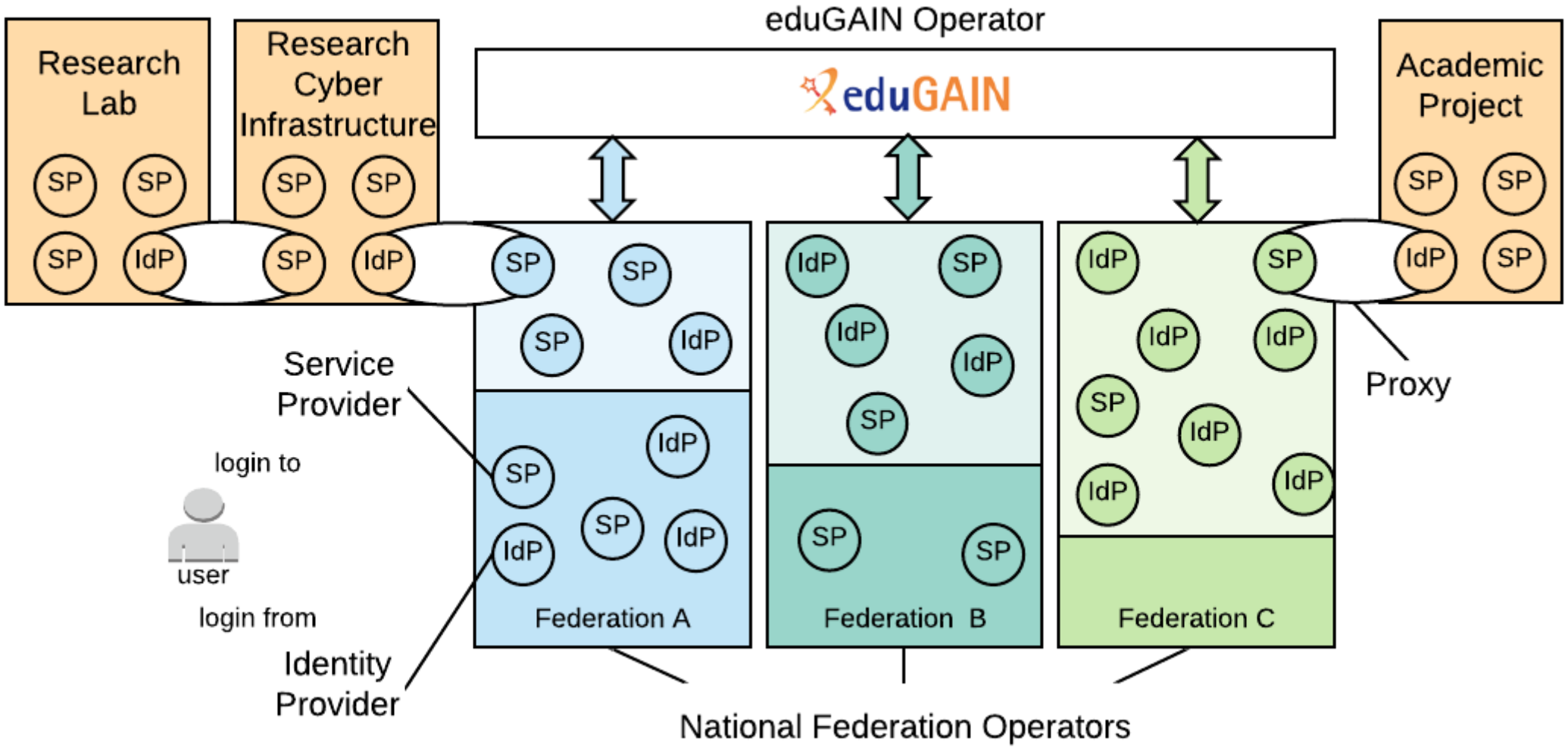
Trust Frameworks Across Proxies

Tom Barton

UChicago & Internet2

Recall how federated access happens



Trust Frameworks

- A trust framework is
  - A standard of behavior that applies to participants and/or components in large, complex, even global systems
  - Developed in response to identified needs of research and scholarly activities
- We trust that trust framework adopters reasonably observe the defined standard of behavior because of our shared mission in Research & Education
- Federations and other organizations enable and monitor trust framework participation and may operate processes to verify or compel adoption

Research & Scholarship attribute release

- Name, email, affiliation, persistent identifier
  - Common need for “research and scholarship” services
- Those service providers are “tagged” by their national federation operators as “R&S”
- Identity Providers automatically release the R&S attributes to R&S tagged services
- Such Identity Providers are also tagged as “R&S” so that services can elect to require R&S attributes in order to provide service
- The R&S program contributes to good privacy practice under the European General Data Protection Regulation (GDPR)

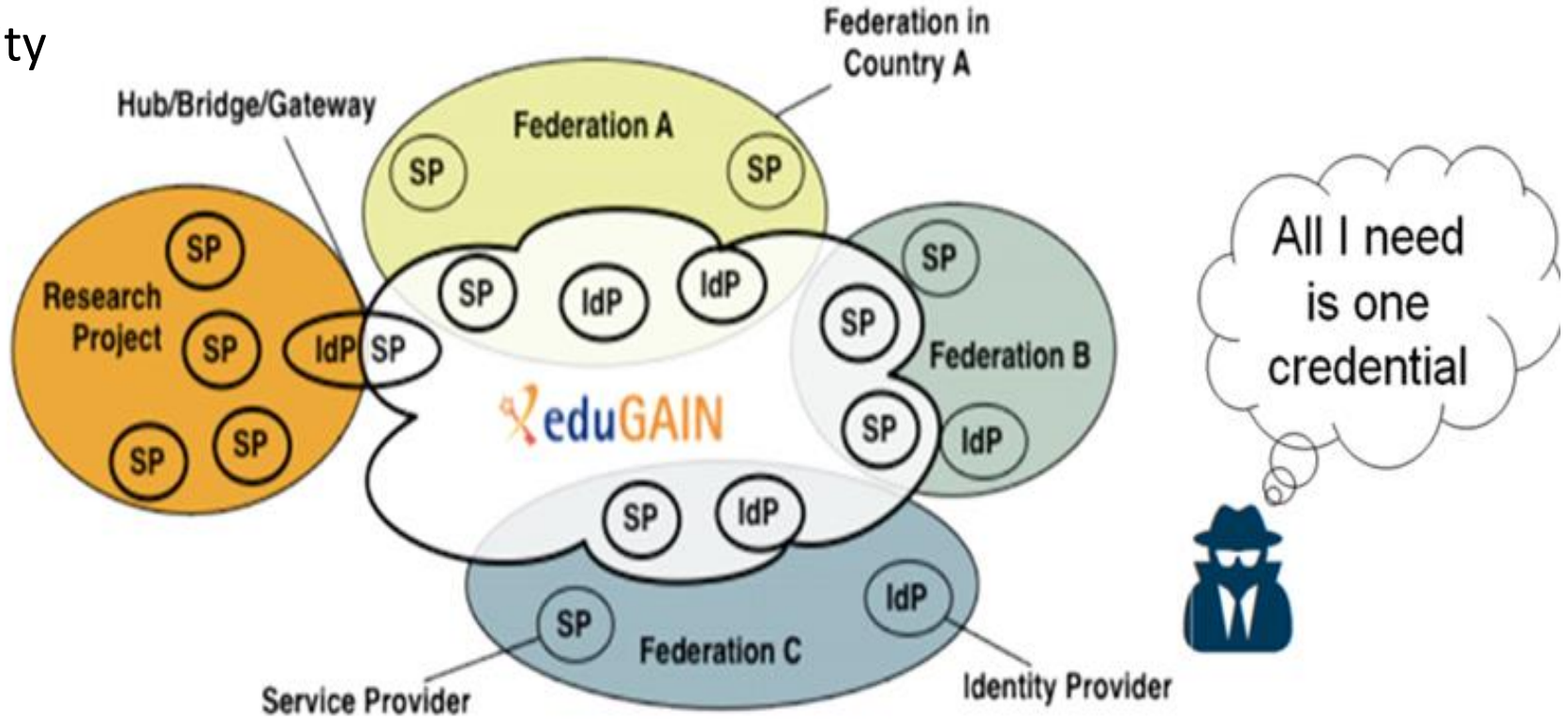
SIRTFI - security incident response trust framework for federated identity

Be willing to collaborate in responding to a federated security incident.

Apply basic operational security protections to your federated entities

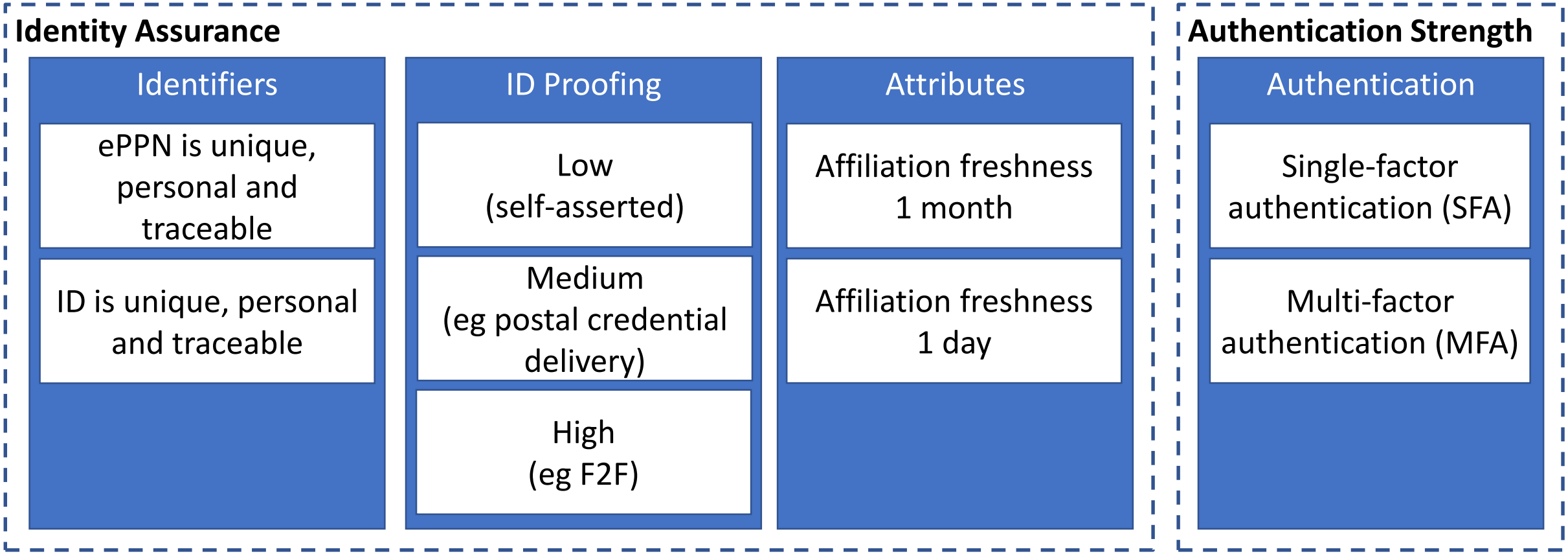
in line with your organization's priorities.

Self-assert SIRTFI "tag" so that others will know to trust this about you.



REFEDS Assurance Framework

Defines a standard means for service providers to receive information about identity assurance practice and request and receive information about strength of credentials



Proxies

Good

- Enable federated access to resources not designed for that
- Efficient design compared to alternative of outfitting each resource to handle federation
- Good means to harmonize access management across many resources

Not so good

- Bridges distinct communities

→ Hard for operators

→ No common community leadership group or authority

→ Trust frameworks need not cross the bridge

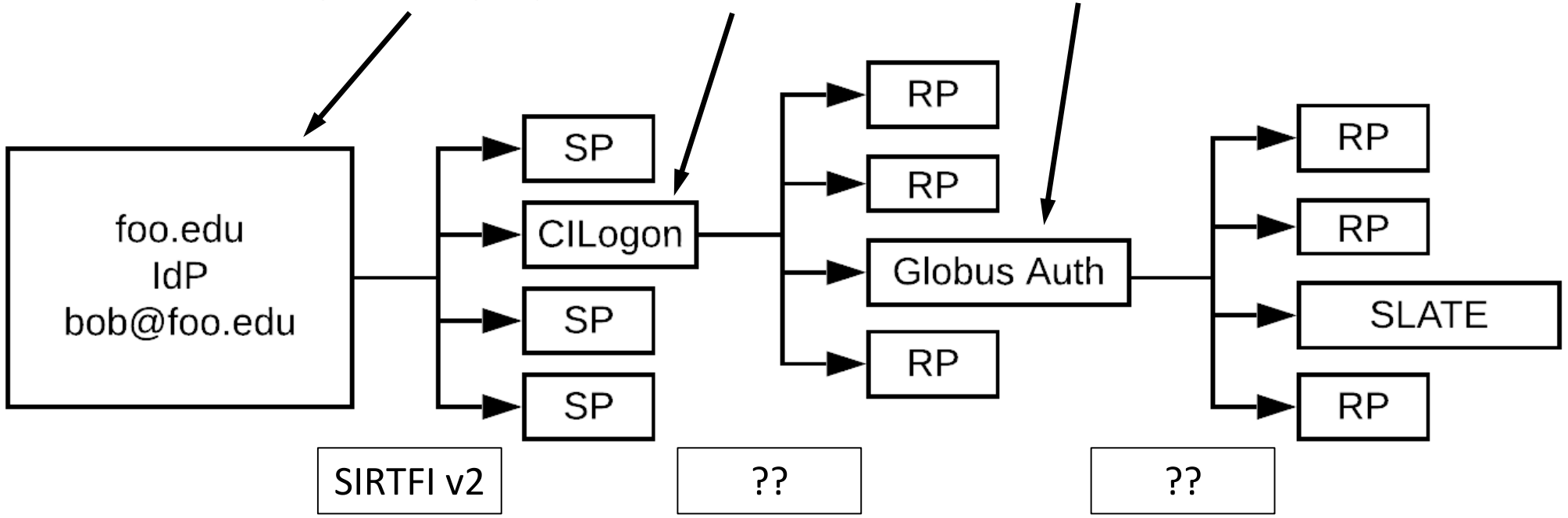
We certainly want an incident response trust framework to apply.

Any others we really care about?

Focus: compromised account notification

- SIRTFI v2 will include an obligation to suitably notify downstream stakeholders of compromised accounts
- How can notification happen across the proxy-integrated R&E Fed ecosystem?
- SLATE example

1. Deactivate Bob's credentials
2. Dig out login|token records & notify (ID, date, status)



- Commercial SP|RPs are not notified (origin org's CERT handles by contract)
- Which non-commercial SP|RPs should be notified?
- How should notification be delivered?
- Deliver 2 notifications: status = bad, status = good?
- Any significant variations depending on credential|token type?

That approach can work, but …

- Manual steps mean slow propagation
- No single policy or trust framework applies across the system

→ Each proxy operator must figure it out themselves and gain cooperation of their downstream RPs

- No single body has standing across all interconnected communities
- Need SIRTFI v2 to set compromised account notification in motion!

ID-Events: How some cloud services do it

- IETF secevent working group
- JWT schema to express security events such as
  - Fraudulent use of account
  - Revocation
  - Logout
  - Provisioning events
- Push/pull over HTTP
- Subscription & validation of subscription requests
  - Technical, not policy

How might R&E adopt id-events?

- ID-Event API at each org? No!
  - O(10^3) orgs, immense change management, not much better than email
- So, more centralized API operation, across IdPs & SP|RPs
  - Operator(s)
    - Liability, trust
  - Delegated management of API tokens
    - Towards those who actually know whether a given org/actor should source or subscribe
  - Policy
    - Who can source events
    - Who can subscribe
    - MOUs for subscribers, delegates, sourcers
- One per “domain”? (national federations, groups of research CIs,…)
- One for R&E, globally?

Is a more centralized id-events approach worth it? Is there another way?

How can any trust framework be adopted across the R&E Fed ecosystem?