# UMA and OpenID Connect optimization opportunities

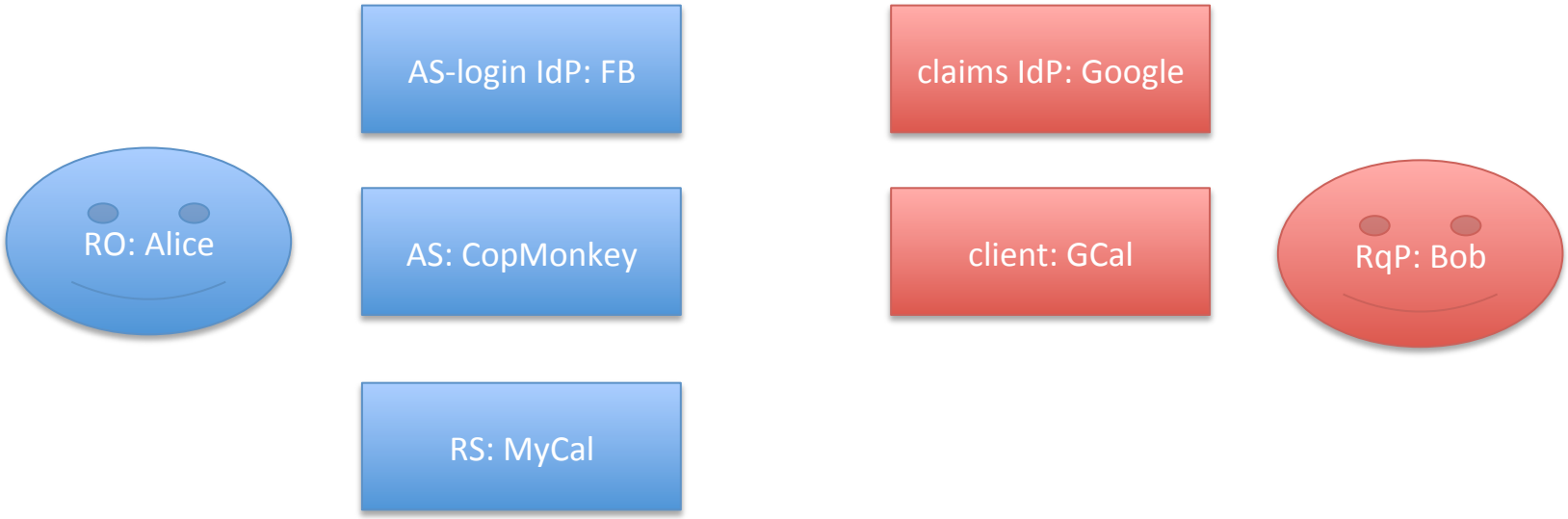
May 2013

IIW 16

# Goals

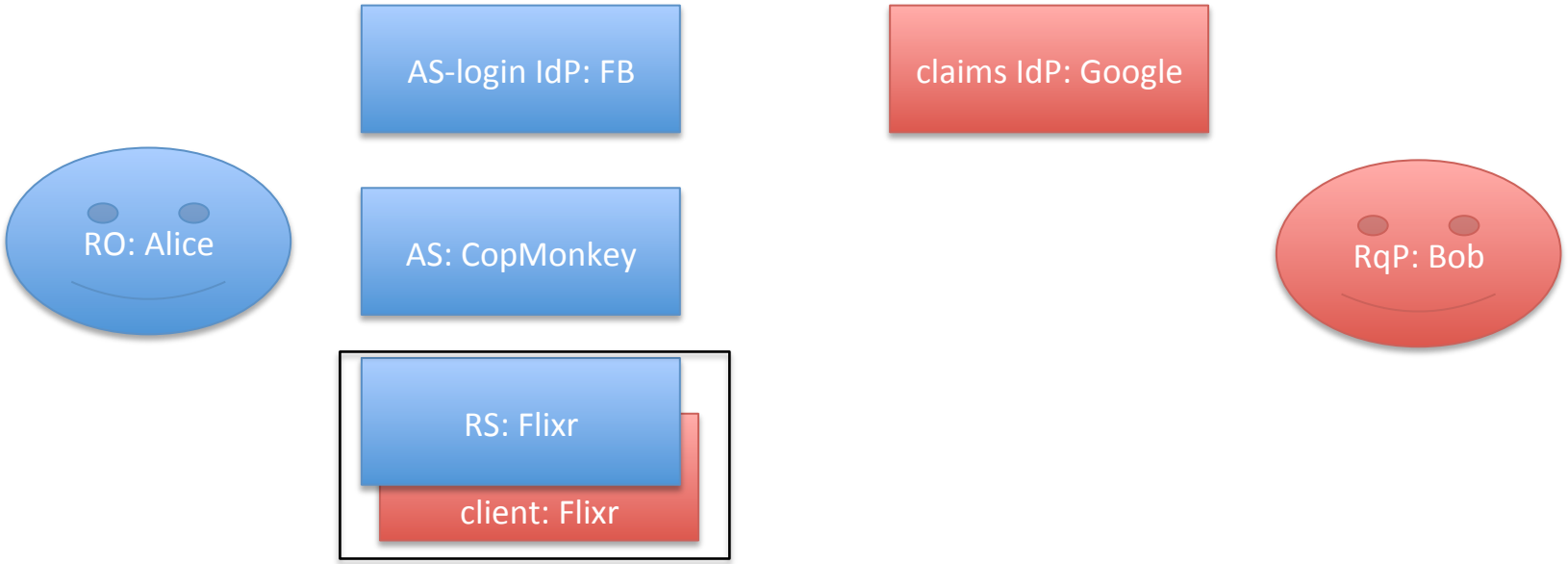
- Identify highest-priority optimization opportunities (OOs) with both UMA and OpenID Connect in the picture
- Identify candidate UMA flow revisions that make sense to solve them
  - Possibly through profiling or simple extension
  - If necessary, through backwards-incompatible changes
- Head towards UMA Implementor's Draft once this is done
- The following scenarios highlight candidate OOs

# 0. “Worst case”: UMA-protected person-to-person resource sharing



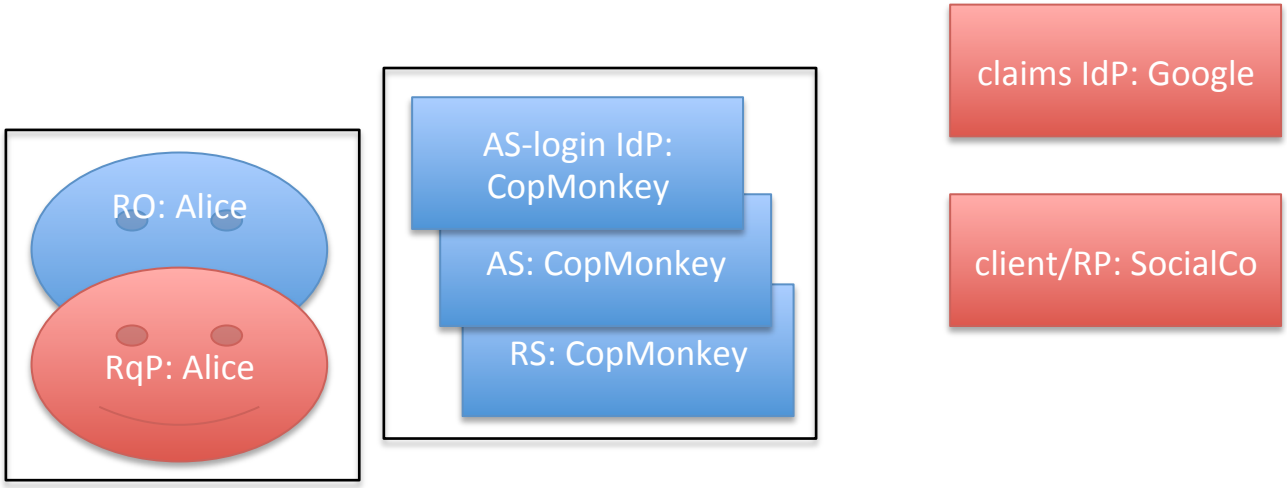

- Scenario: CopMonkey protects Alice’s calendar at MyCal. Bob can use GCal to view her calendar if Alice’s policy says so.
- Simplifying assumptions: None.
- Initiation: Bob/GCal attempts to access calendar directly at MyCal.
- *(Candidate variant of less interest: AS-login IdP = AS, meaning that Alice has a local login at CopMonkey vs. a federated one. This probably applies to most of the following scenarios too.)*

# 1. “Same app”: Person-to-person sharing within same resource server



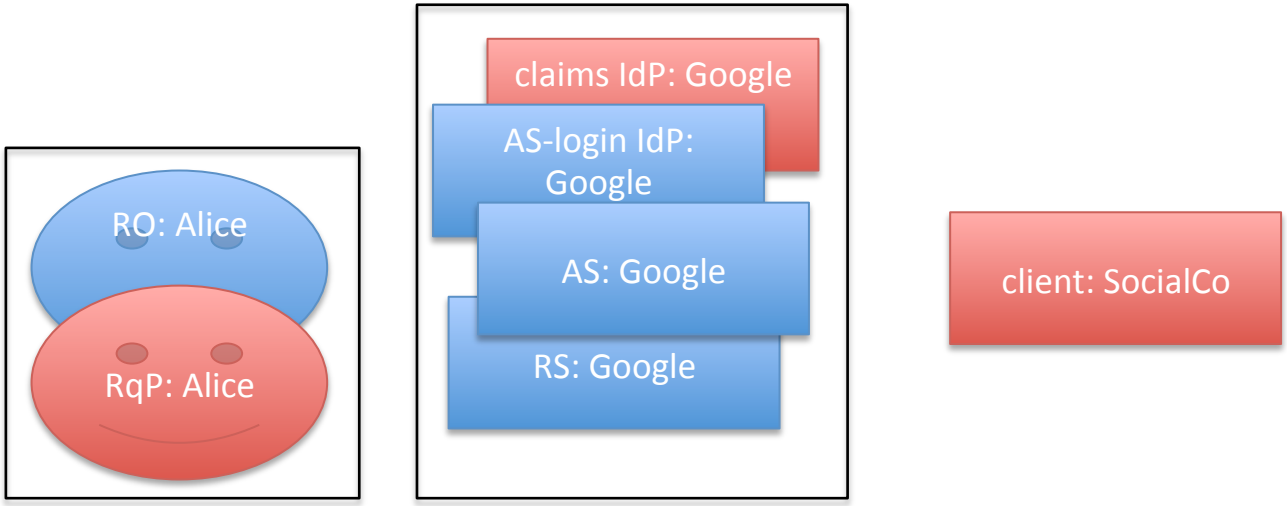

- Scenario: CopMonkey protects Alice’s photo albums at Flixr. Bob, also a Flixr user, can use it to view some album if Alice’s policy says so.
- Simplifying assumptions: RS = C.
- Initiation: While logged in to Flixr, Bob attempts to access Alice’s album.
- *Comments: Twitter etc. could also use for controlling multi-person access to the same “account”.*

# 2. “UMAfied claim transfer”: OIC login and UMA-protected attribute sharing



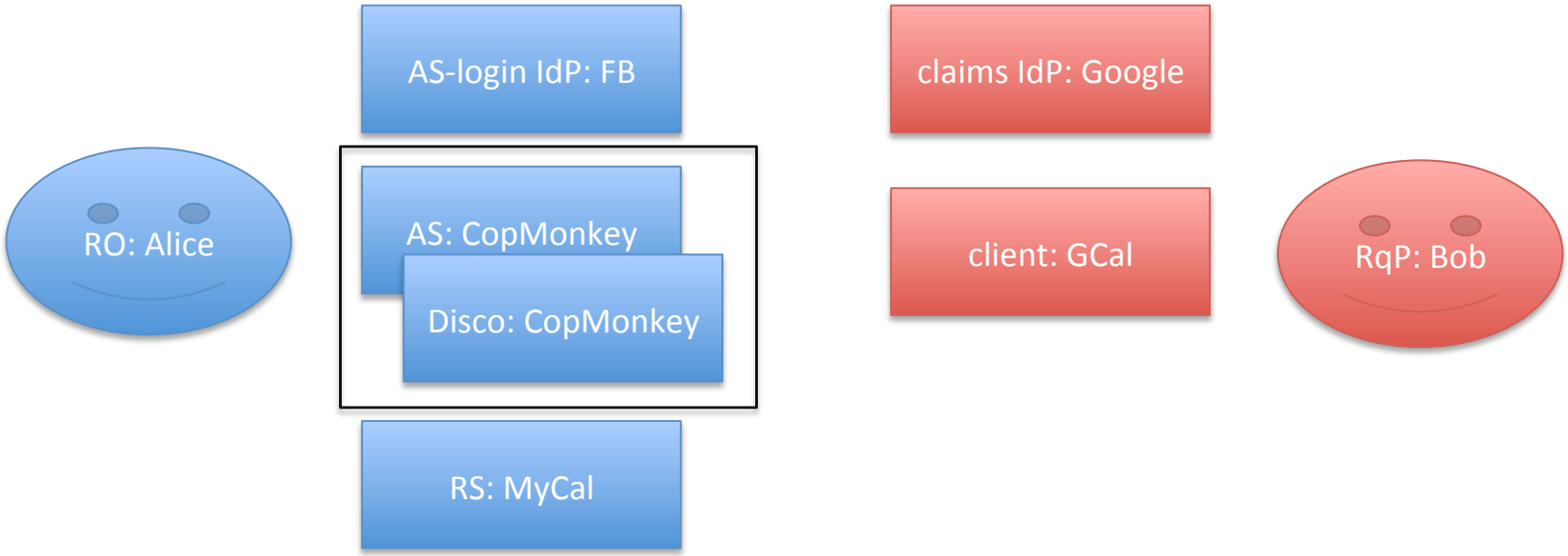

- Scenario: Alice wants to log in to SocialCo using her IdP, CopMonkey. SocialCo requires her time zone, which CopMonkey stores and also controls access to. Her policy says “Only alice@gmail can release this claim,” which CopMonkey sources from Google as a claims IdP.
- Assumptions: RO = RqP; AS-login IdP = AS = RS.
- Initiation: Alice registers at SocialCo by logging in to CopMonkey (as IdP); as AS, it requires her to log in to Google and release her email claim to satisfy her own policy.
- *Question: Does she also routinely log in to SocialCo the same way, or does she have longer-lasting permissions than this?*

# 3. “Simple UMAfied claim transfer”: same as #2 with common IdP




- Scenario: Same as #3, but this time, Google is the same IdP/AS/etc. all around.
- Assumptions: RO = RqP; AS-login IdP = AS = RS = claims IdP.
- Initiation: Alice registers at SocialCo by logging in to Google (as IdP); as AS, it requires her to (log in to Google and) release her email claim to satisfy her own policy.
- *Question: Can claims transfer be done automatically?*

# 4. “Personal discovery”: Bob finds Alice’s calendar’s location to access it




- Scenario: CopMonkey protects Alice’s calendar at MyCal. Bob doesn’t know where Alice’s calendar is but knows her Disco service, where he can ask for its location and to get access rights.
- Simplifying assumptions: AS = Disco. (***NEW component***). RS registered enough info at AS/Disco for the latter to enable “personal discovery”.
- Initiation: Bob/GCal makes a query of CopMonkey (as Disco).
- *(Question: Does this look like Bob/Gcal making a normal resource access attempt? What does it look like? What does he get back?)*