uk

UK Federations Timeline

- "Toy" federation: Q3 2004
  - zero to a handful of entities
- SDSS "development" federation: Sep 2004
  - a handful to a hundred
- Formal "UK federation": Nov 2006
  - a hundred to...

regulation

is

restriction

Regulation at Scale

- Small communities are less diverse than larger ones
- Small communities can be tightly regulated
- Attempts at tight regulation of large communities will restrict membership
  - Who does that serve?
- Don’t forget you need to talk to the rest of the world
- Foster smaller self-regulating sub-communities
- Separate concerns: technical and behavioural trust

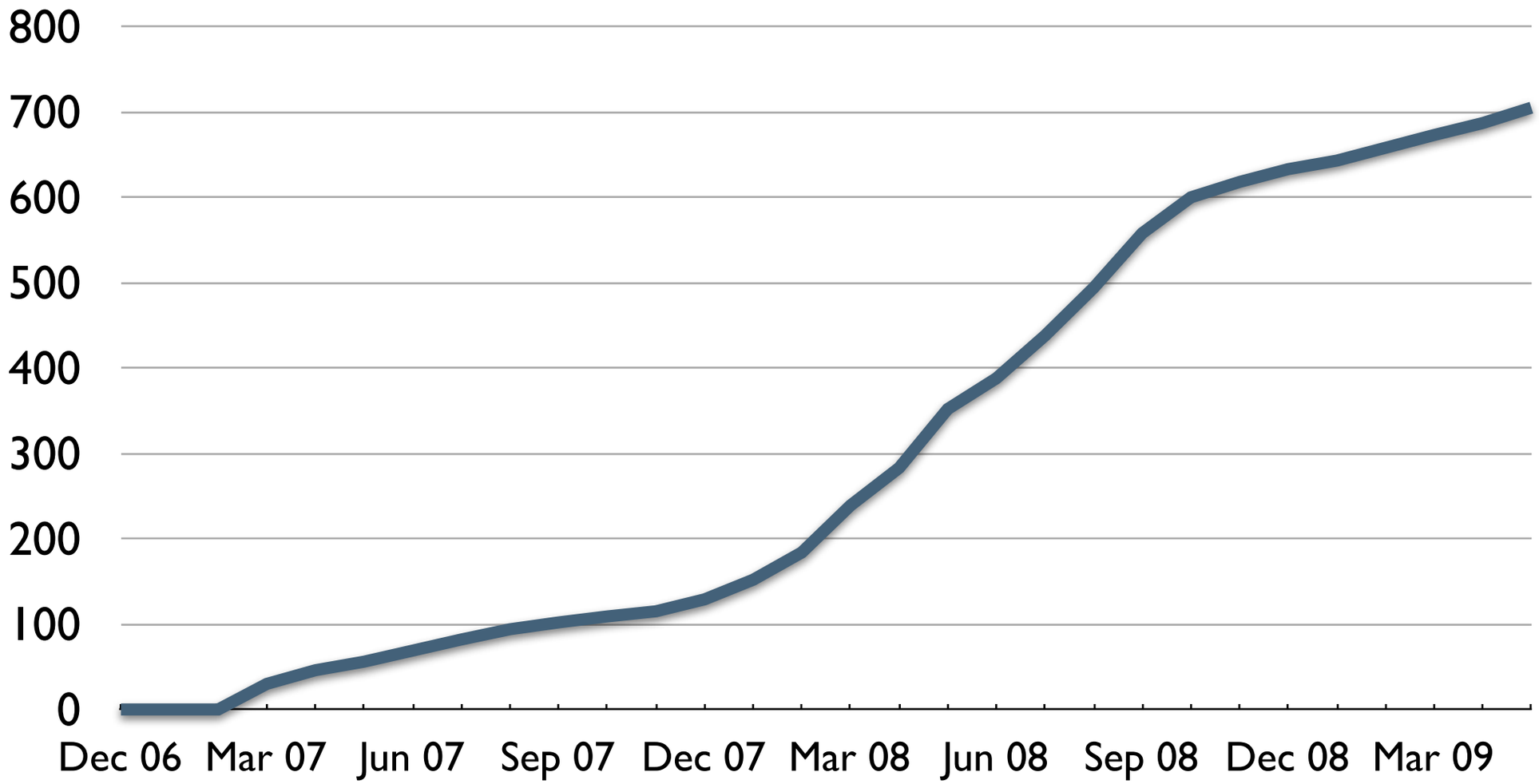
SDSS Federation Policy V1.0

- All members of the federation must:
  - Observe best practice in the handling and use of your digital certificates and private keys
- All identity providers (origins) must:
  - Make reasonable attempts to ensure that only members of your institution are provided with credentials permitting authentication to your handle server, and that the assertions made to service providers by your attribute authority are correct.
- All service providers (targets) must:
  - Agree not to aggregate, or disclose to other parties, attributes supplied by identity providers.

UK: A Light Touch

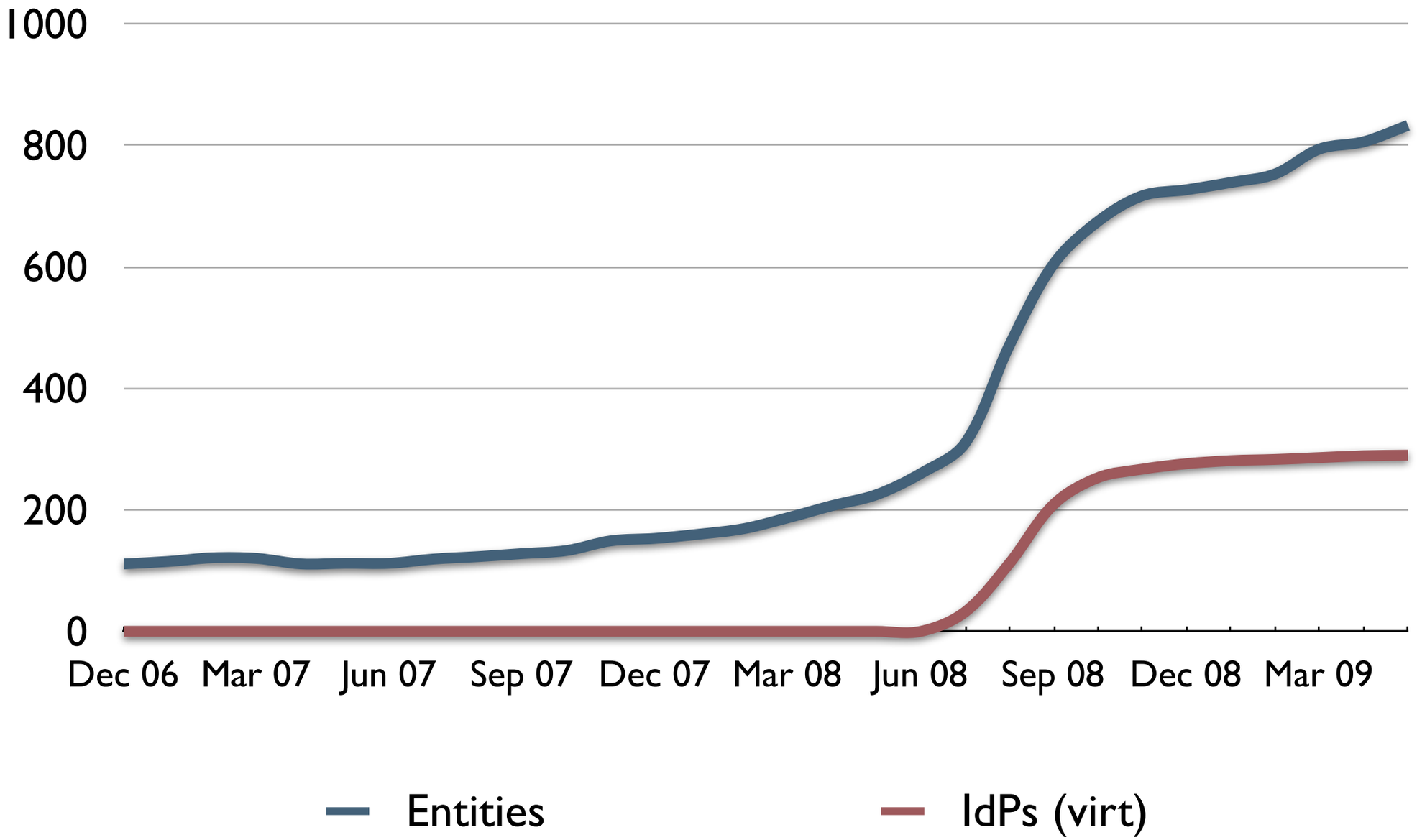
- Lightweight membership agreement
- Broad eligibility criteria
- Never say “mandatory”, always “recommend”
- Non goals:
  - 100% interoperability
  - stupidity eradication

UK federation membership



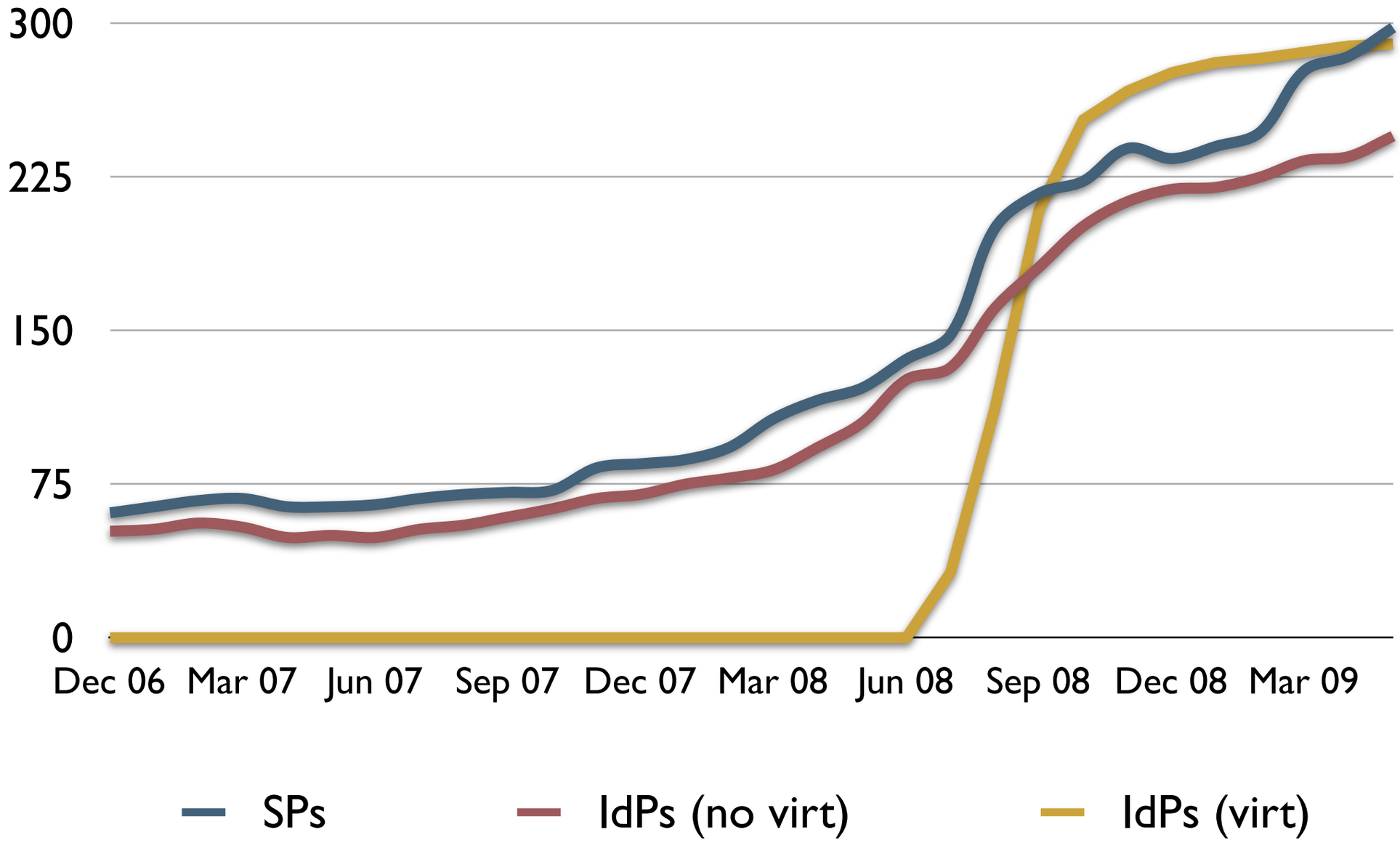
Data: 27 Apr 2009

UK federation entities



Data: 27 Apr 2009

UK federation entities by type

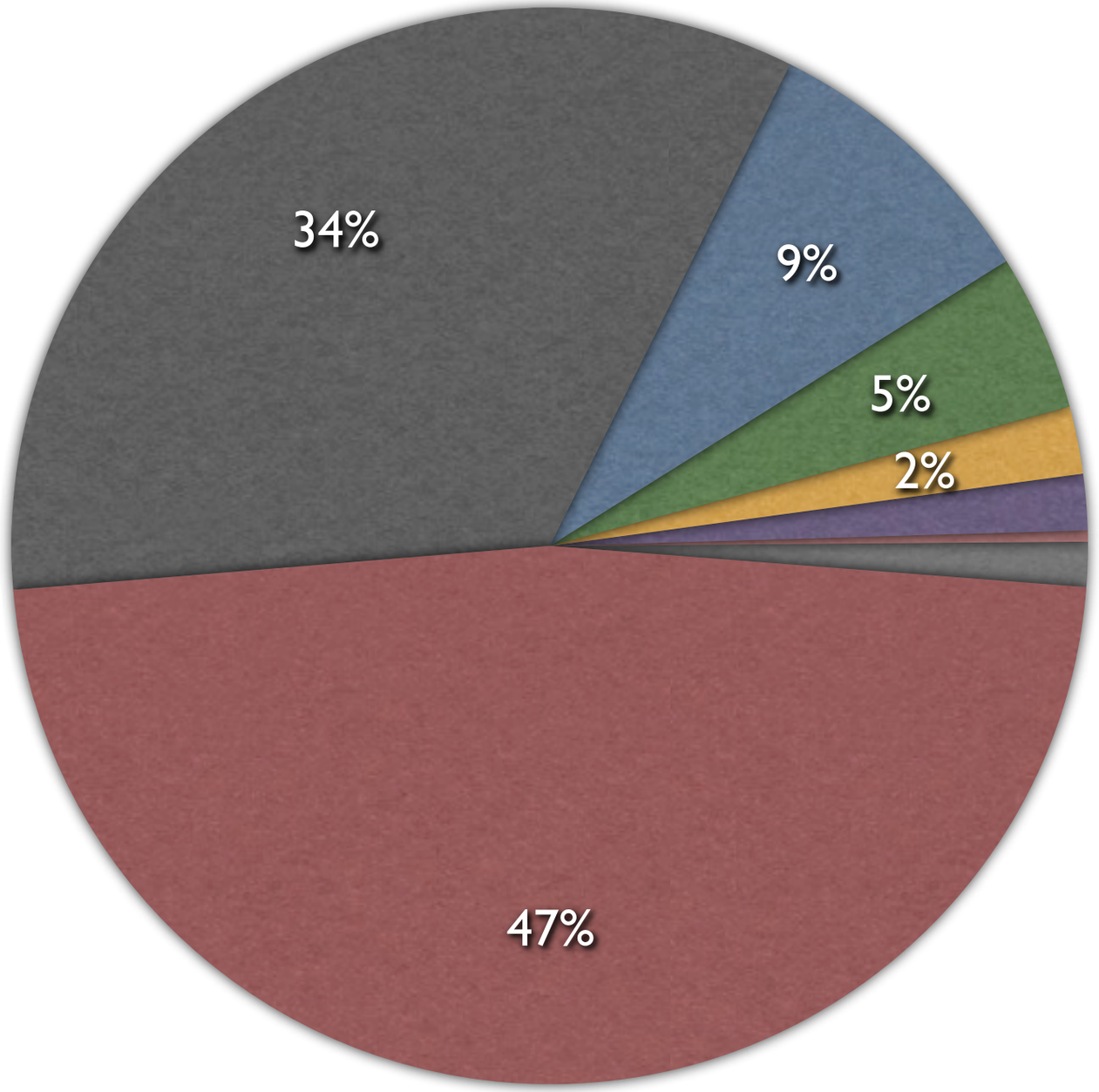


Data: 23 Apr 2009

Vital Statistics

- Members: 705
- Entities: 833
  - SPs: 299
  - IdPs: 536
    - Virtual: 290
    - non-Virtual: 246
    - Scopes: 6282

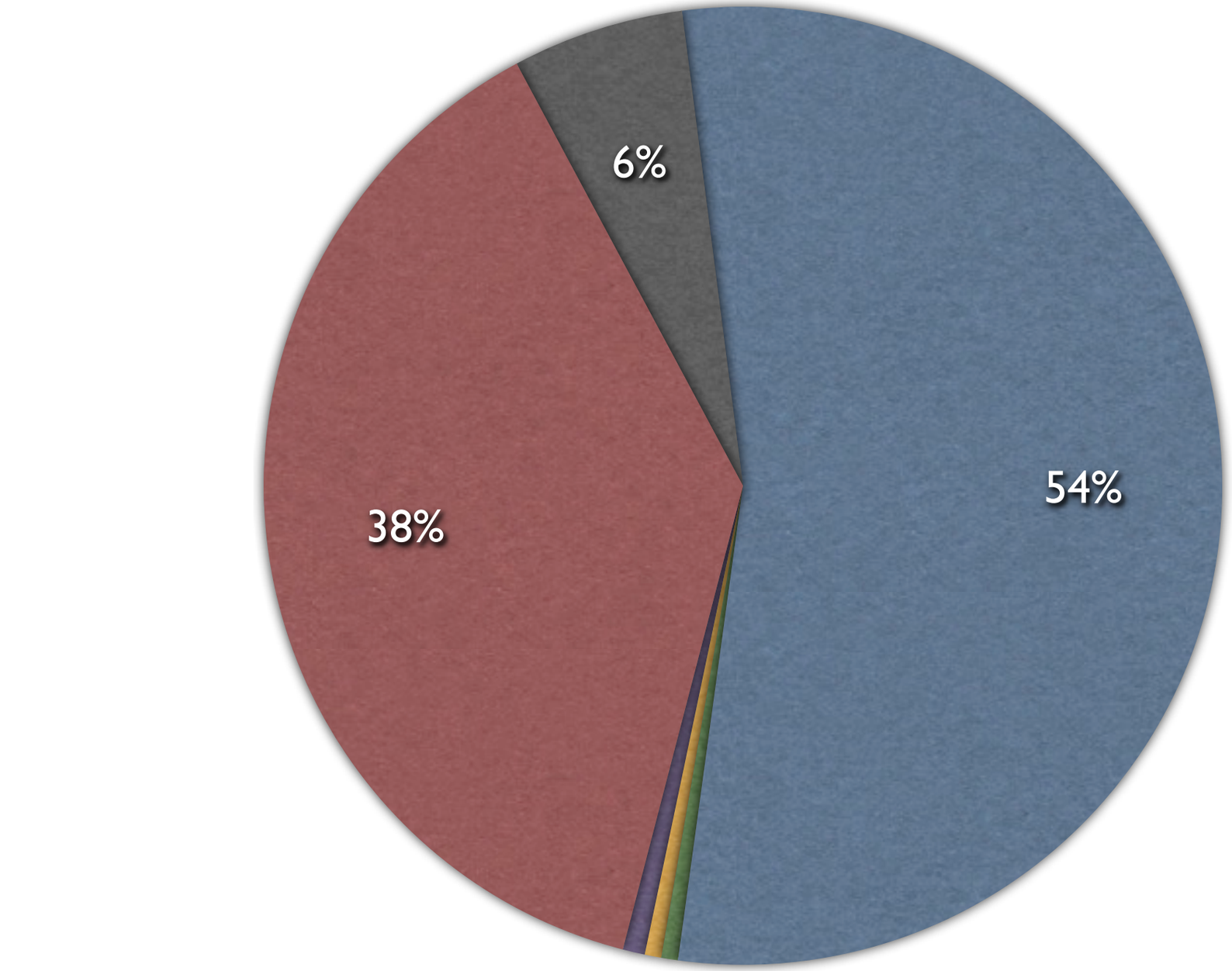
Software in use (SPs)



Data: 23 Apr 2009

- Shib 1.3
- Shib 2.x
- OpenAthens SP
- Atypon
- Guanxi
- EZProxy
- simpleSAMLphp
- Other

Software in use (IdPs by entity)



Data: 23 Apr 2009

Shib 1.3
Shib 2.x
OpenAthens
simpleSAMLphp
Guanxi
Other

invention

hinders

integration

invention

leads to

isolation

Role of Invention

- Easy, and fun, to invent things!
- Invention is easy, adoption is hard
- Doubly so outside your community
- Steal from elsewhere when possible
- Avoid speculative invention
- Plan to be agile when – if – problems arise

UK: Attributes

- There is no "ukEduPerson" profile
- Hierarchy of recommendations:
  - "Core" 4 shamelessly stolen from eduPerson
  - Plus community-based profiles
  - Plus list of supplementary sources
  - Plus recognition that partners always have the last word; it's a negotiation

pioneers

are not

prophets

But he said…

- Following other federations' lead is good…
- … but don't assume they are always right
- Look at multiple examples, select what will work for you
- Remember that other people made decisions in a context, perhaps long ago
- This technology is still changing

UK: Trust Fabric

- Initially followed InCommon and SWITCH
  - PKIX-based, mix of own CA and commercial authorities
- Started embedding keys, experimenting with self-signed, to solve particular issues
- InCommon now embedding
- Long term trend towards self-signed