OTTO Overview

Open Trust Taxonomy for Federation Operators

Colin Wallis
Executive Director, Kantara Initiative

February 21, 2017

Kantara OTTO Working Group leads

- Michael Schwartz, co-chair
- Janusz Ulanowski, co-chair

- Working Group members include some from the R & E communities

What is a federation?

- ‘Collaboration between autonomous entities where they use a central authority for efficiency’ .. practical definition
  - Examples: EU, USA states, vertical industries (e.g. defence), InCommon – 600 IDPS, 300 SPs, large private enterprises (e.g. Boeing), large public agencies (US DHS etc)

  - Identity federations typically do the following:
    - Vet members (are you a university?)
    - Normalize legal (one participant) Agreements
    - Establish standard security policies and procedures
    - Define schema e.g. EduPerson
    - Publish keys (trust model!)

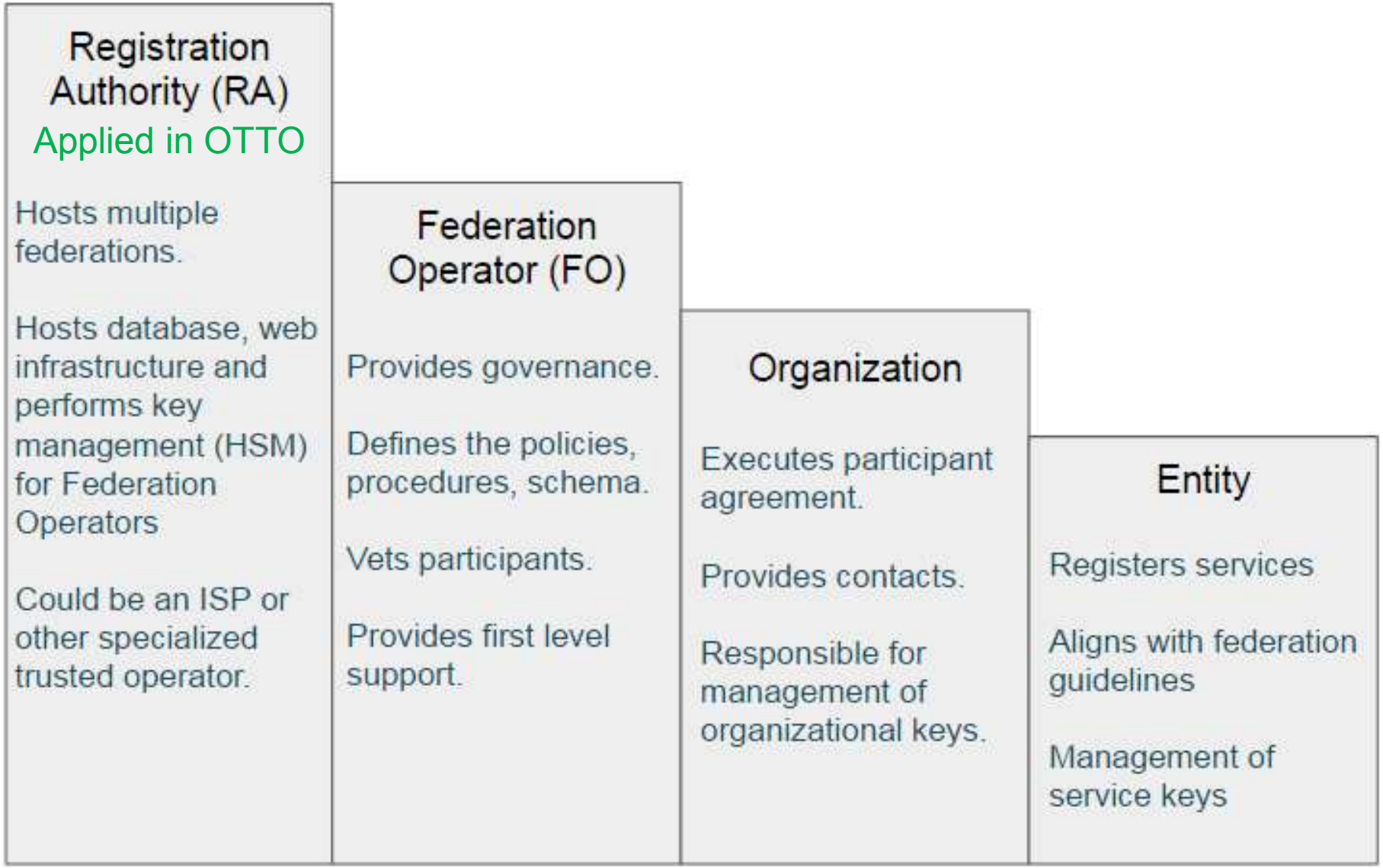
Design Goals for OTTO

- Next generation federation standard for Oauth2
  - SAML federations like InCommon were first
  - But what about OpenID Connect and UMA?

- Use Cases
  - New entities for Oauth2
    - OpenID Connect OP / RP
    - UMA AS / RS / Client
  - Better search / query
  - Less duplication of data
  - More developer friendly (JSON)

- OTTO designed for medium sized federations

Overview of actor roles in federations



The JSON-LD data model's role in OTTO

- Linked Data model convenient for describing federation inter-relationships.
- Uses standard schema described in https://schema.org where possible; extend common schema at Kantara; provides for further extension by RA's or FO's.
- Can be converted to RDF and processed by standard tools.
- Developer friends—looks like JSON, and linked data features can be ignored by those who don't care.
- See https://www.w3.org/TR/json-ld/#basic-concepts

API's

- Endpoints
  - Federation
  - Federation entity
  - Organization
  - Discovery / Configuration

In essence, OTTO offers Schema + API for federation

Test Implementation

- Server was written to demonstrate feasibility
  - MongoDB was used as the backend—loose schema
  - Performance was tested with 10,000 entries
    - Query and filter features seem to scale
  - MIT license

OTTO vs OpenID Connect federation draft

- Complementary – ‘better together’
  - OIDC spec doesn’t say:
    - How organizations register
    - How federation metadata is distributed
    - How key metadata is updated (i.e. revocation)
  - OIDC spec puts a big burden of key management onto the organizations
    - OTTO federations could provide a kind of centralized solution
    - OTTO fills in some assumptions/gaps that FOs would have to fill otherwise.
    - (It tells the FO ‘what to do’ but not ‘how’.

http://openid.net/specs/openid-connect-federation-1_0.html

What still needs doing to make OTTO a reality?

- Need to finalize JSON-LD schema (test and validate them)
  - Organizations
  - SAML, OpenID, UMA Entities (OIDC has been done first)
  - Trustmarks – define policy standards and procedures according to GTRI schema https://trustmark.gtri.gatech.edu/team/
  - User schema (i.e. eduperson)
  - Authentication: ACR / AMR
- Need to convert technical spec to English with good examples
  - Need writers!
- Kantara / Rutgers / DHS ‘ERASMUS’ pilot will use OTTO— a real world test. (ERASMUS: Emergency Responder Authentication System for Mobile Users)

Links

- Join the WG: http://www.gluu.co/join-otto
- Github Project: https://github.com/KantaraInitiative/wg-otto
- Test code: https://github.com/GluuFederation/otto-node
- Swagger UI for test code: http://otto-test.gluu.org/swagger/
- OTTO test data generator: http://otto-test.gluu.org:8080/

Invent. Innovate. Innovate.

Colin Wallis, Executive Director Kantara Initiative:
colin@kantarainitiative.org
+44 7490 266 778