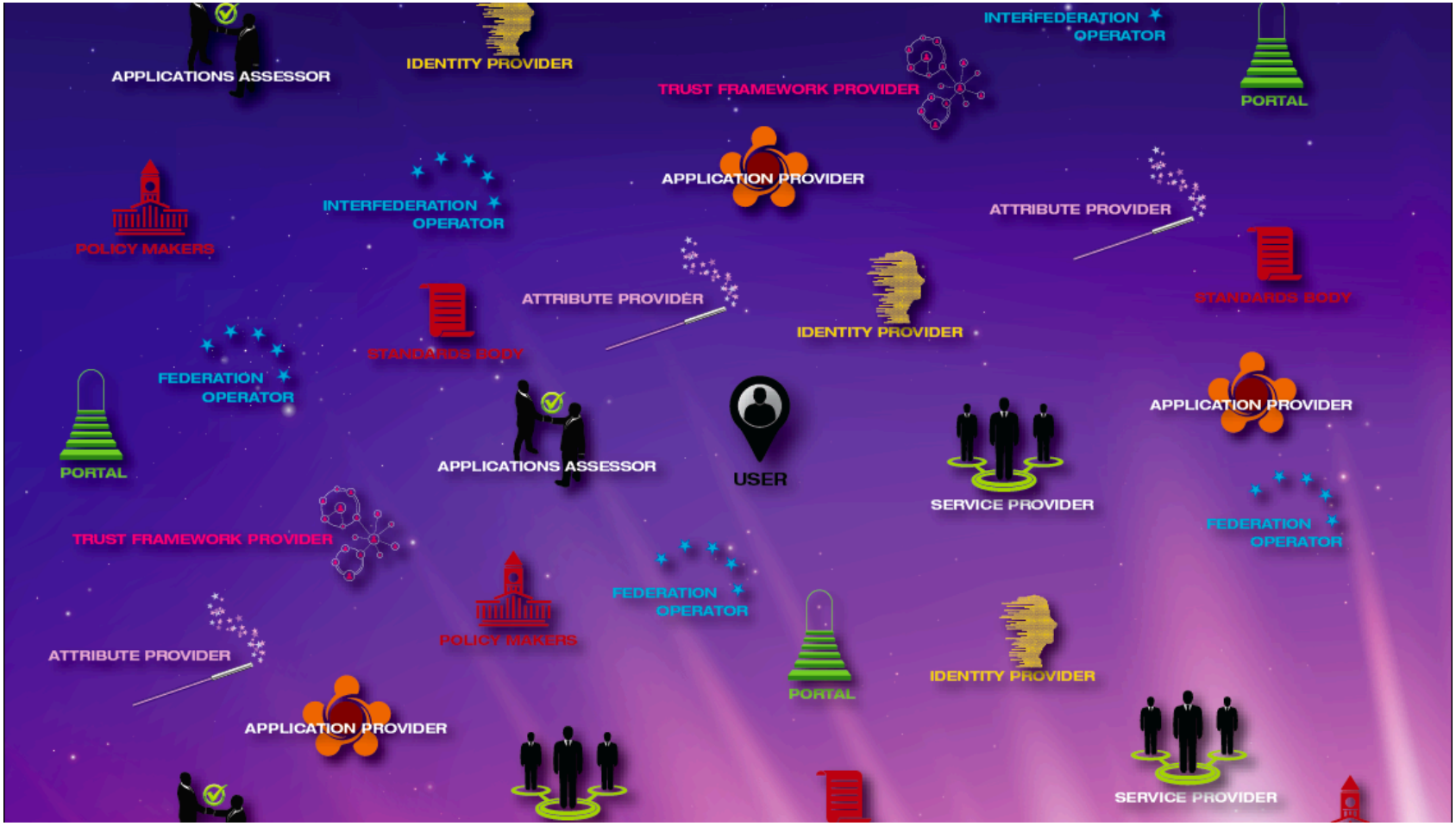
The Attribute Ecosystem

The Attribute Ecosystem

- Those parts of the identity ecosystem that focus on attributes in the ecosystem
- Centers on the creation, exchange and use of attributes associated with those in the identity ecosystem
- Critical to privacy, scalable access control, etc.
- Depends heavily on other aspects of the identity ecosystem, including authentication, trust, etc.
- The relatively unexplored part of the landscape.

A part of the attribute ecosystem



Elements of the Attribute Ecosystem

(an evolving understanding)

- IdP's
- SP's
- Attribute authorities and providers
- Attribute verifiers
- Trust frameworks and trust framework providers
- Third parties, portals, etc.
- Federation operators
- Application auditors
- The user, and, if applicable, the subject

Elements - 1

- Identity Providers (IdP) – A kind of service provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers within a federation (SAML Glossary)
- Service Providers (SP's or RP's) – Services that consume Assertions about Identity Attributes to make access control or business decisions (e.g., eligibility or entitlement) concerning the delivery of outputs.
- Attribute authorities/providers – sources of authority (either directly or through delegation to an Attribute Provider) for attribute values about a user
- Attribute verifiers - A type of Authoritative Party that provides yes-No Assertions, at some Level of Assurance, as to the correctness of one or more Identity Attribute values. If the Assertion is about more than one Identity Attribute value then it is an Assertion to the validity of each of the Identity Attributes and that they belong together as a set

Elements - 2

- Trust Framework (American Bar Association Id Management Legal Task Force):
  - The combination of rules and requirements and existing law for a specific identity system consisting of:
  - the Technical and Operational Specifications that:
  - o define requirements for the proper operation of the identity system (i.e., so that it works),
  - o define the roles and operational responsibilities of participants, and
  - o provide adequate assurance regarding the accuracy, integrity, privacy and security of its processes and data (i.e., so that it is trustworthy); and
  - the legal rules that govern the identity system and that:
  - o regulate the content of the technical and operational specifications,
  - o make the technical and operational specifications legally binding on and enforceable against the participants, and
  - o define and govern the legal rights, responsibilities, and liabilities of the participants of the identity system.
- Trust Framework Provider (TFP)
  - The organization that specifies, and certifies services that are in compliance with, a Trust Framework. A TFP can adopt a Trust Framework developed by another organization.

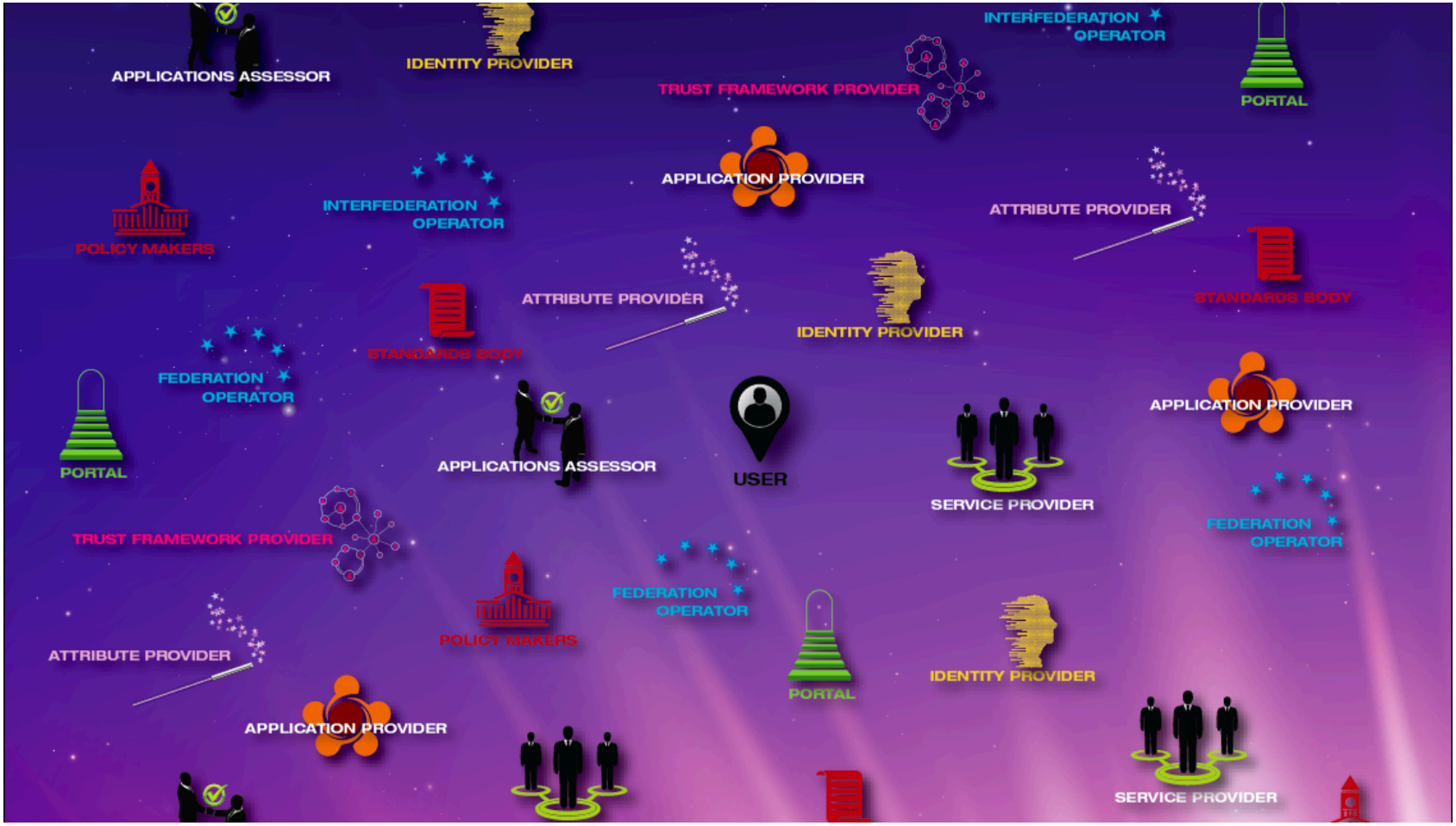
Elements -3

- Third parties, gateways, etc – organizations that act as intermediaries across a number of autonomous sites, trust frameworks, etc
- Federation operators – organizations that manage federations, vetting participants, gathering and publishing metadata, etc
- Application auditors – organizations that verify that applications are behaving as required by a Trust Framework with respect to attribute use and disposal.
- Standards Orgs – IETF, OASIS, Kantara, ITU, etc.
- Elements yet to be discovered…

The “User” Element

- Users, typically operating in one of several roles: employee, citizen, consumer, social, etc.
  - Some attributes cut across roles (e.g. preferred language) and some attributes are unique to a certain role (e.g. avatars, employee ids)
  - Roles may influence defaults, preferences, etc.
- One particular role – guardian (aka authoritative party, aka representative authority) is of particular importance and is distinguished by the subject of attribute assertions being different than the user making the assertions
  - Importance for legal and government processes, COPPA
  - Creates a useful user/subject distinction

Attribute Ecosystem Elements



Decomposing Google

- Google plays many roles within the attribute ecosystem:
  - As a very very large IdP
  - As an applications provider for many applications
  - As an applications auditor for third party apps in their stores
  - As an attribute authority for "harvested" attributes
  - As an attribute authority for self-asserted attributes (e.g. groups)
  - As a trust framework provider for its business partners
  - And more…
- The multiple roles, while essential to the business model, introduces complexity and tradeoffs that can raise public or market issues
- Other current organizations in the biz can also be re-viewed.

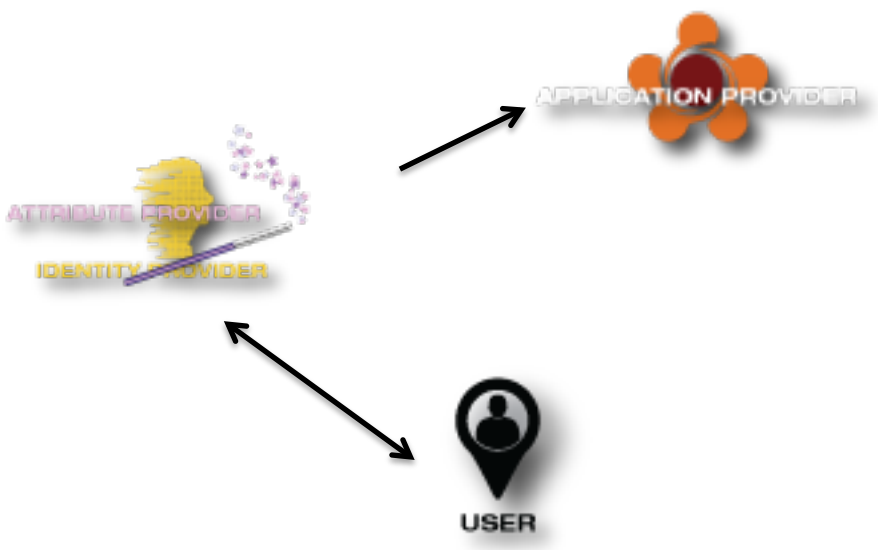
What Flows Within the Ecosystem

- Attributes
  - May be externally asserted (e.g. student, citizenship), self-asserted (e.g. preferred language), third party asserted (e.g. resident of a town), etc.
- Management of attributes
  - Trust, verified application information, user consent flows, etc.
- Others?
  - Liability,

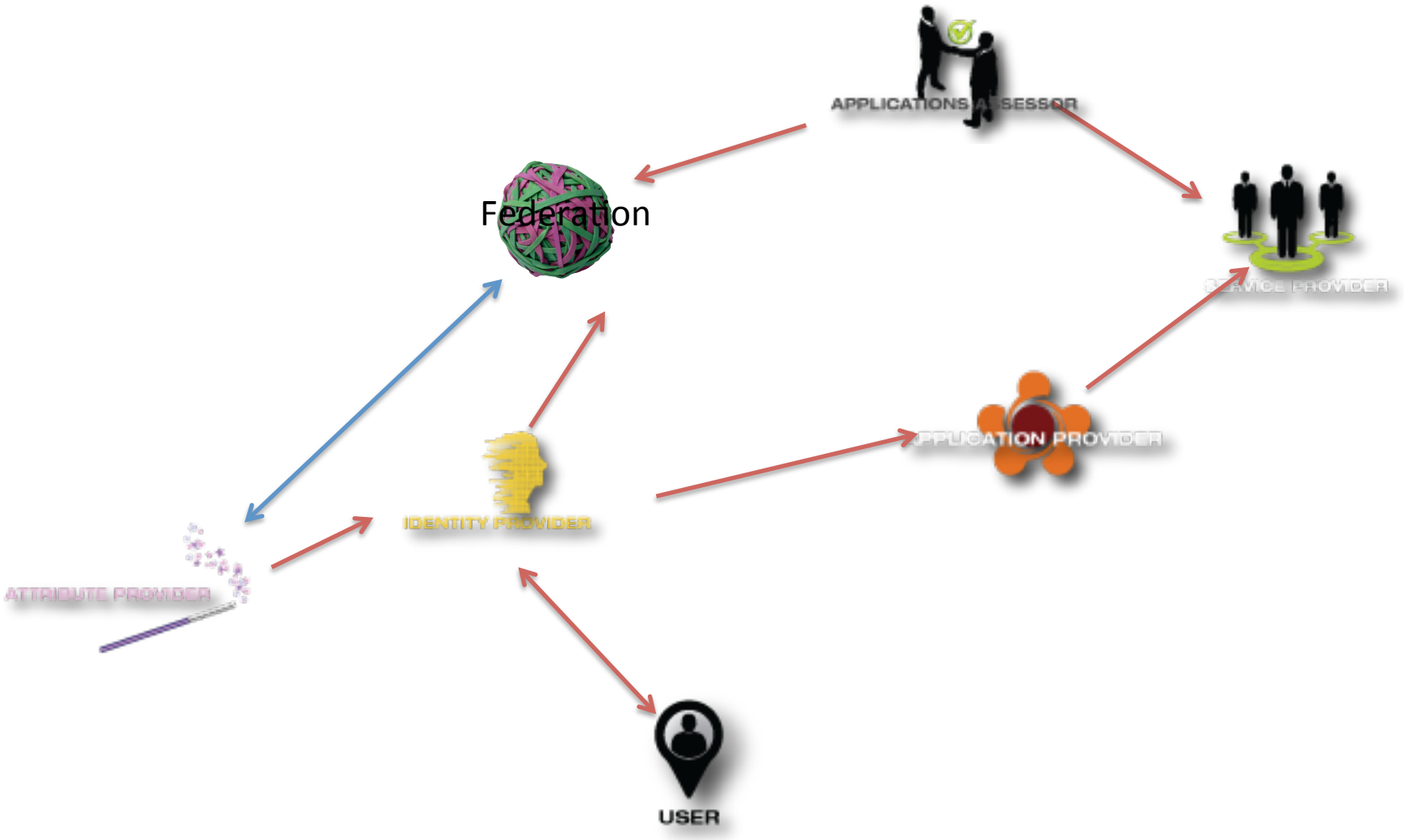
Types of attributes (by authority)

- Enterprise/employer-asserted
- Self-asserted
- Reputation systems asserted
- Government asserted
- Third-party asserted
  - Business
  - Certification authority
  - Device asserted?

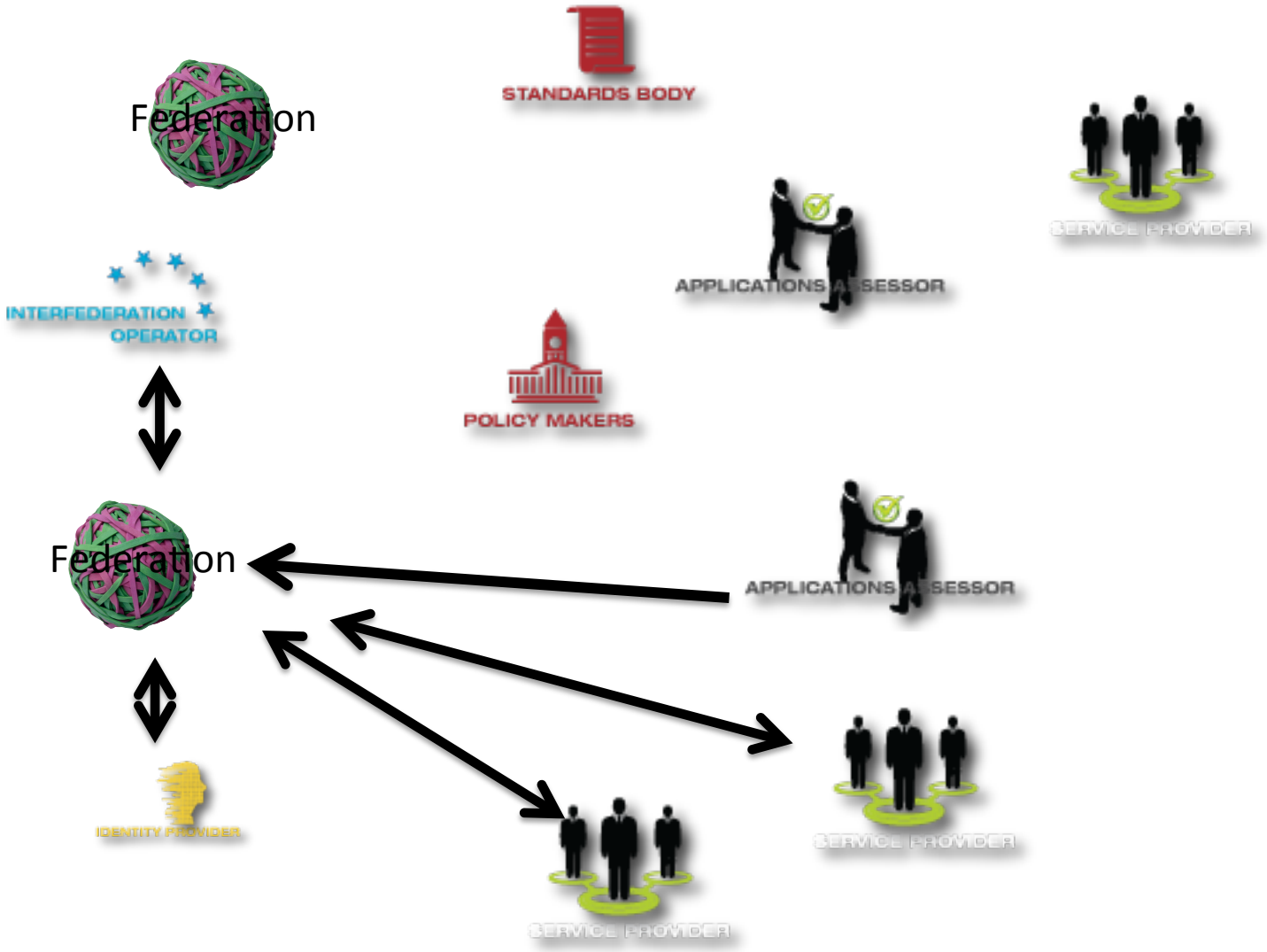
Standard enterprise attribute flow



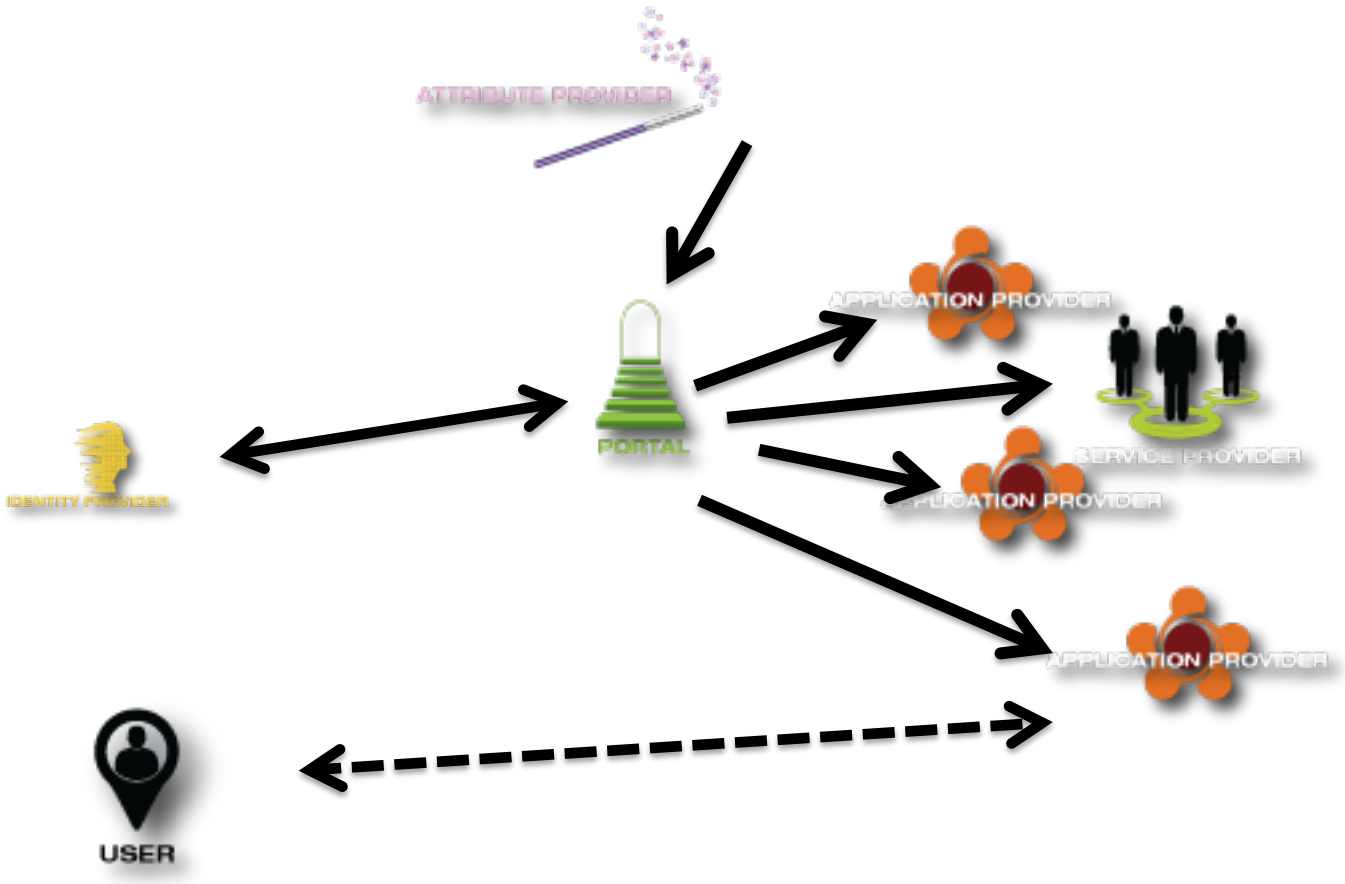
Sample associated meta flow



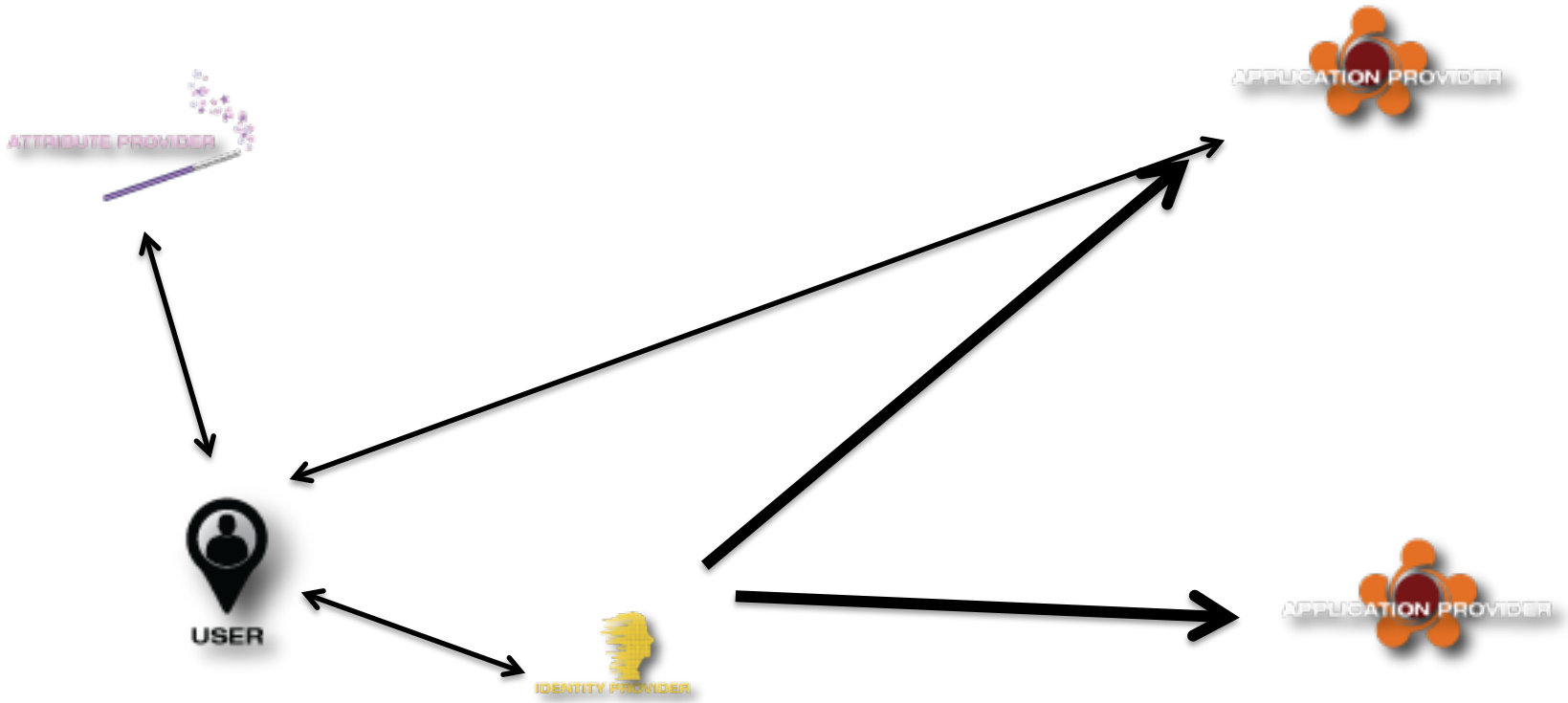
Anchor trust flows



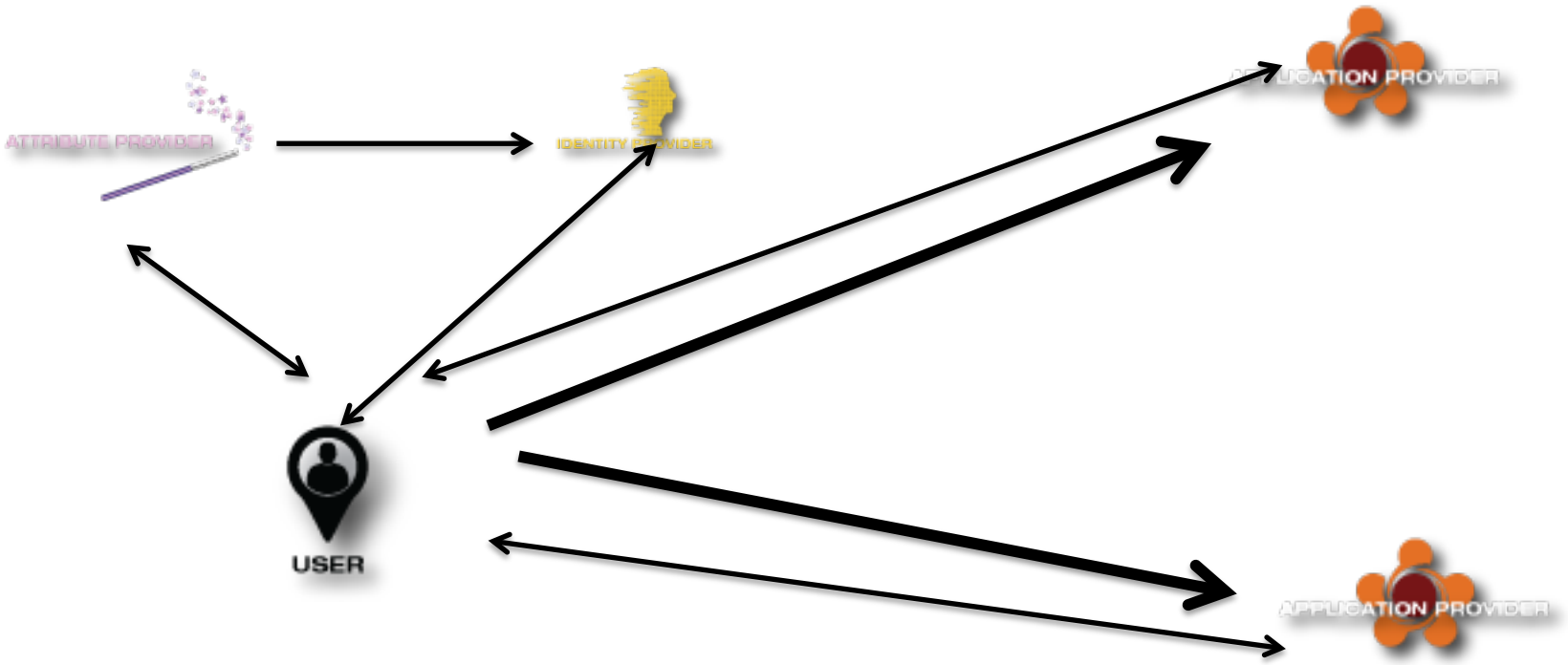
Science Gateway/VO Scenario



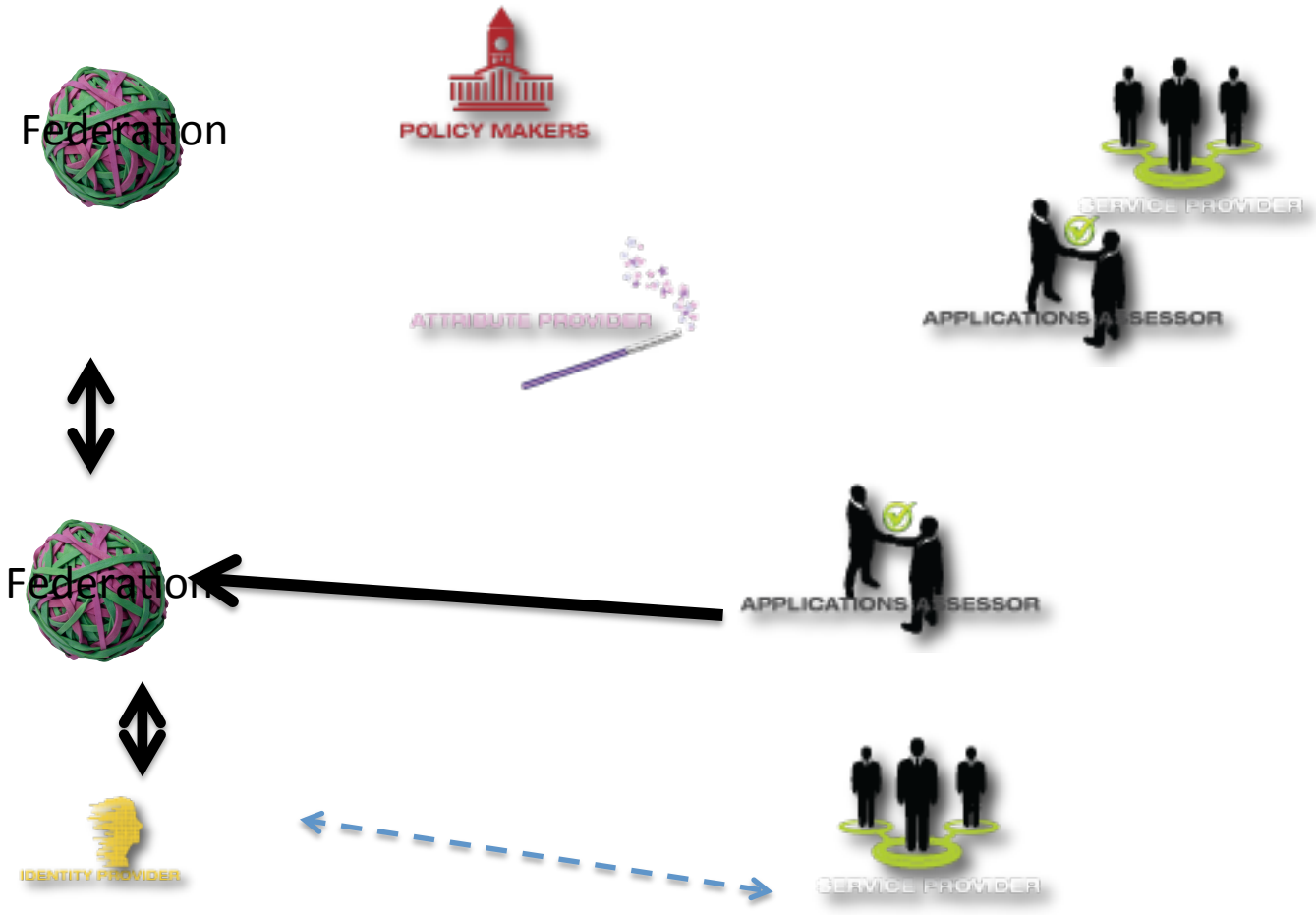
Anonymous Credential “Classic”



Anonymous Credential from AA to IdP and then on to Apps (Federated anonymous credentials)



Associated metaflow



Representative Capacity Scenario

- Occurs, in flavors, in many use cases
  - Government interactions
  - COPPA
  - Age-related disabilities
- Management of underage consent,
- Management may be one time, per transaction, per relying party category, etc.

Next steps

- Refine elements
- Construct a few more sample flows and metaflows
- Start to name arrows in flows by payloads
- Start to identify protocols/processes for flows
- Start to identify gaps

Next call Discussion Topics

- Downstream use, DRM on metadata, etc.
- Revisiting Kim's Laws of Identity with an attribute-centric perspective
- LOA of attributes
  - What does it mean?
  - What does it depend on?
- What are the needs for revocation?
- Is "Minimal disclosure for a constrained use" the goal and if so, does it have a usable interface?

Flow Icon Sheet

Federation

Representative/Gu