Federation 101 Refresher

Interfederation and eduGAIN

Peter Schober, ACOnet (Austria)

GÉANT SA5 T4 Training

Vienna, April 21st & 22nd, 2015

Large-scale interfederations

In the academic vertical sector:

- eduroam
  - Global WiFi roaming, 802.1X
- Kalmar 2
  - 1st WebSSO interfederation, Nordic countries
- eduGAIN
  - Global SAML WebSSO Interfederation

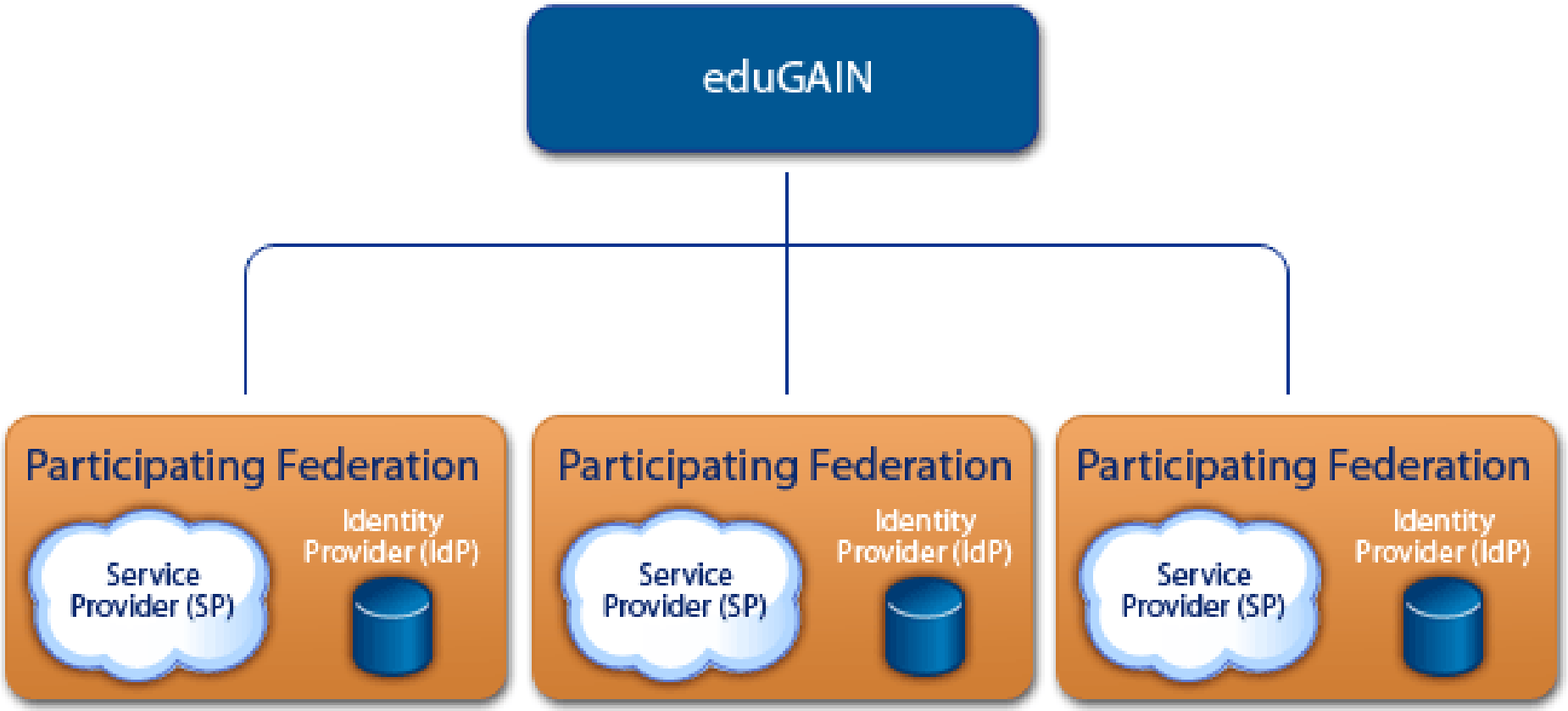
Confederation vs. Interfederation

Confederation often implies common rules for all federations and/or their members, i.e., common rules for every HO/IDP and SP.

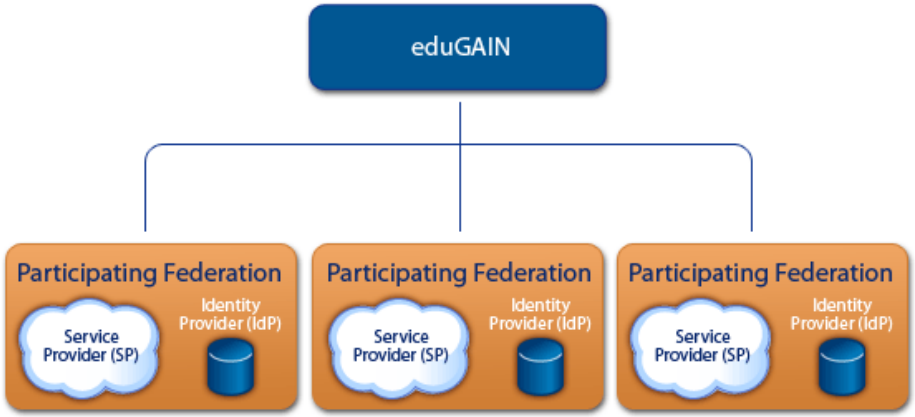
Interfederation inter-connects federations without establishing One Rule To Bind Them All

Today we refer to eduGAIN as an *Interfederation service.*

eduGAIN basic structure



eduGAIN basic structure

So what does 

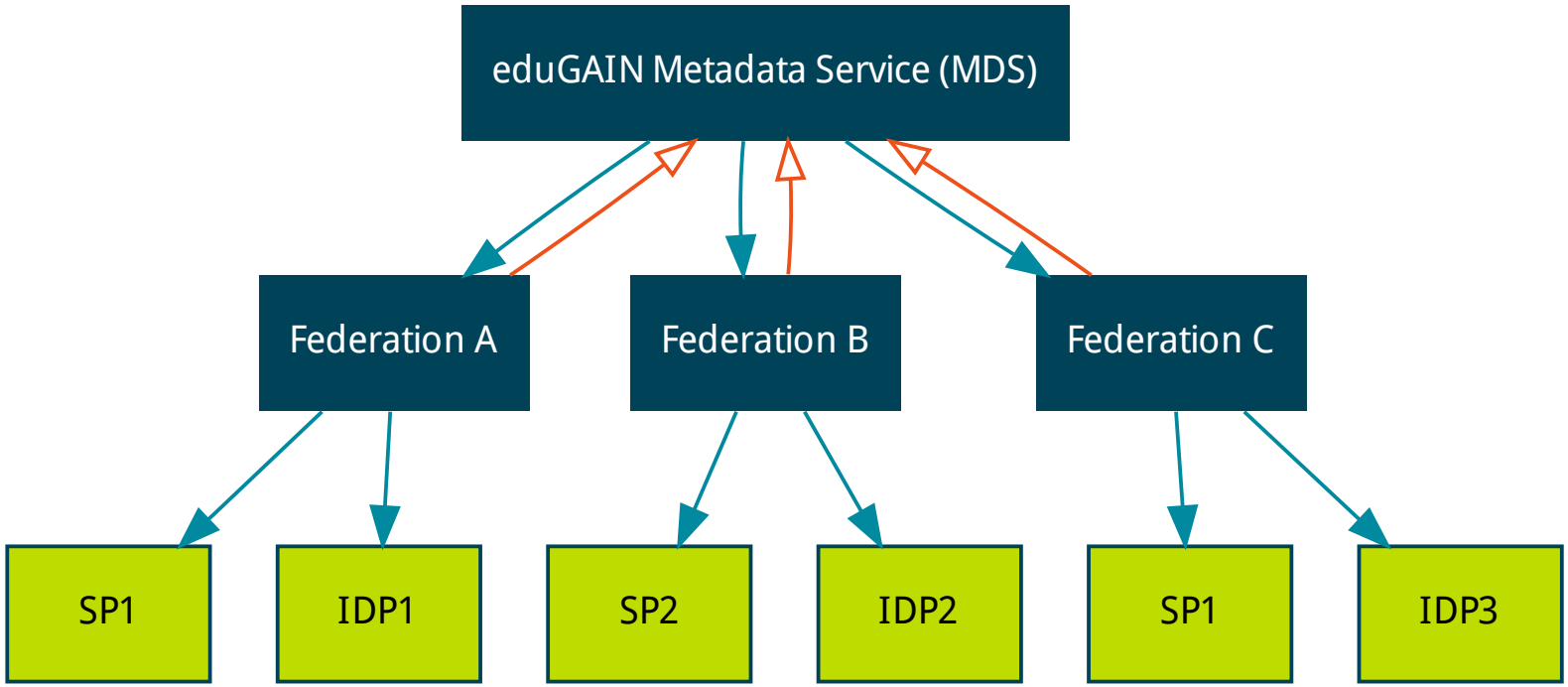
mean?

What eduGAIN does

eduGAIN mediates the exchange of SAML Metadata – describing IDPs and SPs – between participating federations (plus a bit of policy).

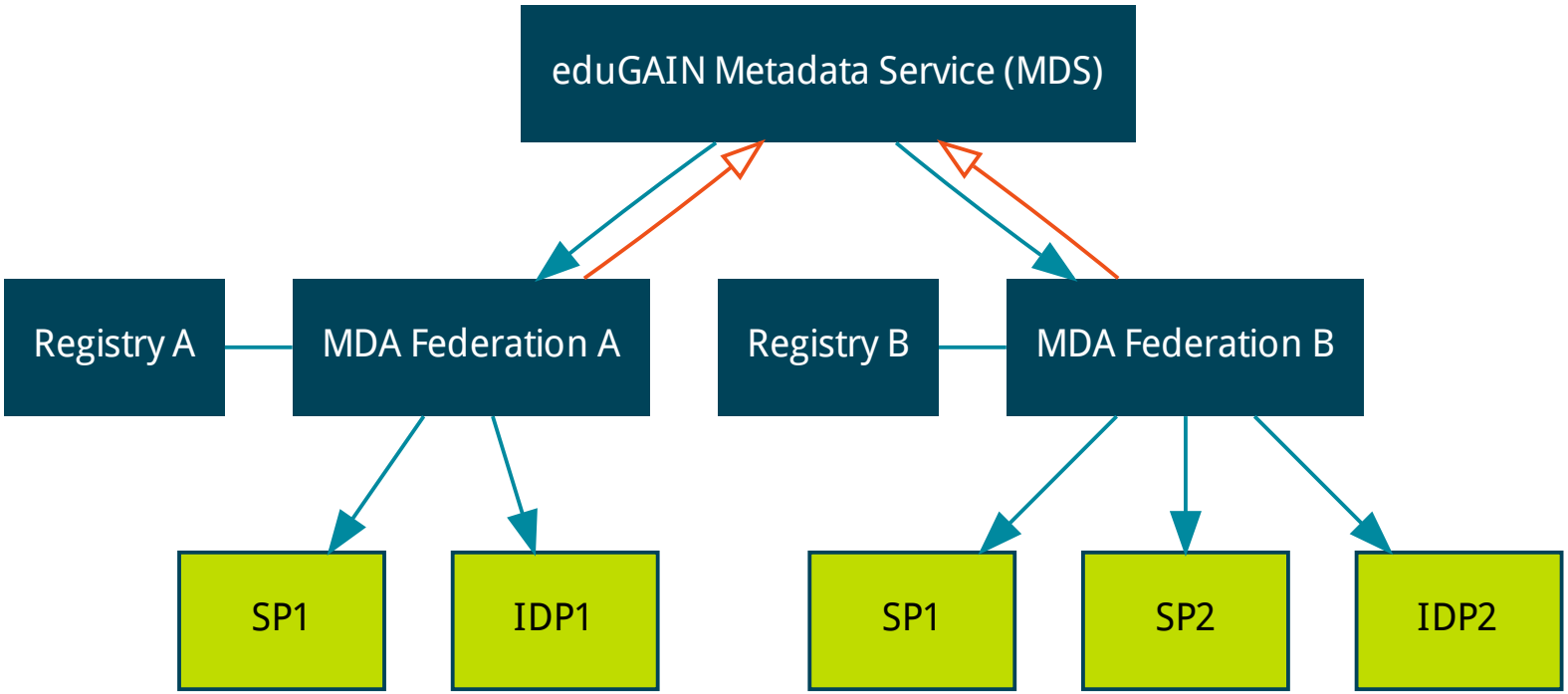
eduGAIN Metadata flow (1)

Upstream and Downstream flows, from Aggregators to Entities:

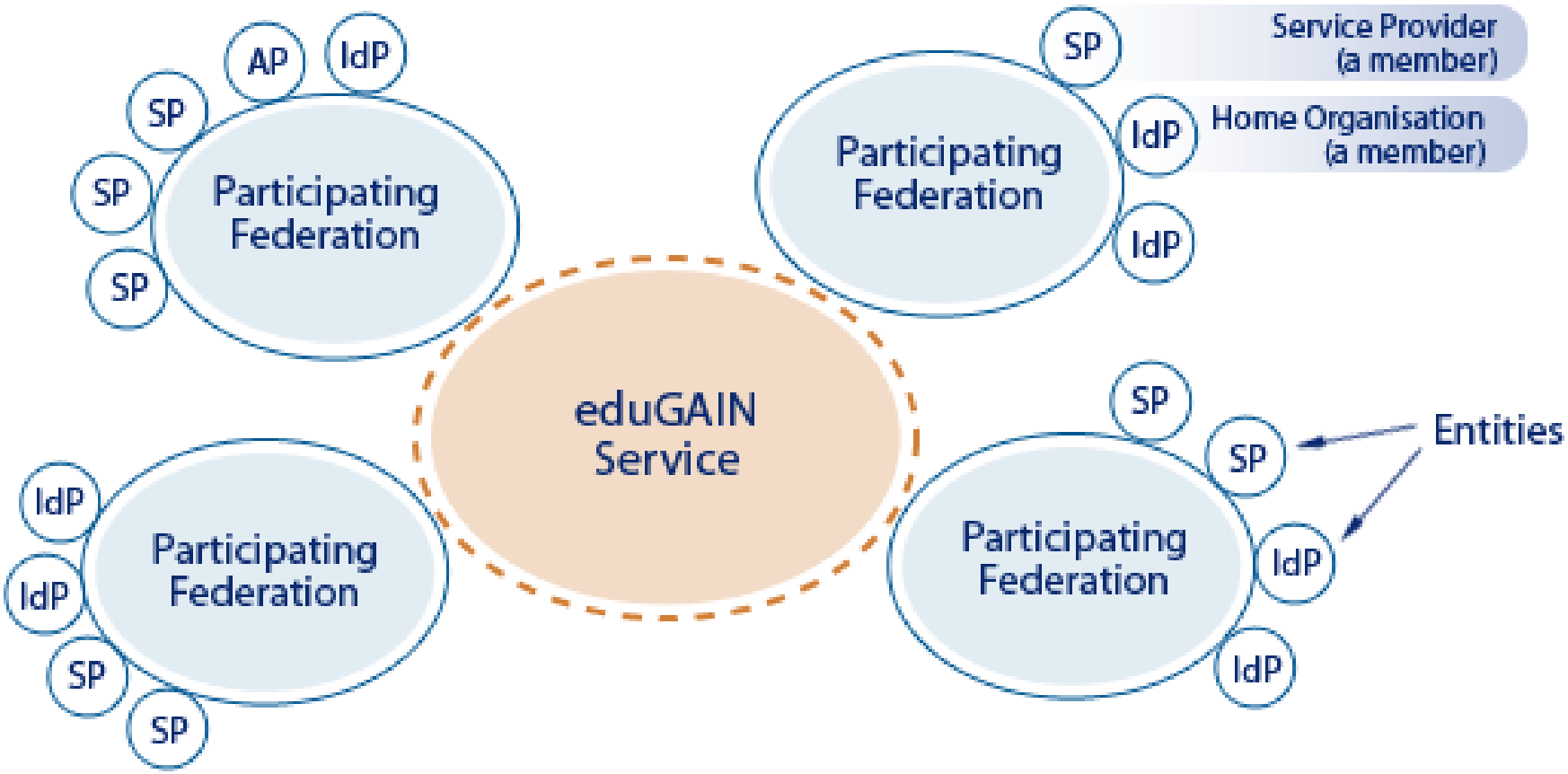


eduGAIN Metadata flow (2)

Upstream and Downstream flows, from Aggregators to Entities:



The eduGAIN “pond”



eduGAIN vs. `/etc/hosts`

- Who remembers (or has heard of) the `hosts` file?
- What is it?
- Sounds a bit like eduGAIN:

  Only the ones “in the pond” know about each other

  - Neither necessary nor sufficient for communication
  - But is needed to scale communication between “members”
- (Identity) infrastructure!
  - Because most use cases are too small to justify the effort

Interfederation as the norm (1)

- Building federations is building silos
  - Makes sense: trust, resilient/distributed architecture
- Not inter-connecting those silos is failing your community
  - Services and research are heavily inter-/multinational today

Interfederation as the norm (2)

Current thinking in the eduGAIN community:

- Expose all “your” IDPs to eduGAIN by default
  - but allow for opt-out
- Decide whether to do the same for SPs (or opt-in)
  - Opt-in may never happen, often for no good reason

Near-term goal

Make interfederation participation *much* easier, make it the default/norm where possible.

Interfederation as the norm (3)

Existence of entities in SAML Metadata (incl. eduGAIN) alone is almost *never* sufficient for service access! Nothing to fear!

Identity Providers

protect themselfs via controlled attribute release.

Service Providers

protect themselfs via Access Control Lists/rules.

Let the Metadata flow!

Interfederation as the norm (4)

Trade-off between

- Automating IDP Discovery (and Access Control?!) via specially tailored Metadata aggregates

versus

- Connecting the silos, connecting Subjects with Services, wherever they are! (NREN mandate!)

Questions & Answers

- Can you name differences between a federation and an interfederation service?
- Is participating in (inter-)federation different for IDPs and SPs? What about risks?
- What services benefit most from Interfederation/eduGAIN? Which services the least/not at all?