Federated Access Management Futures

Ian A. Young

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

Prediction is very difficult,
especially about the future.

– Niels Bohr

What to expect

- Prepared material is just a guide, this is not a lecture
- *Please* stop me to extend a section, go into more depth or just repeat something
- General Q&A, discussion at end (if time)
- If you don't disagree with at least one thing I say, you are probably asleep…

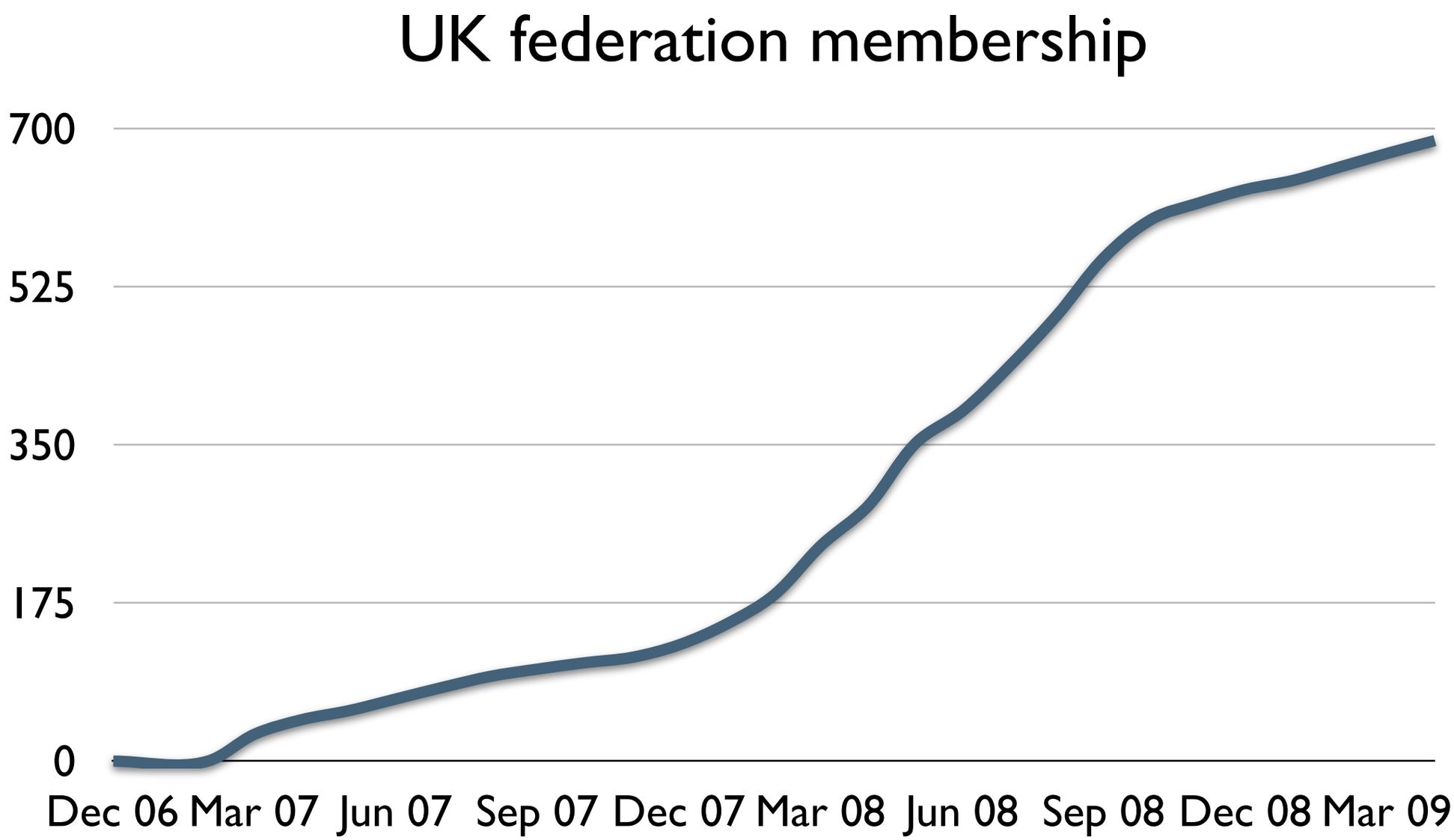
Topics

- Adoption
- Software and Protocols
- Discovery
- LoA / IAP
- Authentication
- Interfederation
- Others?

Adoption

Past performance is
not a guarantee
of future returns…

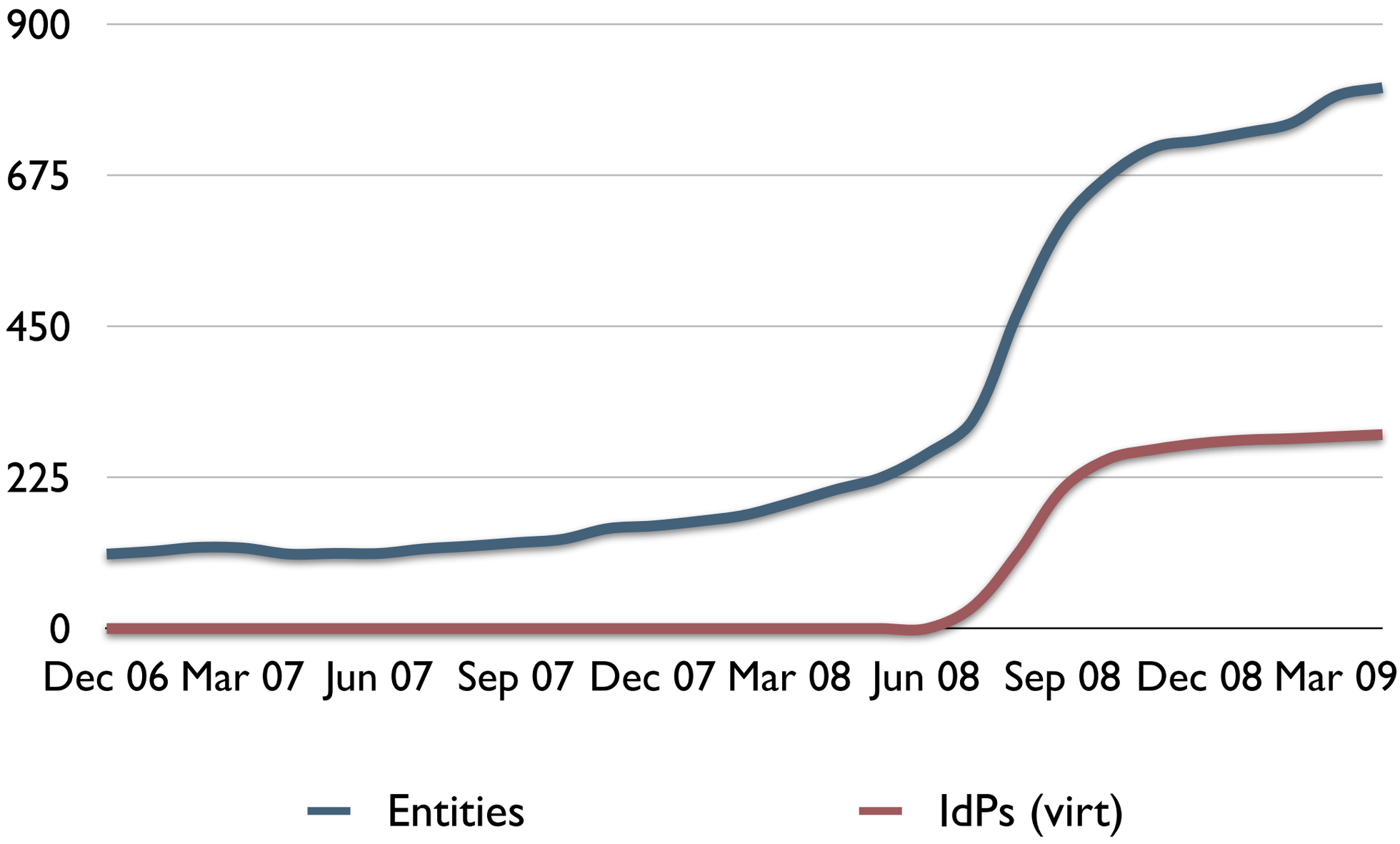
– A. Fund Manager


UK federation membership
700
525
350
175
0
Dec 06
Mar 07
Jun 07
Sep 07
Dec 07
Mar 08
Jun 08
Sep 08
Dec 08
Mar 09

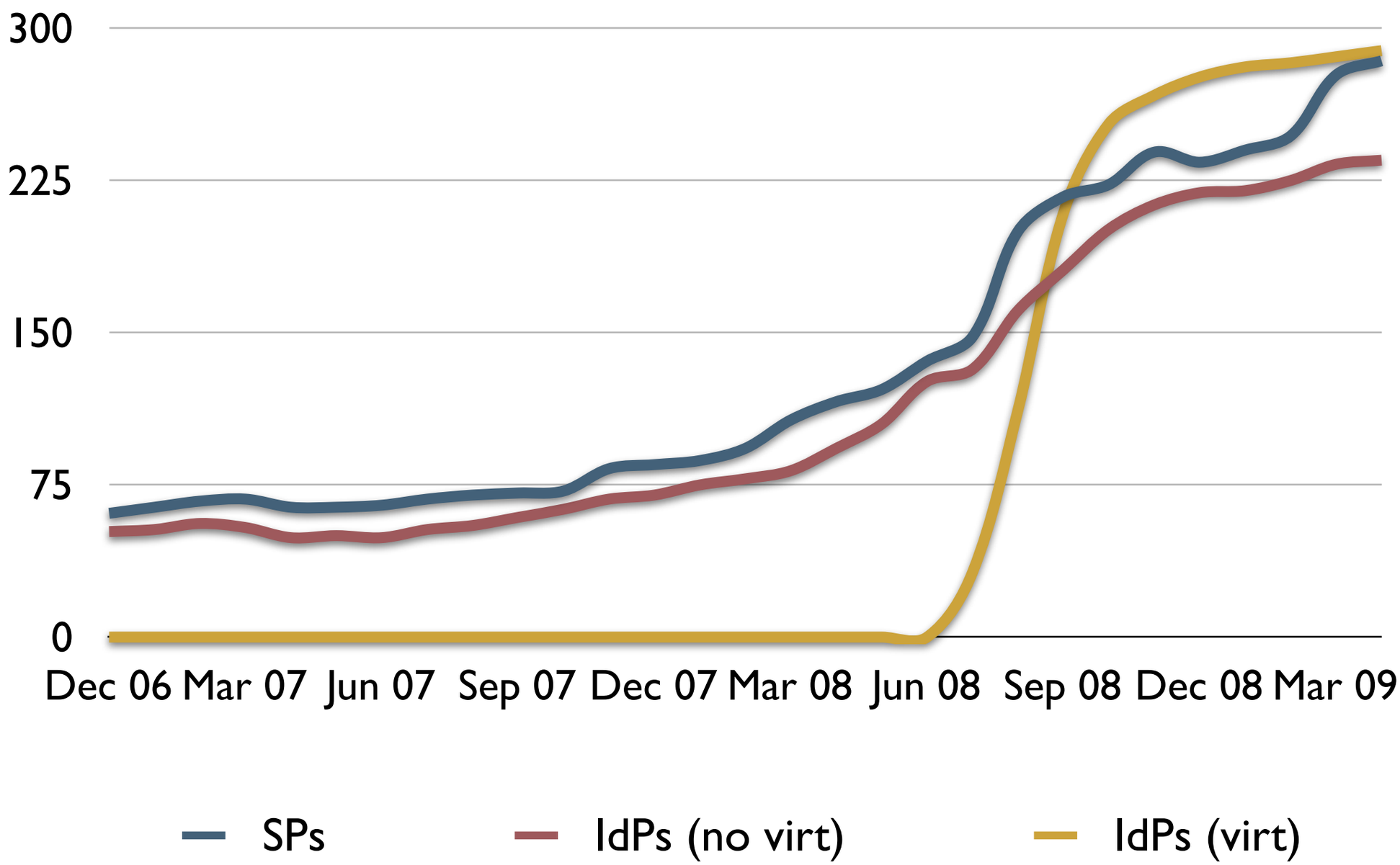
Membership

- Largest in the world, and still growing
- The broader the membership, the fewer assumptions you can make about a member
- Ultimately, you're dealing with *everyone* and can make *no* assumptions
- …just like the Internet in general

UK federation entities



UK federation entities by type

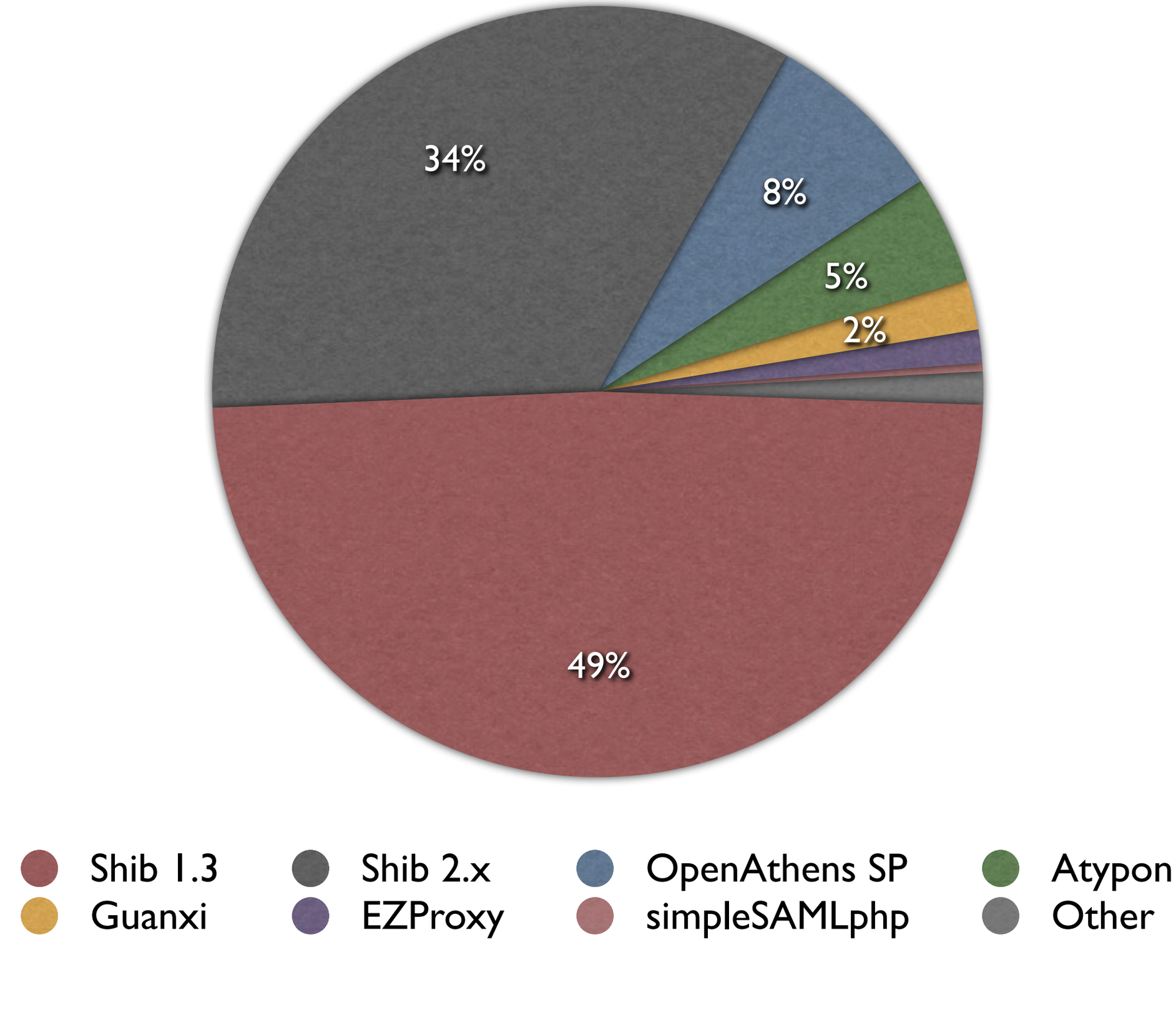


Adoption

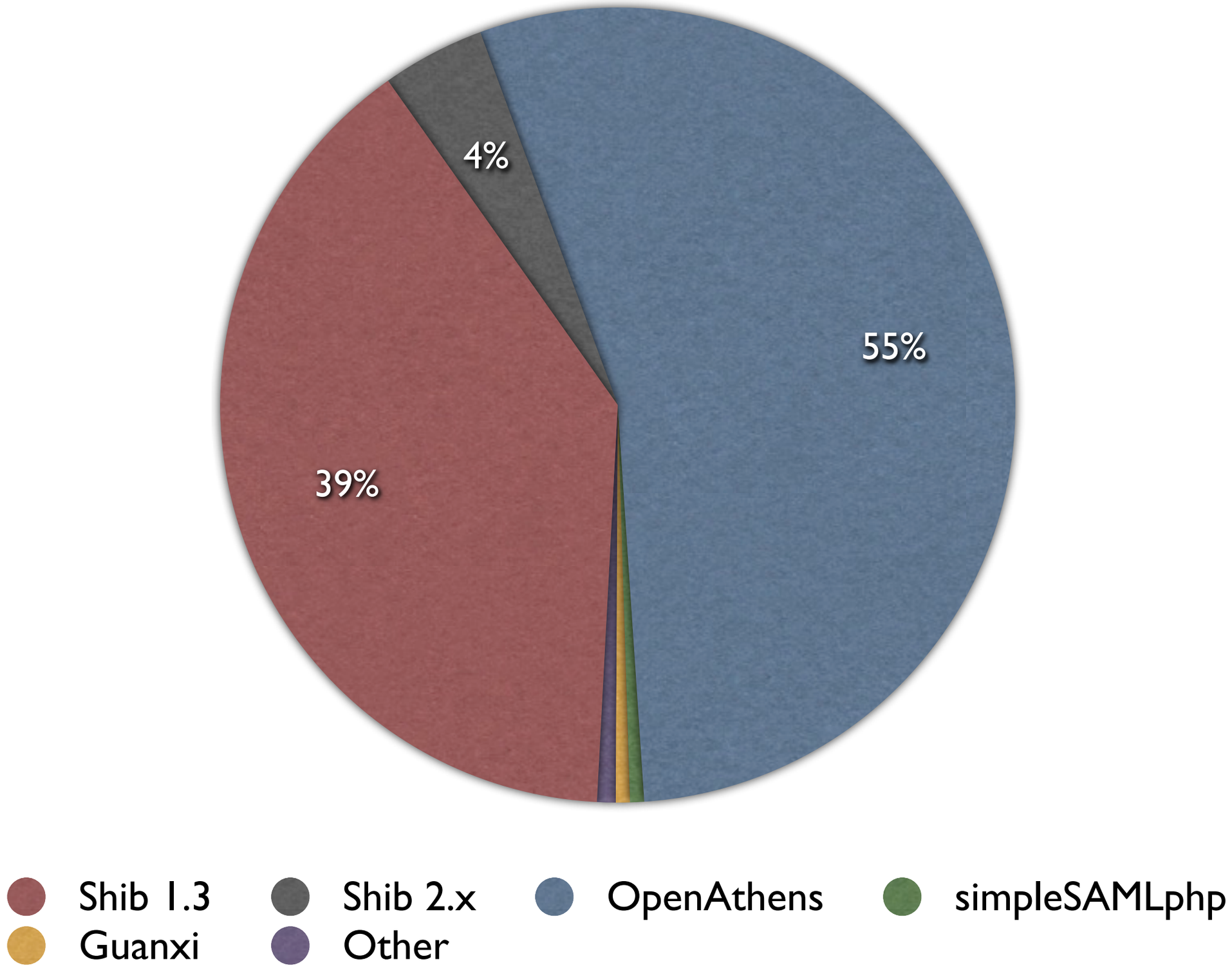
- The UK is unusual in many ways…
  - large outsourcing component
  - very broad membership
  - these are related
- …but probably not unusual for long
- Still growing, no end in sight!

Software and Protocols

Software in use (SPs)



Software in use (IdPs by entity)



Software and Protocols

- Lots of diversity in software
- Move from single-protocol software to multiple-protocol *platforms* is good news
- SAML 2 not yet widely available, but coming
- This will enable yet more diversity
- …but take care with software choice, not everything is equally suitable at this scale

Discovery

Centralised Discovery

- Federations deploy centralised discovery services (e.g., WAYFs) for use *as a last resort*
- Trivial for SPs to use but user experience is not good, and getting worse
- Choice of 526 IdPs (and counting) can never be done well (although we'll try)

Client Centric Discovery

- For example, Microsoft Cardspace
- This is probably the best long term approach for users
- But it still doesn't exist widely enough to let anyone off the hook

What can SPs do?

- Don’t rely on others to solve this problem, own it on behalf of your customers.
- Perform your own discovery locally:
  - you know who your customers are
  - you can do this job better than any third party
- Provide “session initiator” locations to help out IdPs (sometimes called “WAYFless URLs”).

What can IdPs do?

- Don’t rely on others to solve this problem, own it on behalf of your users.
- Ask SPs for session initiator (“WAYFless URL”) details for their services.
- Give your users resource links that use these to avoid discovery entirely.

LoA / IAP

Identity Assurance Profiles

- IAP: more general term than LoA (levels of assurance) without implicit hierarchy.
- All SPs consider their content valuable…
- …but expect assurance cost to be borne by IdPs.
- Best agreed and specified within a specific community of interest.
- Impossible to impose anything significant on a broad community.

UK federation IAPs

- Currently, only “section 6” specified
  - only one page
  - very lightweight requirements
  - not tightly specified
  - required by several services
  - (self) asserted by almost all IdPs (91.8%)

InCommon IAPs

- Specific community need for IAPs targeted at NIST level 1 and 2, e.g., for NIH.
- Bronze and Silver profiles are defined (25pp).
- Very specific *auditable* requirements.
- Hard to specify, hard to implement, but deliver major value where they are needed.
- Many sites "working towards" these.

Authentication

The future is here.
It's just not widely
distributed yet.

– William Gibson


signature card
openPGP
GNU - PRIVACY - GUARD -
OPEN PGP
01010001 00000A7C


UKf 86 74 E2 C8 58 1C
Ian Young
UKf Signer 1.8
Production Mode


acs
LED2
61079
eToken


SELECT
FUNCTION
RBS
The Royal Bank of Scotland
ON/OFF
Identify
Respond
Sign
MENU
C
CL
OK
1
2
3
4
5
6
7
8
9
0


PayPal
Identity
Protection

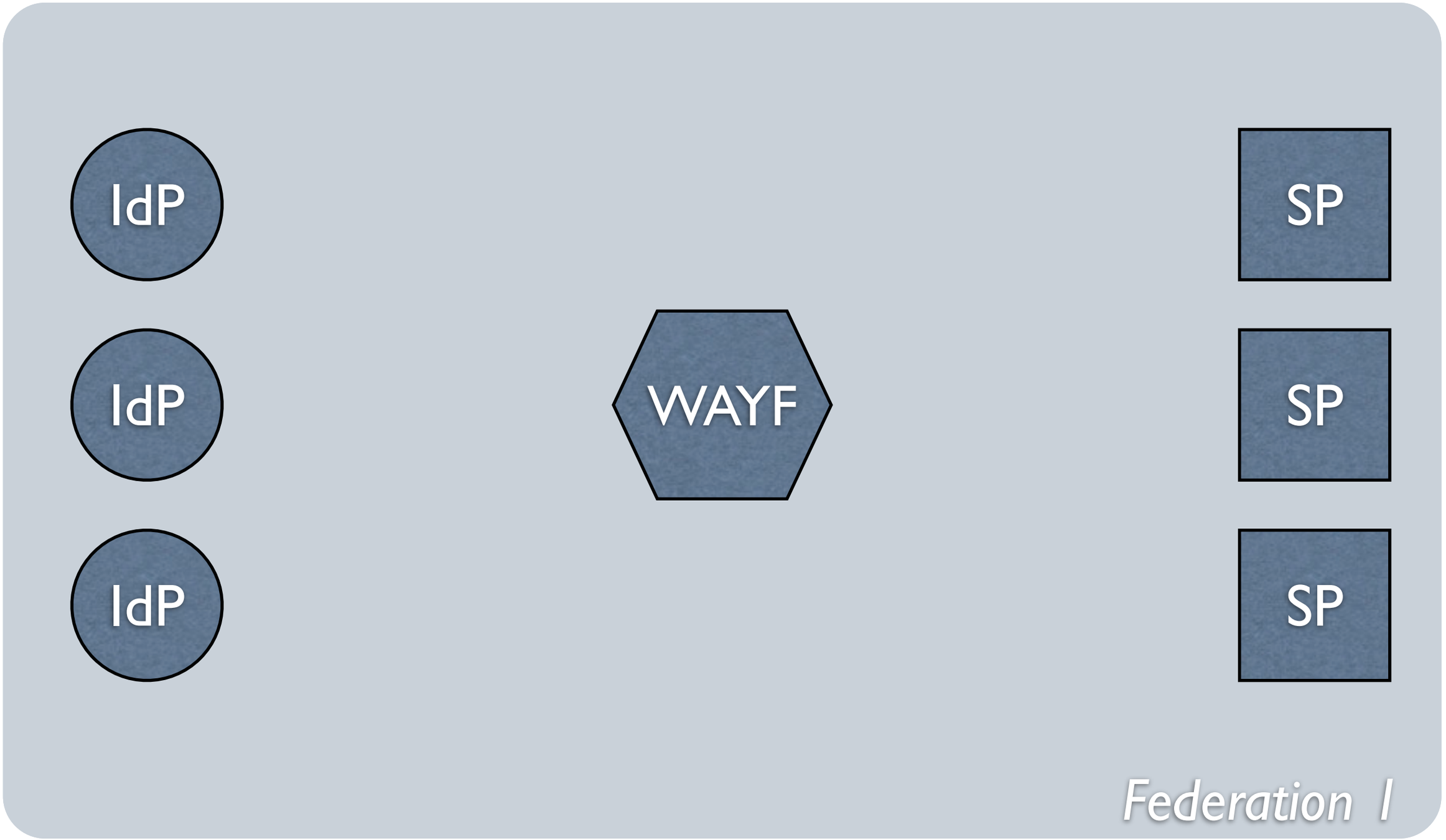

9:20:41

Interfederation

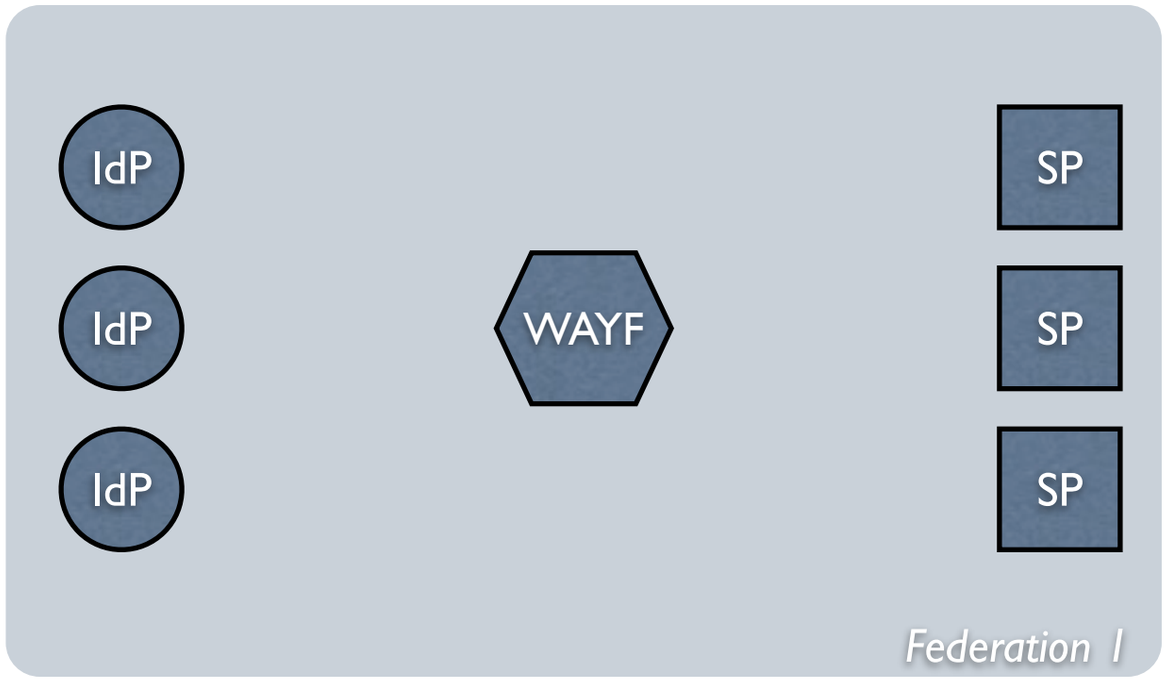
The best way
to predict the future
is to invent it.

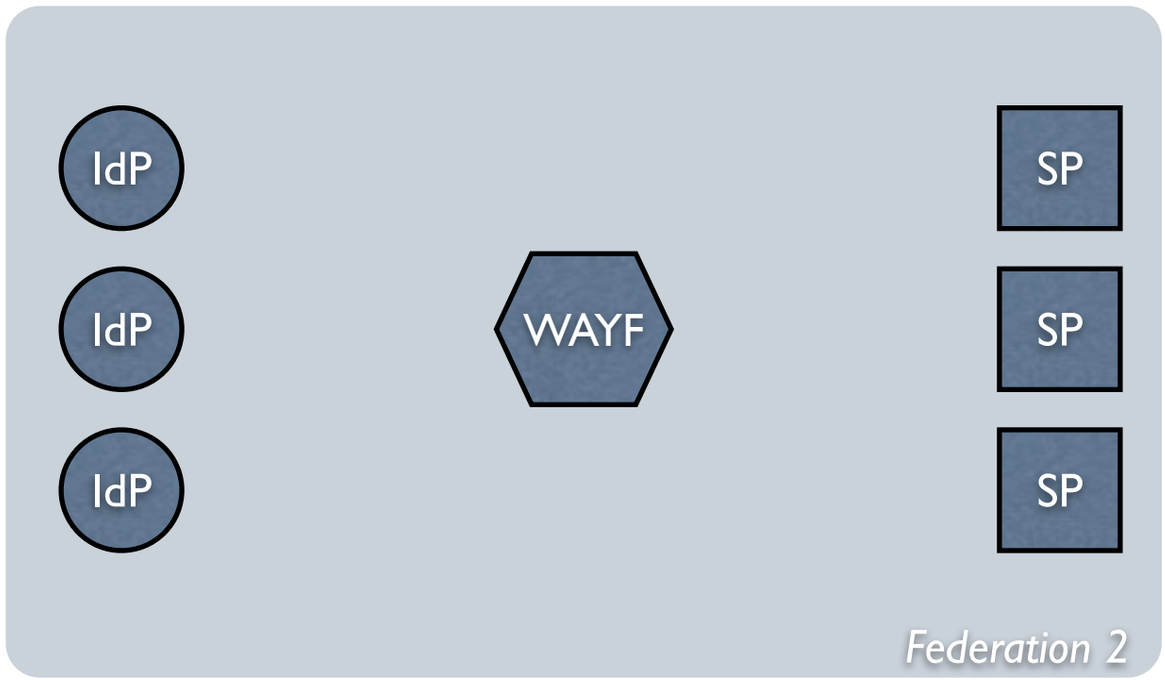
– Alan Kay

How *not* to think about interfederation

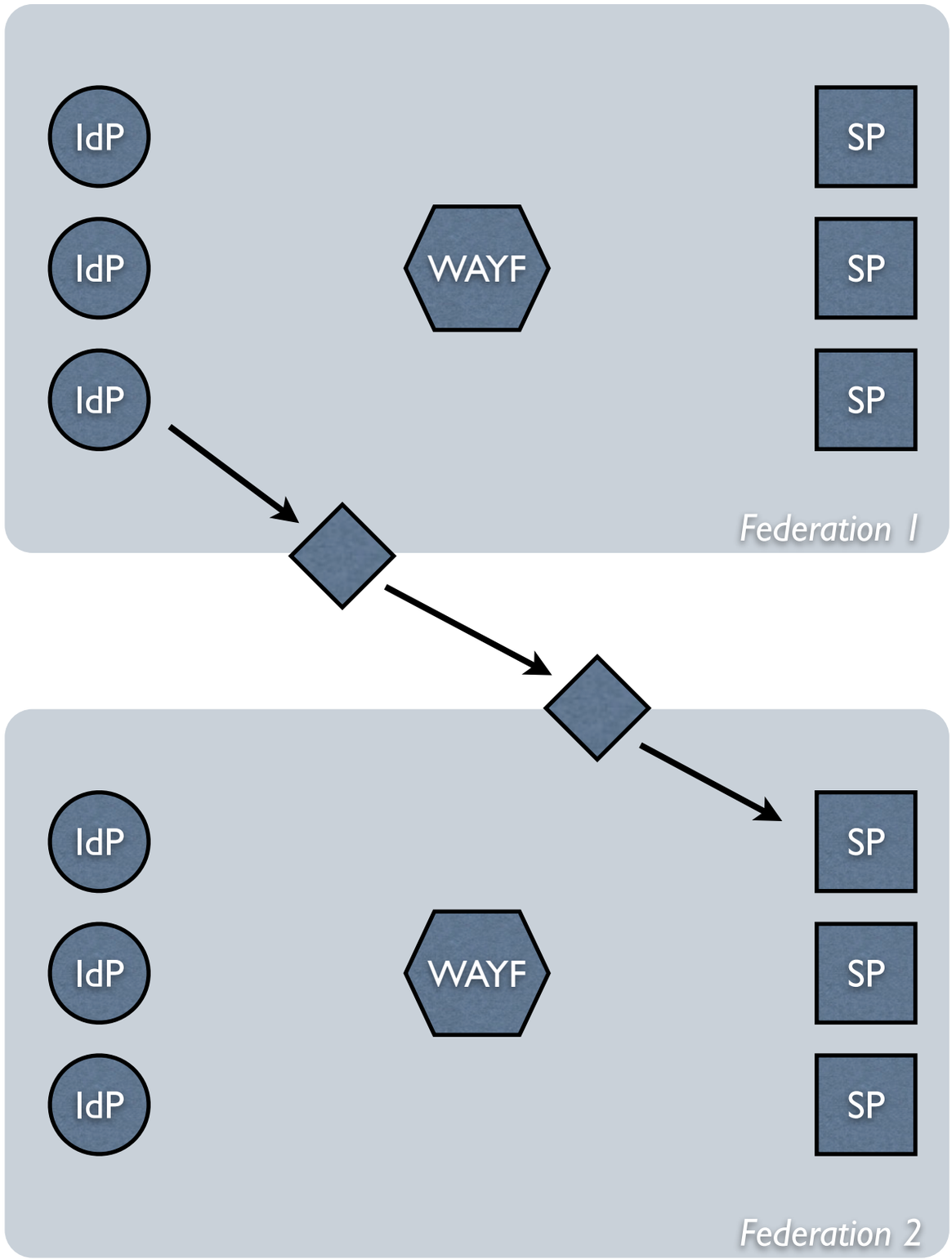


How *not* to think about interfederation





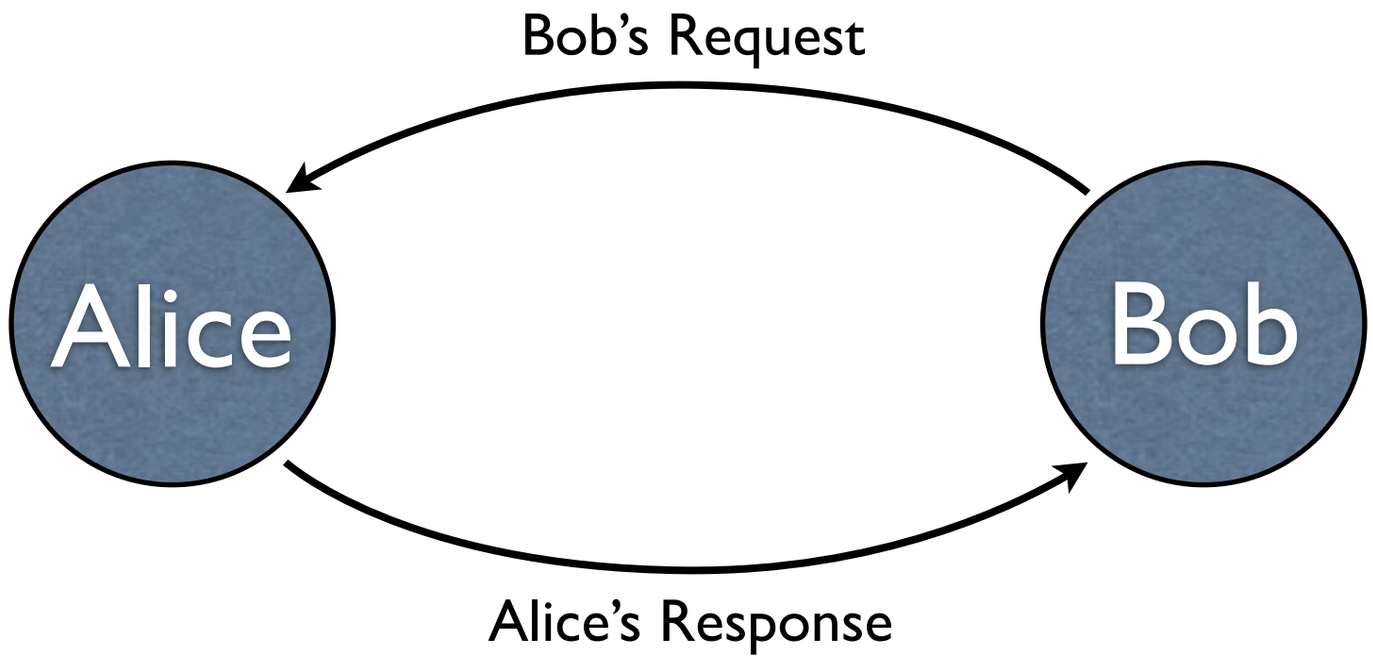
How *not* to think about interfederation



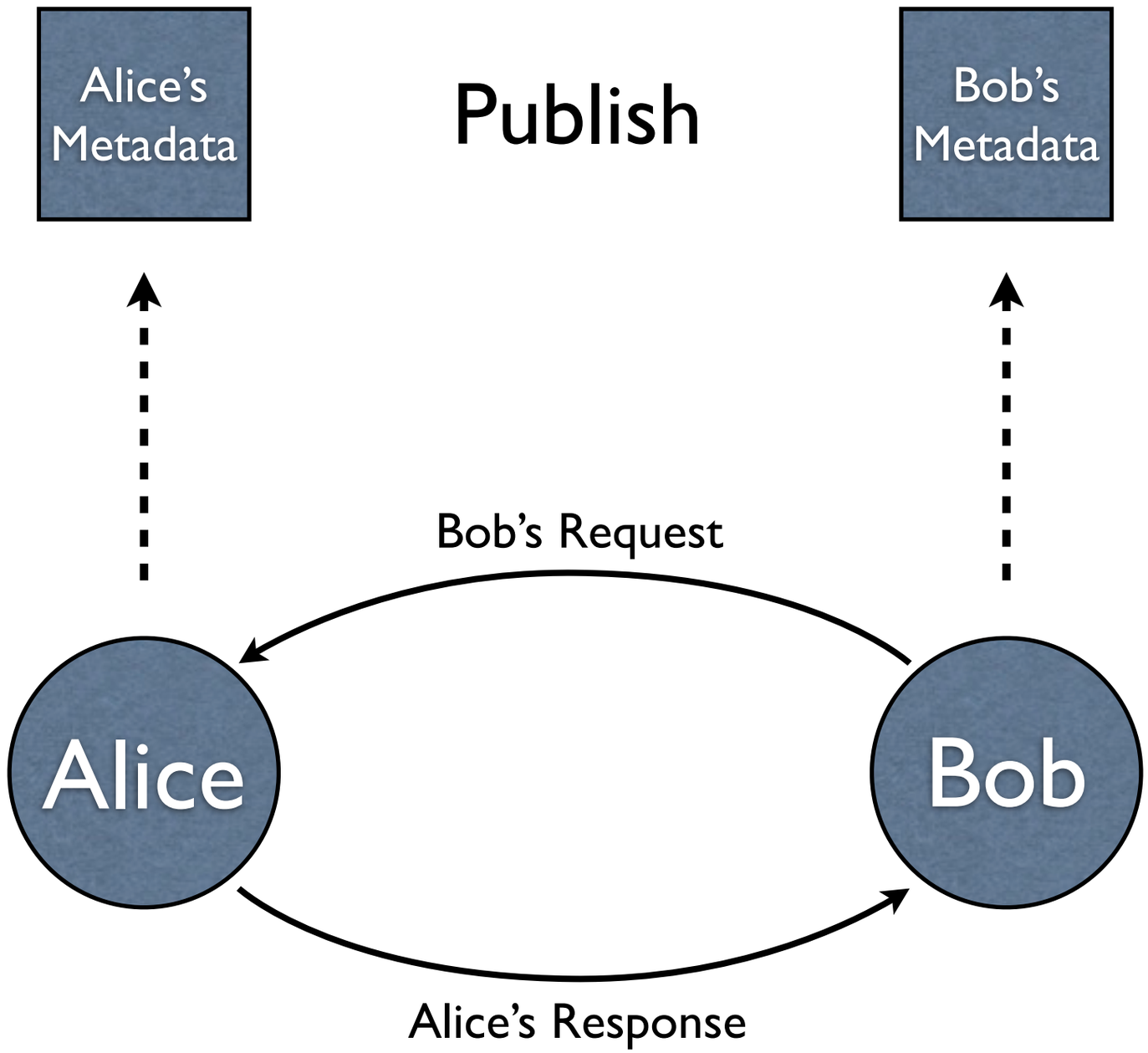
The software doesn't know about federations

– Scott Cantor

Peer to Peer Conversation



Peer to Peer Conversation

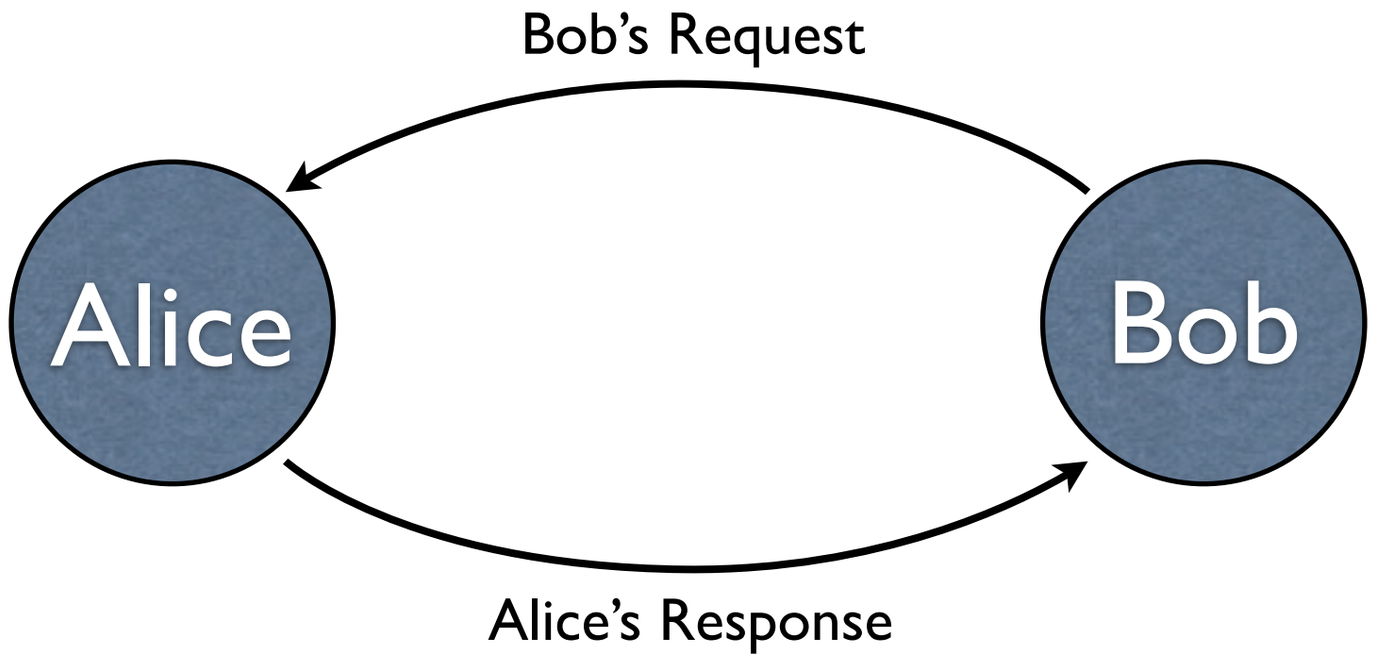


Peer to Peer Conversation

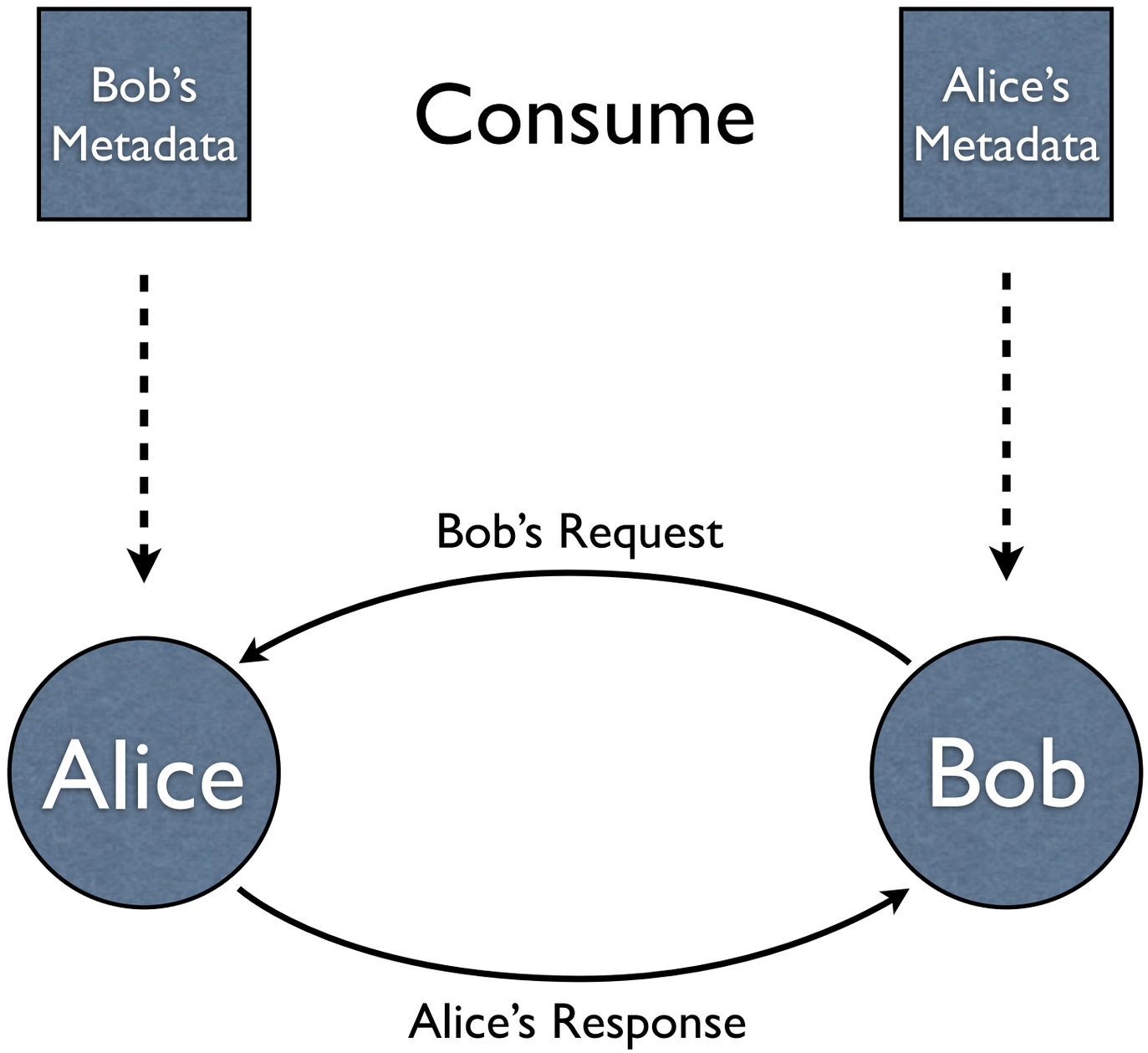
Bob's Metadata

Exchange

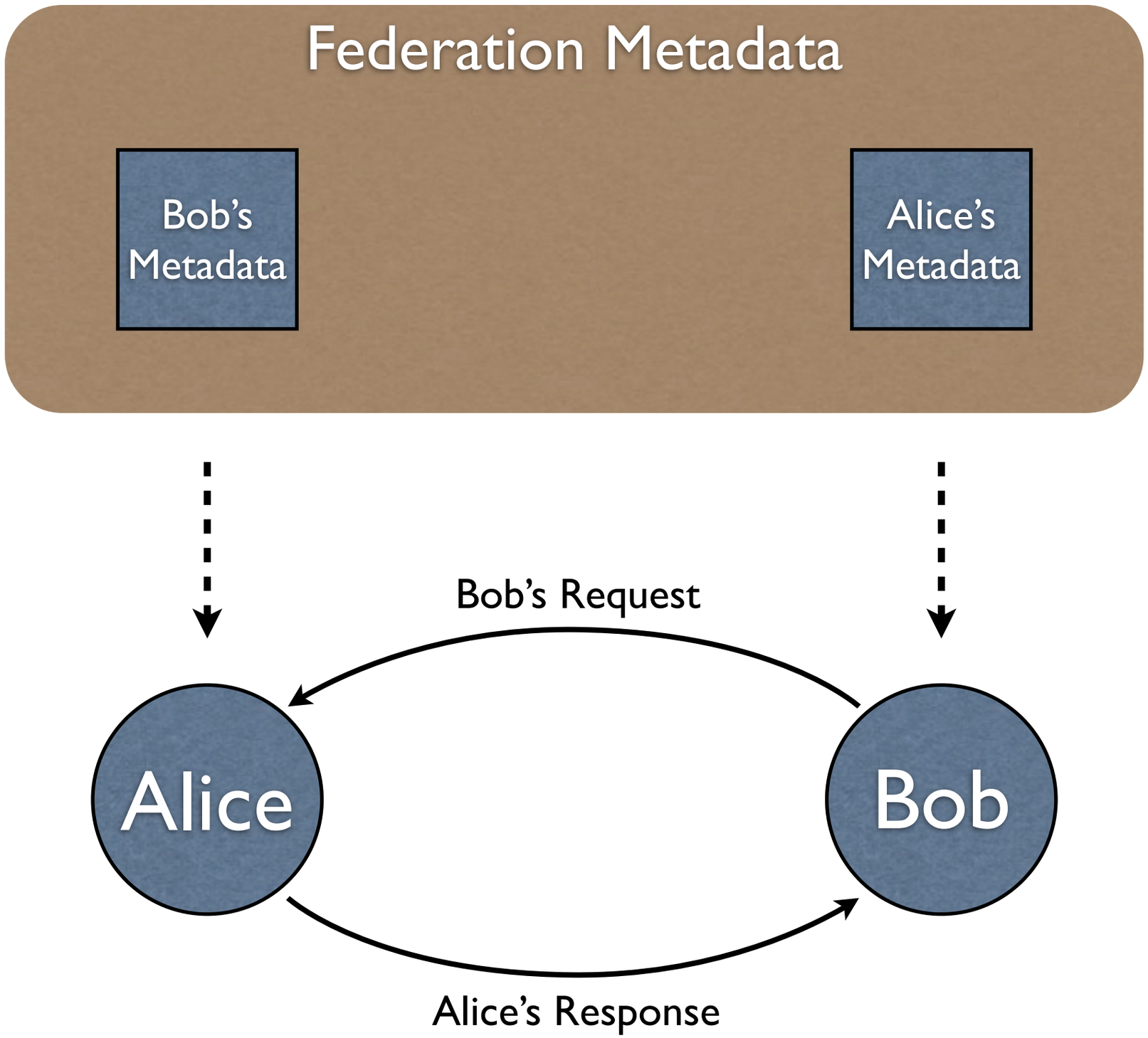
Alice's Metadata



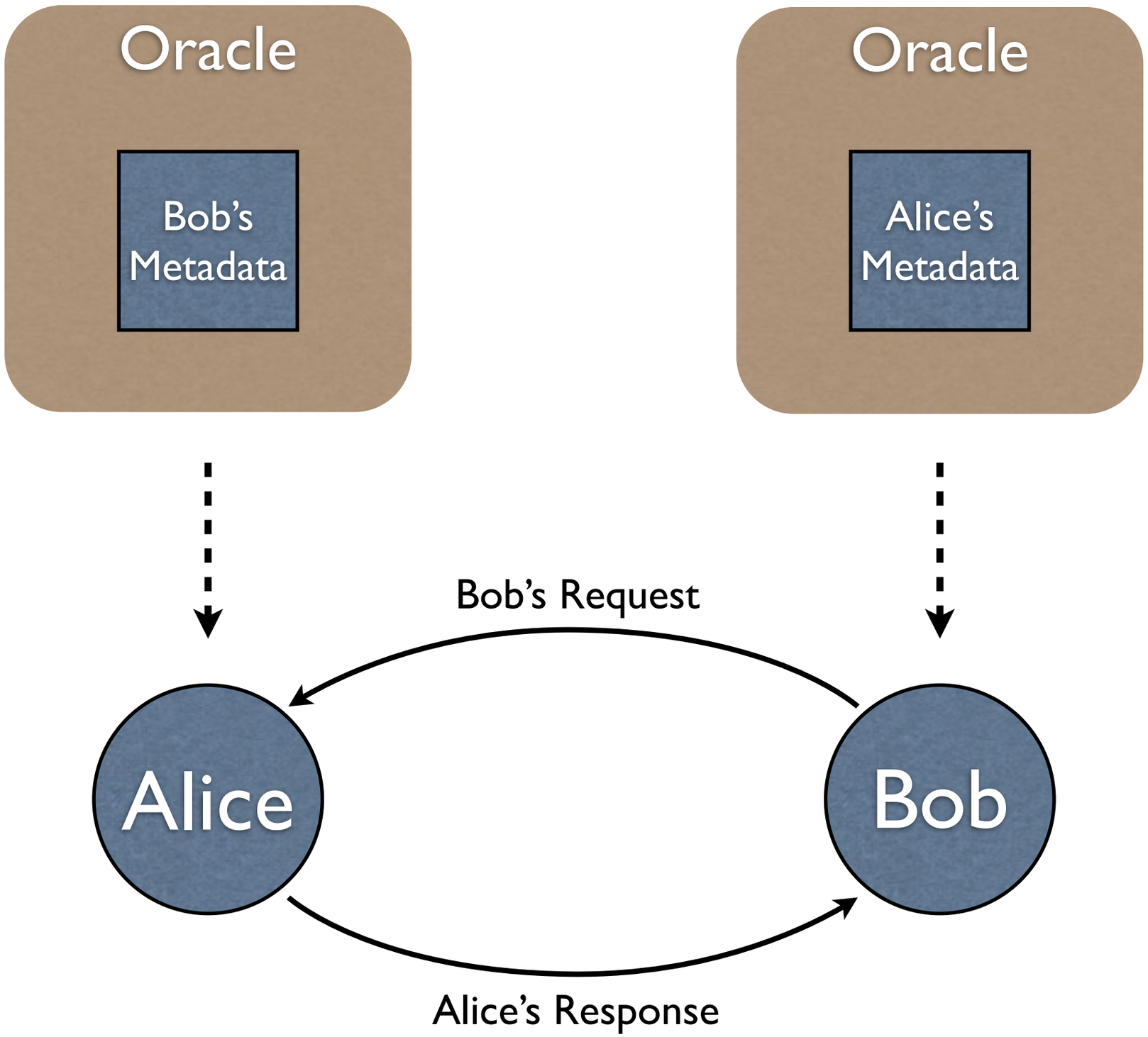
Peer to Peer Conversation



Peer to Peer Conversation



Peer to Peer Conversation



Interfederation is Easy!

- Entities register with their "home federation" with an expectation of universal publication (as with, e.g., the DNS).
- Federations collaborate to exchange entity metadata universally.
- Each federation provides its members with a trusted subset of all available metadata.

OK, not so easy

- Metadata exchange technology ("aggregation engines") yet to be invented.
- Scaling issues if done naively.
- Harder to build multi-lateral agreements between federations than bilateral ones.
- Summary: not trivial, but very possible.
- Watch this space.

Q&A / Discussion