User Federation Best Practice for the Real Estate Industry

Version 1.0
June 19, 2018

Synopsis

Having a collection of best practices for User Federation will improve interoperability between systems and applications.

Rationale

With the increased use of Single Sign On in the real estate community, the need for end users to be able to federate their identity from one organization to an identity issued by a second organization has grown. An example of this is an agent logging into their broker's intranet site as user "Alice" and then wanting to seamless move to her MLS website where she is known as user "97236". Another example is logging into one of the REALTOR.org sites using her NRDS ID and then wanting to move to the broker's site. In all cases, user Alice has an identity and is the same person. She simply wants to use technology to link her accounts.

One way to accomplish this is for the various Relying Parties (Service Providers) to support integration with multiple Identity Providers at the same time. Alice's broker intranet could support both its own IdP and also support the MLS systems IdP. This multiple IdP support is not widespread in the real estate vertical.

Best Practice Method for User Federation

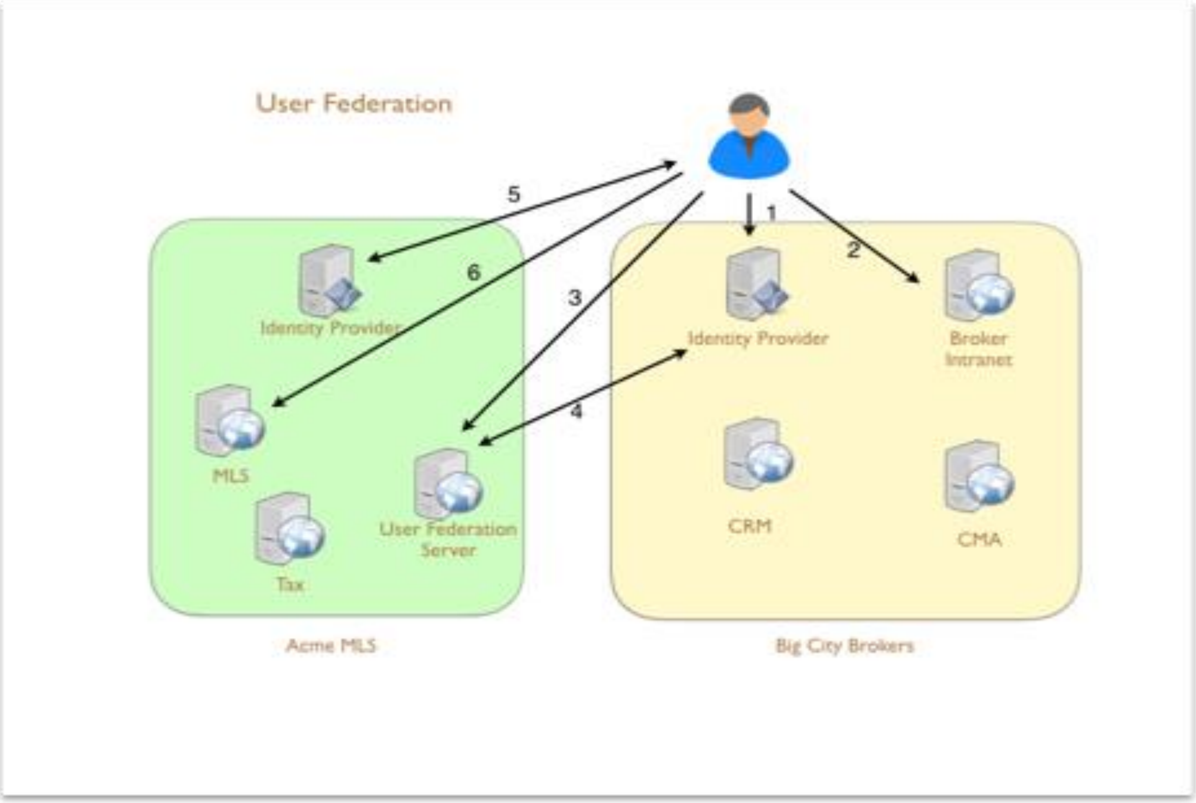
This best practice method offers a solution which does not require defining any new protocols, only mutual agreement on a process for federation. Additionally, the best practices method can work with both SAML and OpenID Connect protocols. The key component of this idea is a Relying Party Proxy (RPP). The function of the RPP is to authenticate the user with the remote Identity Provider and then proxy that to the user's identity in its local system. Here's an example flow illustrated by the diagram:

- Alice starts her day, new browser, no sessions (arrow 1)
- Alice logs into Big City Real Estate, her brokers intranet, as user "alice" (arrow 2)
- Alice then clicks on a link to go to her MLS at acmemls.com
- That link goes to the Acme RPP server (arrow 3)
- The Acme RPP notes it does not have a session with the browser but knows the request came from Big City Real Estate (via the destination on acmemls.com and/or query parameters)
- The Acme RPP issues an authentication request to the Big City IdP (arrow 4)
- The Big City Real Estate IdP recognizes Alice's browser session and issues an SSO response to acmemls.com
- The Acme RPP now knows user "alice" is authenticated and asks Alice to login to her Acme account so they can be federated (arrow 5)
- Alice provides her Acme credentials and the Acme RPP links the accounts
- The Acme RPP then asserts her identity to the MLS (arrow 6)

So the federation of the identities happened inside of the RPP. All external transactions between the organizations happened using standard SSO protocols (SAML or OIDC). The RPP at each organization can set their own policies regarding how long the federation is good for. So it could require a local re-authentication every 10 visits or once a month or whatever the business requirements dictated.

The RPP is really a hybrid of an Identity Provider and Relying Party bridging an external identity to an internal one. But how it does that is all behind the curtain of the organization it represents. Each organization wishing to support user federation would simply build their own RPP and agree to mutual federation policies with cooperating organizations.

This is different from a Relying Party supporting multiple IdPs. In this proposal, a Relying Party only has to talk to a single IdP. The RPP handles creating the SSO session that crosses over the organizational boundary. The user benefits from seamless access to all RPs in both organizations with a single login.



Best Practices Key Points

- No new protocols are defined
- Any mutually agreed SSO protocol may be used
- Requirements for authentication remain within each organization

- Each organization sets their own business requirements for maintaining the federation
- Federation can be bi-directional or uni-directional
- Each organization defines their implementation in an opaque manner to others

Authors

The Best Practices Method for User Federation was formulated and refined by:

- Paul Hethmon (CoreLogic) – Author
- Paul Stusiak (Falcon Technologies) – Editor
- Greg Moore (Regional Multiple Listing Service of Portland) - Editor
- Jeremy Crawford (RESO) – Editor
- *With the input of members of the RESO Research & Development Workgroup and the RESO Transport Web API Workgroup*