RISC Association Bootstrap Scenarios

OpenID RISC WG Call

Aug 8, 2017

Introduction

- Subscription process: RISC decides to share events about a subject based on discovering a common interest based on user actions:
  - Implicitly Federated
    - By providing an email, telephone# or other as part of account creation at a web application provider (WP)
  - Explicitly Federated
    - The user explicitly logs into an identity provider (SAML or OIDC) in order to create or log into a remote web application (WP)

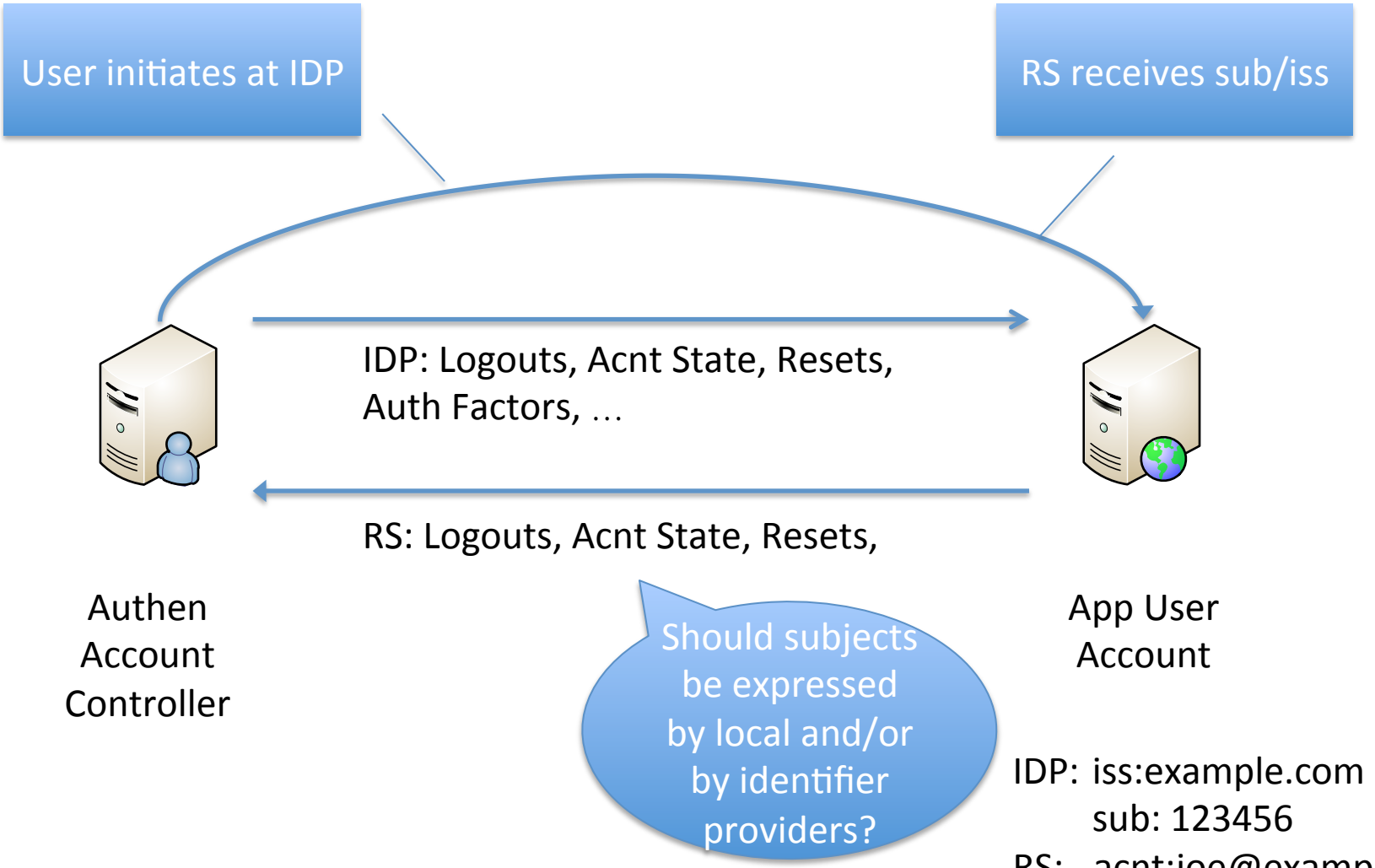
Observations

- User Accounts and Identifiers
  - How the user is known at the WP and the IDP may be different
  - An identifier may be associated with either the IDP or the WP or both
  - A web provider may establish multiple federated relationships (explicit and implicit) for a single user account (e.g. login with email, twitter, or facebook)

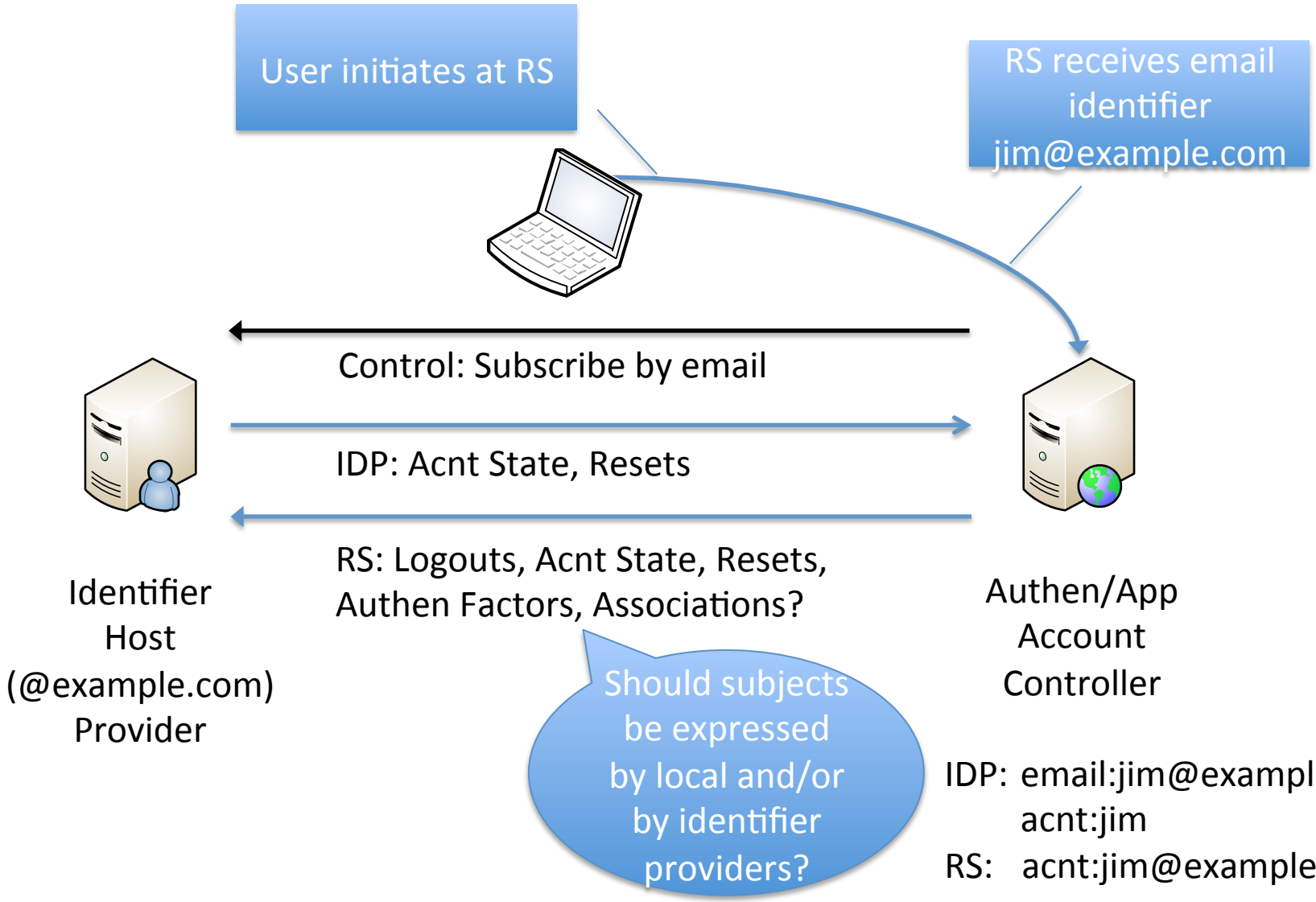
Questions

- How should parties identifier users to each other?
  - Should the WP remember the IDP identifier and use it for events issued to the IDP?
  - Should the IDP use its own identifier when issuing events to one or more WPs?
  - Are Implicit cases different from Explicit cases?
- Should multiple subject identifiers be used?
- How to express subjects
  - dictionary/composites, multi-value, multi-type?

Explicit "Connect" Case



Implicit "Email" Case



Other Questions

- Should events ever express multiple subject identifiers?
  - Complicates PII leakage
  - How much effort should issuers make to use receiver's identifier for a user?
- What if provider has multiple identifier services?
  - e.g. OIDC, Email Host, Telecom Services
  - Provider MAY have centralized security for user but should RS's know this?