Integration Strategy 1 - Application Service uses only "CommIT" credentials, does not require local credentials

The Story:

Integration Strategy 1

Integration Strategy 1 only uses CommIT accounts. This strategy is for those participants who have no desire to maintain local credential registries for authentication, and will instead rely on CommIT to handle their authentication requirements. Participants will still maintain and Identity Provider, but this IdP will contain the locally useful 'enriched' attributes about a user that their business model requires.

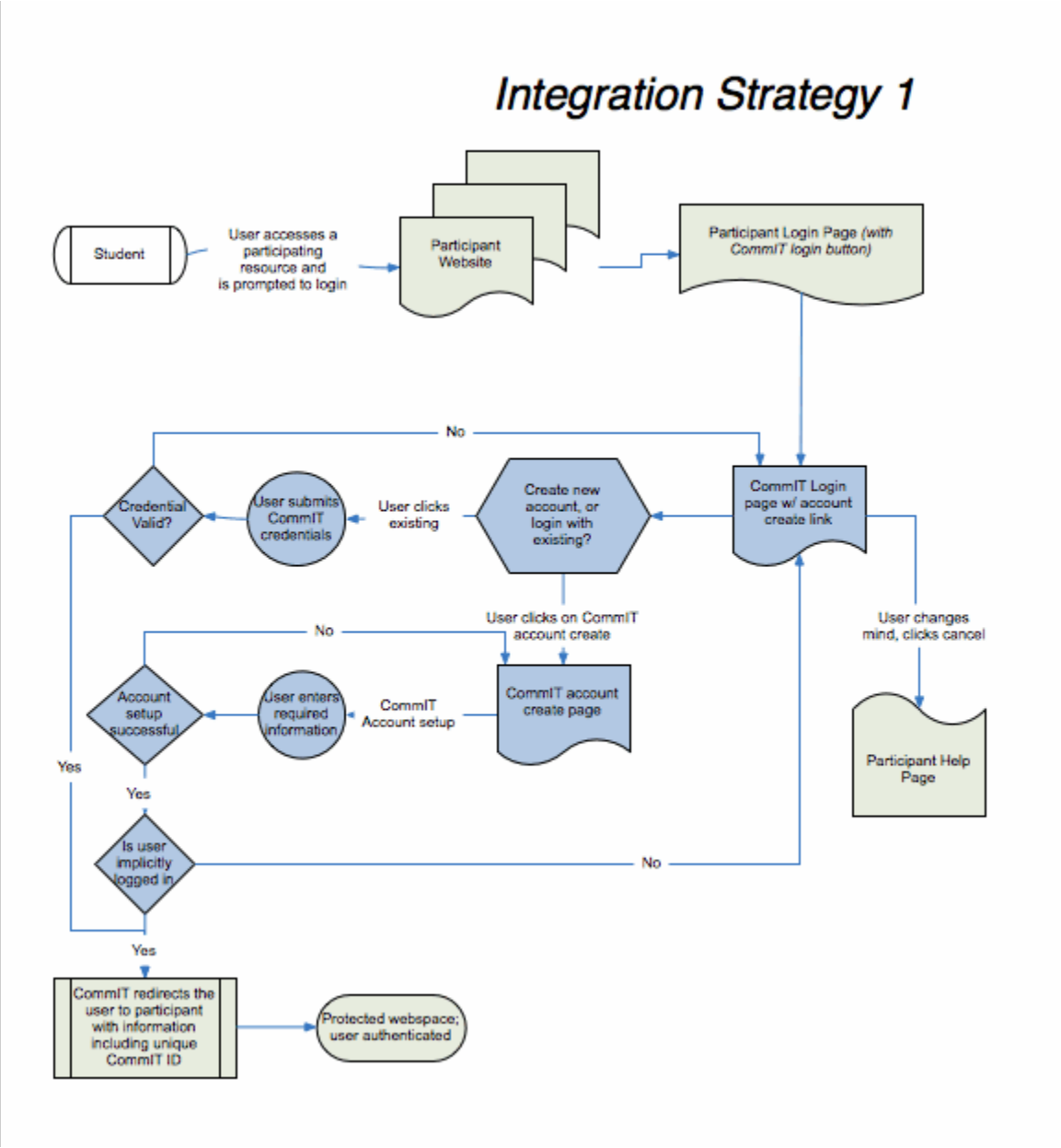
Successful CommIT Account Creation at Participant site

Annie Applicant wants to use an application service. The application service requires a CommIT account for authentication. She has never created a CommIT account anywhere else. She may or may not have local participant accounts elsewhere. She is given the option of logging in with her CommIT credentials or creating CommIT credentials. Since she does not believe she has CommIT credentials, she chooses to create an CommIT account, and clicks on the "new account" button. She is redirected to the CommIT IdP to create her account. She provides her name and other optional attributes about herself to CommIT, which are used only internally by CommIT for password reset and records matching to reduce duplicates. CommIT sends back an assertion that includes information about how the authentication occurred and her unique identifier. At the application service she enters additional information about herself to be stored at the participant's IdP.

Failed CommIT Account Creation at Participant site because Applicant forgot about existing account.

Annie Applicant wants to use an application service. The application service requires an CommIT account for authentication. She has created an CommIT account, but has forgotten it exists. She may or may not have local participant accounts elsewhere. She is given the option of logging in with her CommIT credentials or creating CommIT credentials. Since she does not believe she has CommIT credentials, she chooses to create an CommIT account, and clicks on the "new account" button. She is redirected to the CommIT IdP to create her account. She provides her name and other optional attributes about herself, and CommIT sends back a list of potential accounts that might be her. If she recognizes one of the accounts, she logs in using that account and continues to the application service.

Diagram depicting the combined registration flows described:



CommIT Login to Participant site

Annie Applicant wants to use an application service. The application service requires a CommIT account for authentication. Annie recognizes that she has a CommIT account, and clicks on log in button. She's directed back to the CommIT IdP to authenticate. After successfully authenticating, CommIT sends back an assertion that includes information about how the authentication occurred and her unique identifier. If Annie's attributes are already stored at the application service, they are loaded into a local representation of Annie. If Annie has never been to this application service, a local representation of Annie is created by prompting Annie for attributes which are stored locally and keyed to her unique identifier.