Org Identity Enrollment Refactoring Design Discussion

Background

Organizational Identities are intended to record representations of identities created outside Registry, such as those from Identity Providers or Systems of Records. However, in the early days of COmanage, pulling these identities from outside sources was challenging, and so early on the ability to manually create Organizational Identities via Enrollment Flows was added. In retrospect, this was probably a mistake.

Over time, additional complexities have been introduced. Organizational Identity Sources were developed, along with Pipelines. Enrollment Sources were added as a means to tie Org Identity Sources to Enrollment Flows. EnvSource was developed as a more robust means to collect external identities (vs querying $REMOTE_USER when the magic Enrollment Flow configuration is enabled).

Additional background information is available in C-4 Scoping: Reorganizing Organizational Identities, which also describes the desired overall end state.

Issues For Discussion

1. Review Registry Enrollment Flow Diagram for functionality that needs to be refactored.
    a. Can we more cleanly describe "Petitioner" vs "Enrollee" phases, eg to better distinguish *Petitioner Enrollment Authorization* from *Require Enrollee Authentication*?
2. Automatically update configurations? Or just provide recommendations?
3. Migrate "legacy" records from old style enrollment flows?
4. Ensure full provisioning of Org Identity identifiers (and maybe other attributes) to LDAP or other provisioners
5. Pipeline relation to Enrollment Flows, including Sync Policy or Data Filters for setting status on CO Person created via Pipelines (CO-2021)
6. See also: CO Person enrollment without an Org Identity (CO-870)
7. Related Discussion: Syncing Authenticators (SSH Keys, Certificates) from Org Identity Sources to CO Person Records, possibly via Pipeline Plugins (CO-1382), and maybe Authenticators also implementing the Pipeline Plugin interface
8. Related Discussion: Restarting Enrollment for interrupted petitions (see also CO-1657, CO-431)
    a. ie: leverage petition tokens to reenter an enrollment flow
9. Related Discussion: Consent: where in the flow does it happen under which scenarios?

Notes For Enrollment Flow Changes

1. CO Person Record gets created (by the form) before Org Identity
    a. Implies petitioner attributes is required
2. Move "Require Authentication" out from under "Verify Email"
    a. Self Signup flow should not require email verification, though it may still be desired
3. Env Source only runs in *Identify* mode, ie: after email confirmation step
    a. CO Person is already known, so no match strategy needed
    b. This should work for Self Signup, Invitation, and Identity Linking
4. Need to reconsider if Duplicate Check step needs to be moved/refactored
5. Populating default values from ENV requires environment variable support (ie: mod_auth_shib/oidc, but not SimpleSamlPHP). Ultimately this could move to some plugin based solution, depending on requirements.
6. Email Address validation would happen *before* EnvSource steps runs, which means only the CO Person form address could be validated. See also CO-757.

Backlog Planning

See also JIRA issues identified in C-4 Scoping: Reorganizing Organizational Identities.

Registry v4.0.0 (1H21)

- Overriding "Read Only" Org Identity Source data (not funded)
    - Shadow Org Identities (CO-1635)
    - But also what happens if the Org Identity Source Key changes?
        - eg: EnvSource uses eptid to construct the OIS Key, but then the IdP changes the eptid for the user
        - Maybe allow limited ability to force a new Key (CO-2026)
- CO Person Record gets created (by the form) before Org Identity
- Env Source only runs in *Identify* mode, ie: after email confirmation step
    - See also: update self-signup enrollment template for EnvSource (CO-1638)
- Enrollment Source Invitation Single Org Identity (CO-1578)
- Some sort of transitional document to explain how to set up a new flow that works like the old flow used to - note deprecations
    - Initial document at Migrating to EnvSource, will need to evolve

Registry v5.0.0 (Transitional release to prepare for Framework Migration)

- Enrollment Sources Do Not Trigger Dupe Check (CO-1577)
    - Need to reconsider if Duplicate Check step needs to be moved/refactored
- EnvSource based account link does not work when the new login method is from the same source (CO-1636)
- Old style flows will break as of v5.0.0, in preparation for PE transition (CO-1545)

    - Remove the code that copies $REMOTE_USER to the Org Identity, etc
    - Remove CMP Enrollment Attributes

Registry v6.0.0 (Registry PE)

- Move "Require Authentication" out from under "Verify Email" (CO-757)