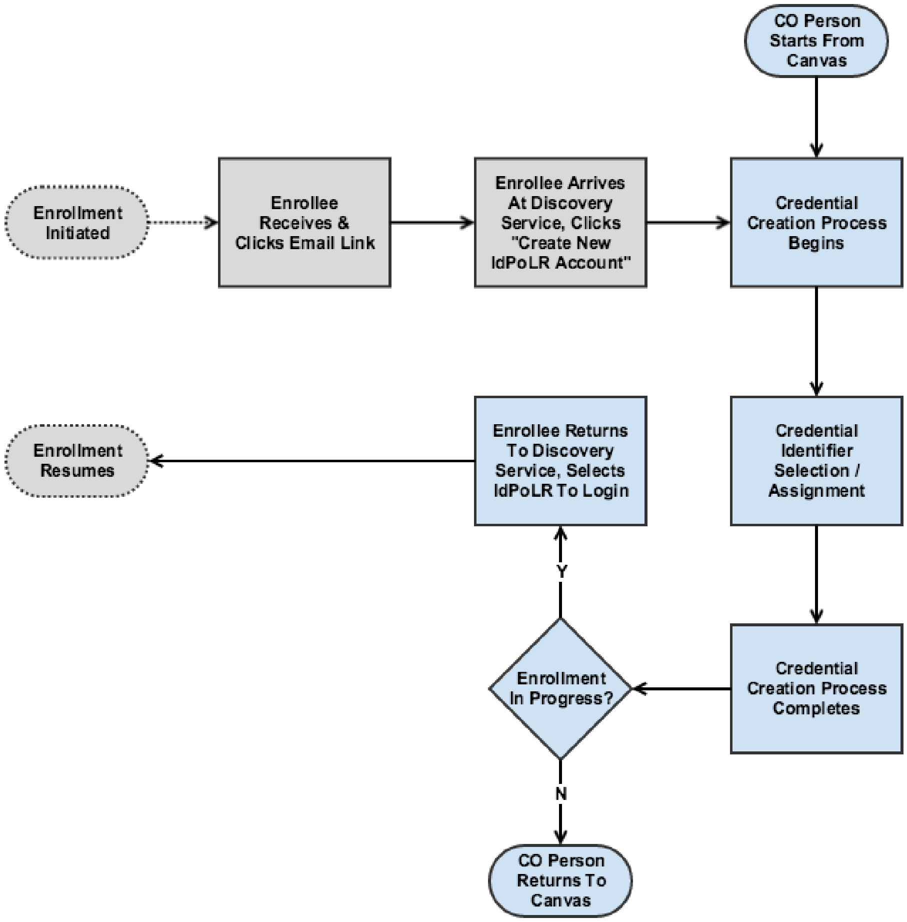
IdP of Last Resort Enrollment Integration

A new Credential Management capability (CO-1256) will be central to the support of IdP of Last Resort capabilities (CO-44). This document describes the interaction between Registry Enrollment and IdPoLR credentialing.


CO Person Starts From Canvas
Enrollment Initiated
Enrollee Receives & Clicks Email Link
Enrollee Arrives At Discovery Service, Clicks "Create New IdPoLR Account"
Credential Creation Process Begins
Enrollment Resumes
Enrollee Returns To Discovery Service, Selects IdPoLR To Login
Credential Identifier Selection / Assignment
Y
Enrollment In Progress?
Credential Creation Process Completes
N
CO Person Returns To Canvas

Discussion Notes

1. The credentialing process will be CO specific, but the Discovery Service is currently CMP-wide. This will not be suitable for most multi-tenant deployments.
2. The actual credentialing process will likely vary according to the requirements of each type of credential plugin.
3. Because the Enrollee will not have authenticated yet, they will enter the credentialing process without a valid login session. Use of a token (similar to enrollment flow tokens for unauthenticated steps, or possibly the same token) will be required.
4. Credential Identifier Selection could be any of
    a. User self selected (with availability checks)
    b. Auto assigned via identifier assignment (but at credentialing step, rather than at CO Person Active status)
    c. Selected by credential plugin
5. Is it possible to skip the discovery service when the Enrollee is returned to the Enrollment Flow?
    a. Yes, though details depend on the protocol involved.
    b. For both SAML and OIDC, redirect the browser to a particular URL