requester_delegate_scenario

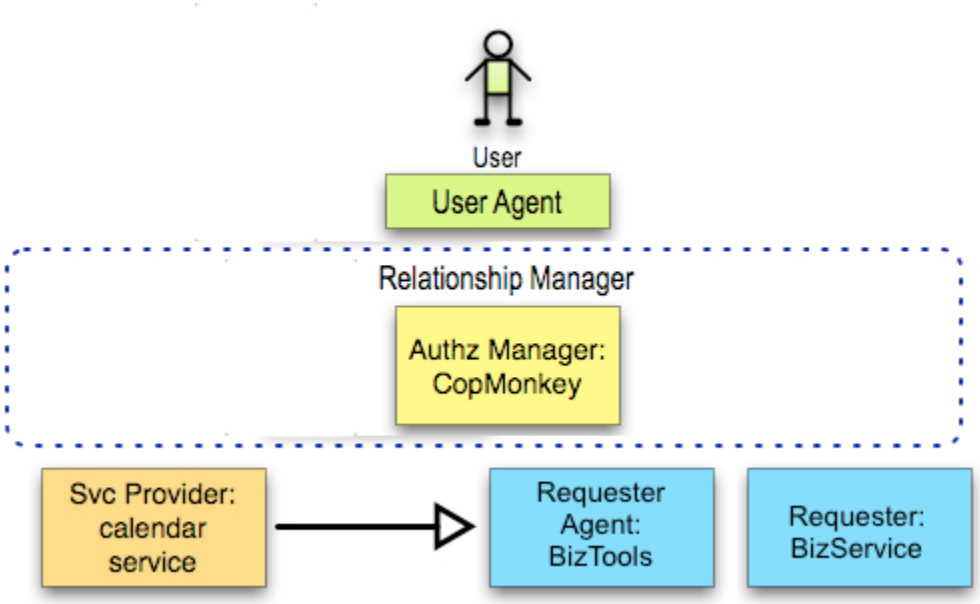
Scenario: Requester Delegate (Accepted)

Submitted by: Michael Hanson

The Requester may be using a hosted service, which may need to make requests on its behalf.

The user has entered a relationship with BizService, and wants to authorize it to access her calendar. BizService is using a website hosted by BizTools, which is the entity that will initiate all network activity and actually hold the tokens generated during the transaction.

The user should be able to authorize BizService to access her data, without granting any privileges specifically to BizTools, and without granting privileges to any other company hosted by BizTools.



Issues:

- Does the user need to be aware of BizTools, or can she grant authorization to BizService in a way that allows BizService to relay access?
- Does this scenario require an explicit model of delegation enforced by the AM, so that BizService can't hand off an access token to anybody they want?

Use Case: BizTools Impersonates BizService (Accepted)

Today, app-hosting relationships commonly involve sharing of private keys (covered by service-level agreements), and concomitant "impersonation" of the company by the outsourced service. This use case would seem to be transparent to the user (for example, if the user is given a real-time opportunity to consent to access when BizTools/BizService attempts it, the request will appear to come from BizService) and to the UMA protocol.

Use Case: BizTools Provides Its Own Network Endpoint (Rejected)

If BizTools approaches the resource not by impersonating BizService but in its own right (on BizService's behalf), true delegation would somehow have to come into the protocol picture. The goal would be to avoid creating an "omnipotent token" that allows the proximate Requester (BizTools) to use the token for access on the behalf of other parties. As discussed on 2009-10-08, we are inclined to reject this use case.