Integration Strategy 2 - Local Authentication Included

Integration Strategy 2

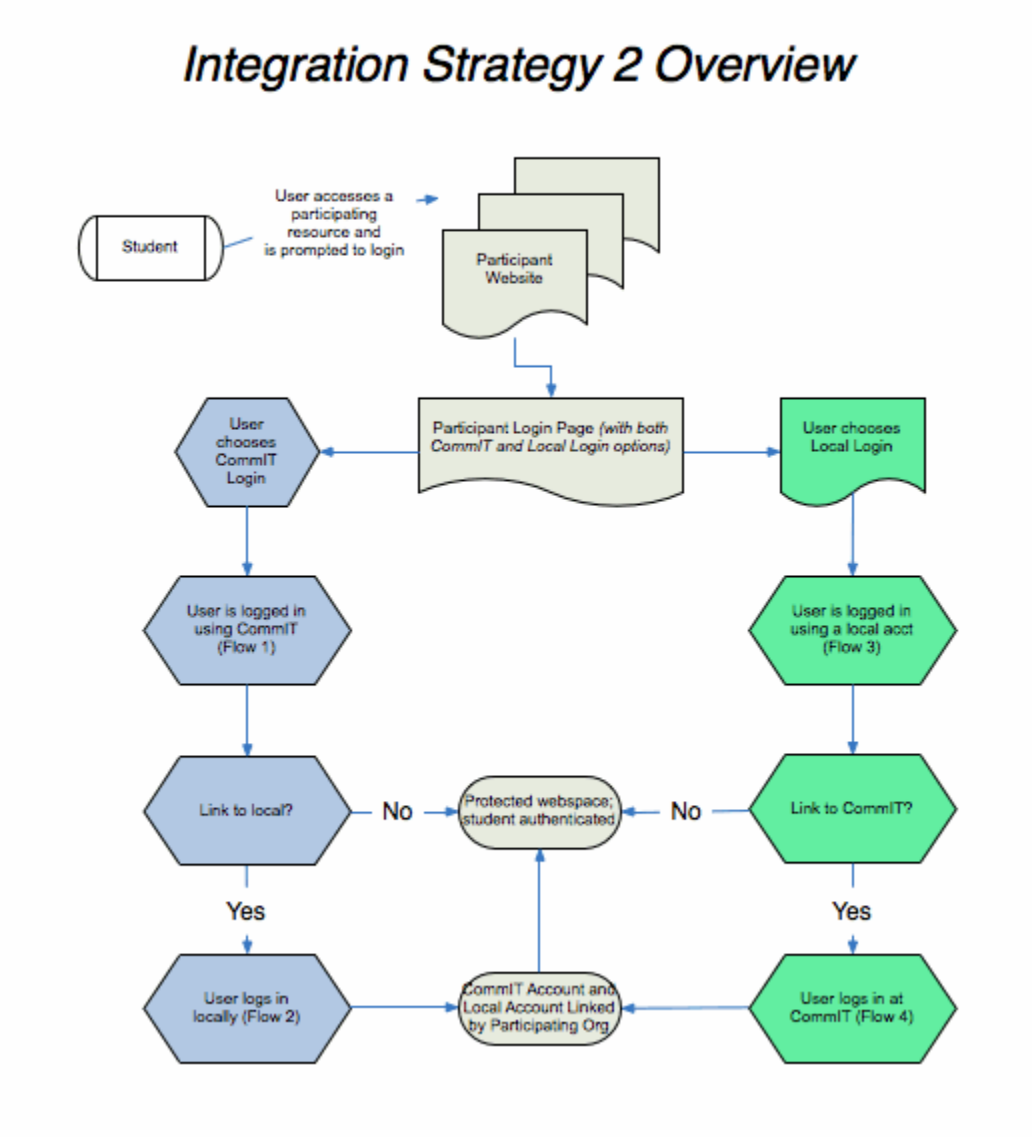
Integration Strategy 2 allows for the use of local accounts alongside CommIT Collaborative accounts. This may be done as a permanent integration approach, or it may be useful as a transition mechanism towards an end state of Integration Strategy 1, where only CommIT accounts are used at a given service.

There are countless ways to thread together local accounts and CommIT accounts into an identity fabric. This integration strategy strikes a balance between accommodating as many different deployer needs as possible and presenting a cohesive, understandable login experience to the user. As such, it is a guide and a harmonization point for an anticipated variety of deployer approaches, intended to encourage interoperability and a consistent, learnable user experience. It is not a complete description of everything that is possible.

Deployers are encouraged to think critically about these flows and the needs of their implementation. Some user interactions or options can be reasonably excerpted by an implementer if they are not appropriate for the scenario. Others may be added. Some flows might not be implemented at all if they create an end state that is undesirable to the integrator.

The following scenarios each describe a hypothetical user transaction that involves:
1. Primary authentication of the user with a CommIT account;
2. Subsequent association of a CommIT account with a local account;
3. Primary authentication of the user with a local account;
4. Subsequent association of a local account with a CommIT account.

Each scenario has a matching story that demonstrates how the flow might be used. There are separate flow diagrams to depict modes of the integrated system, but they compose into a single, unified decision tree. The flow as depicted begins when the user attempts to access a protected service at a participating organization, although it could be invoked at various points on various sites. The flow ends when the user is able to access the desired secured content, or with display of appropriate error and help information when the user is unable to access the resource.



Other flows, such as the aggregation of attributes about a principal from all participants in the CommIT ecosystem at the end stage of the application process, are out of scope for this document, which addresses only authentication.

Actors Involved in These Scenarios

1. **Student**: The user of the service.

2. **Participating Service**: It could be a Service Organization (Ex. Collegeboard, ACT, FAFSA etc) or an Application Service Organization (Aggregation portal, school system etc). A user may have local account with this organization. The diagrams may refer to the participant service as "Participant" for brevity.

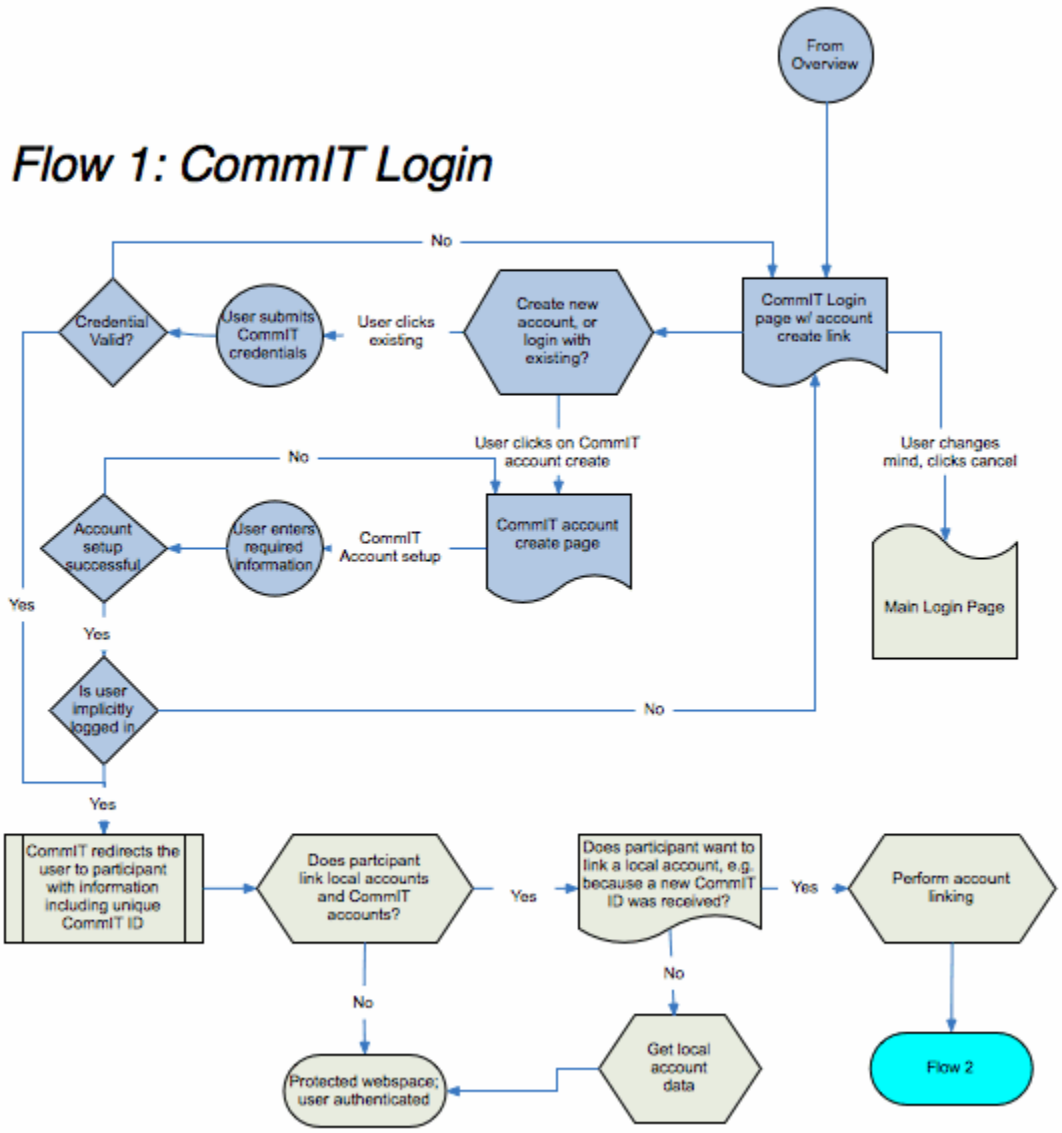
3. **CommIT Identity Provider**: The central CommIT identity provider supporting account creation and management, unique identifier creation and management, authentication, and issuance of user information to affiliated services.

1. CommIT Login

Annie Applicant wants to use an application service. The application service permits both login with an application service credential (also known as local account), or login with a CommIT account. Annie doesn't have a local account yet, and there's an explanation on the page that tells her about all the benefits of using CommIT instead of a local account. She chooses to click on the CommIT button and she creates a new CommIT account. Following account creation, she's directed back to the CommIT IdP to authenticate. After successfully authenticating, CommIT sends back an assertion describing the authentication, the verification level associated with her account, her CommIT identifier, and optionally a set of attributes. The application service optionally creates or loads a local representation of Annie keyed by her "CommIT" identifier which is used to store additional local data about her.

The next time Annie returns to the service, she chooses to login with CommIT. Since she already has an account, she clicks the CommIT button. After successfully authenticating, "ommIT sends back an assertion describing the authentication, the verification level associated with her account, her CommIT identifier, and optionally a set of attributes. The application service optionally loads the local representation of Annie.

Start State: A user wants to access a service using a CommIT account.
1. The user may or may not have a local account.
2. The user may or may not have a CommIT account.
3. The user may be accessing the participating service's website via her CommIT account for the first time.



Successful End State: The user has successfully authenticated to and accessed the participating service's website using her CommIT account.
1. The user now certainly has a CommIT account.
2. The user still may or may not have local account.
3. The user has successfully accessed the participating service's website.
4. The participating service has received the user's unique CommIT identifier.

****

2. CommIT Login to Local Account Creation or Association

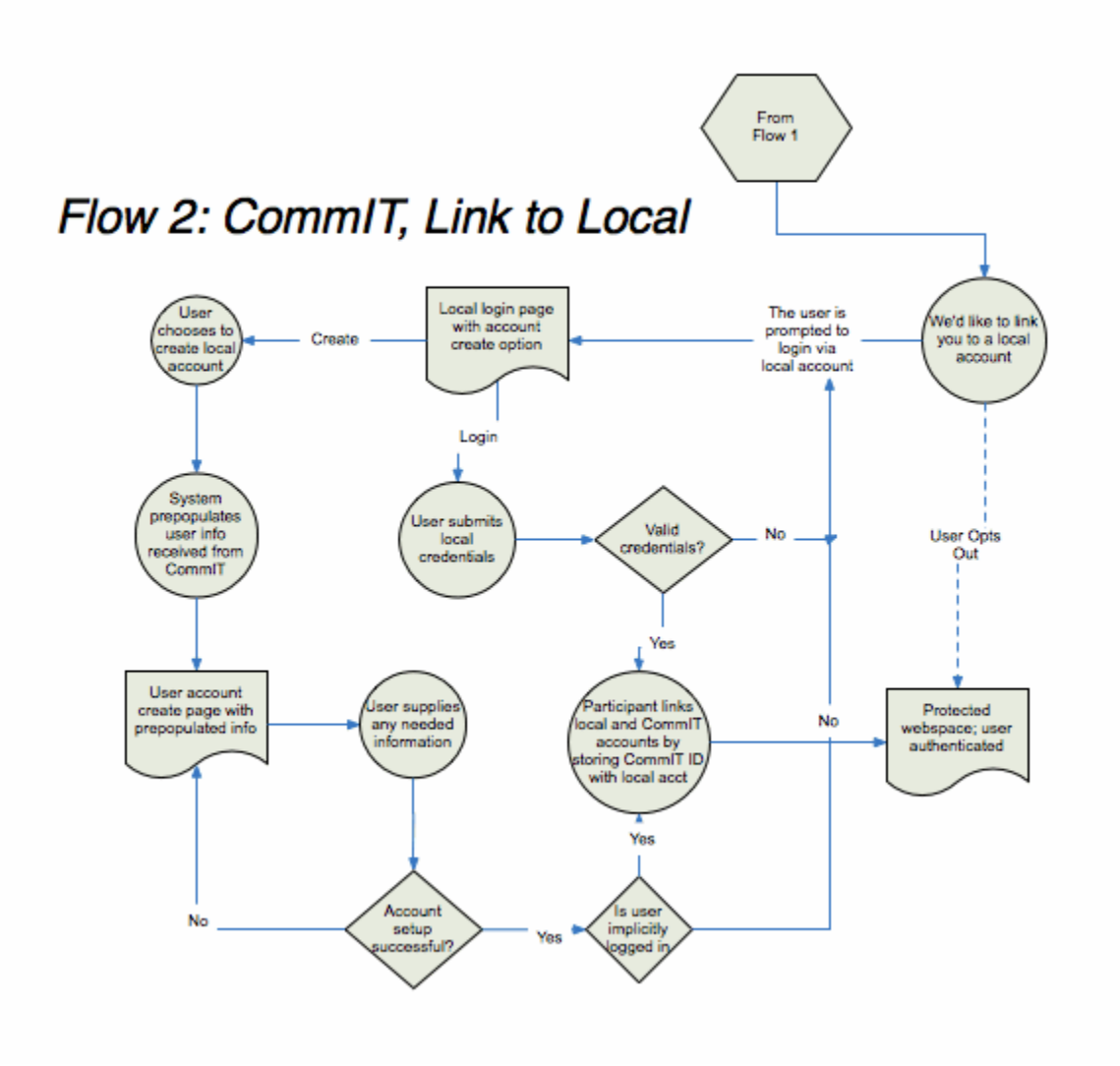
Arnie Applicant wants to login to a standardized testing service. The testing service offers to let him login with a local account, or to use a CommIT account. Arnie doesn't have a local account, but Arnie recognizes that he has a CommIT account, and clicks on that button. He's directed back to the CommIT IdP to authenticate. After successfully authenticating, CommIT sends back an assertion describing the authentication, the verification level associated with his account, his CommIT identifier, and optionally a set of attributes.

The testing service checks to see whether it recognizes the CommIT identifier. If it recognized the identifier, it would already have an associated local account. However, it doesn't recognize the identifier. The testing service prompts Arnie to either login with his existing testing service account so that it can be associated with his CommIT account, or to create a new testing service account. He does so and accesses the service.

Next time Arnie comes back to the testing service, he chooses to authenticate with his local testing service account. He is prompted for authentication by the testing service. His unique CommIT identifier is still associated with his local account, and he is granted access to the service.

Start State: A user has successfully authenticated to and accessed the participating service's website using her CommIT account. The participating service requires, for its own reasons, a local account that can be linked with the CommIT account.

1. The user may or may not have a local account.
2. The user certainly has a CommIT account.
3. The user may be accessing the participating service's website via his CommIT account for the first time.



Successful End State: The user has successfully authenticated to the participating service using principally a CommIT account and associated a local account with a CommIT identifier.

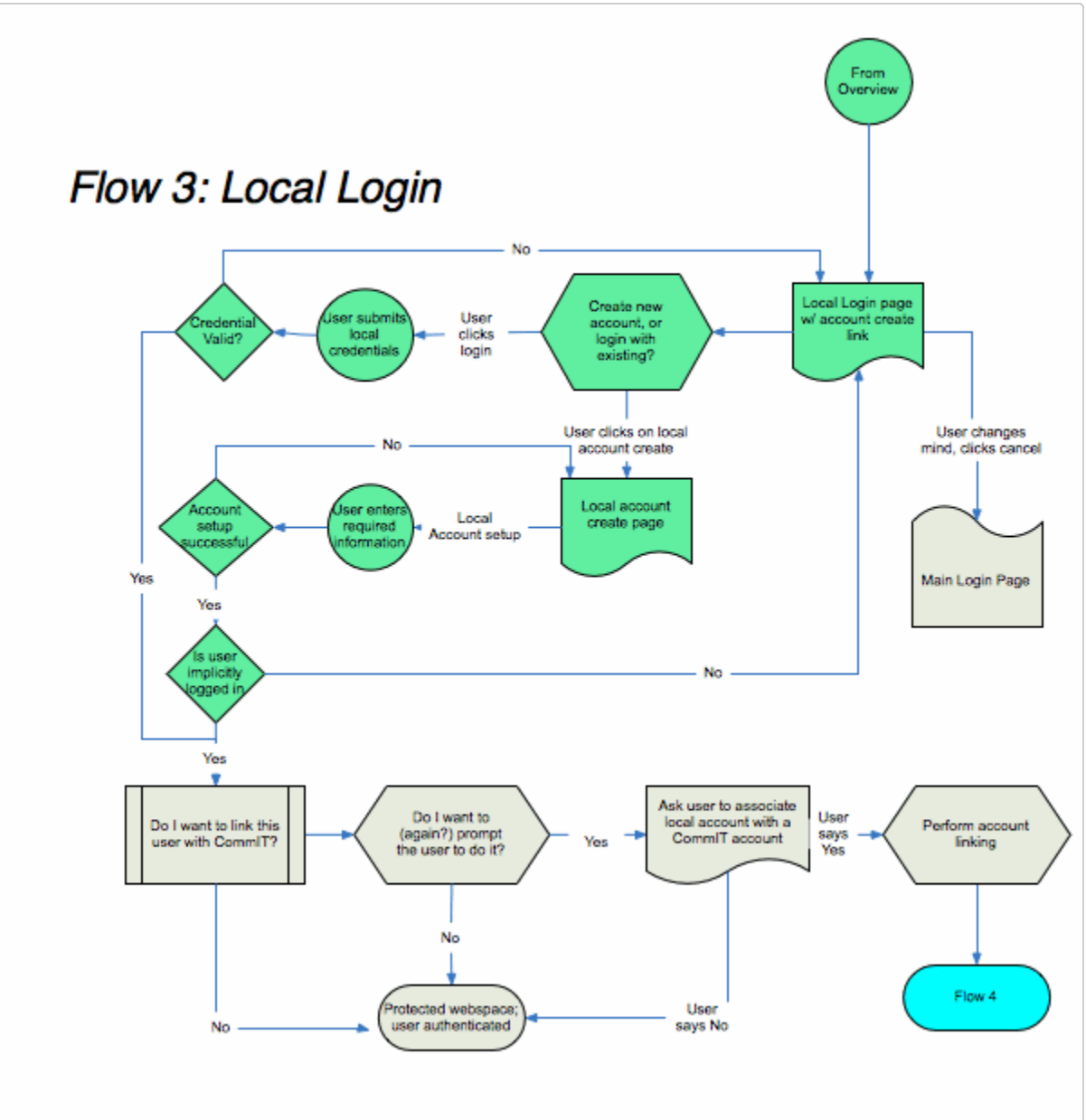
1. The user certainly has a local account.
2. The user certainly (still) has a CommIT account.
3. The participating service obtains a linkage between the CommIT identifier and a local account.

****

3. Local Account Login

Arnie Applicant wants to login to an application service. The testing service offers to let him login with a local account, or to use an CommIT account. Arnie just wants access to the application; he is not interested in using or learning more about CommIT. He clicks the local login button. After successfully creating a new local account or authenticating with an existing local account, Arnie is granted access to the application.

Start State: A user wants to access a protected service using a local account.
1. The user may or may not have a local account.
2. The user may or may not have a CommIT account.



Successful End State: The user has successfully authenticated to and accessed the participating service's website using a local account.
1. The user now certainly has a local account.
2. The user may or may not have a CommIT account.
3. The user has successfully accessed the participating service's website.

****

4. Local Account Login to CommIT Account Creation or Association

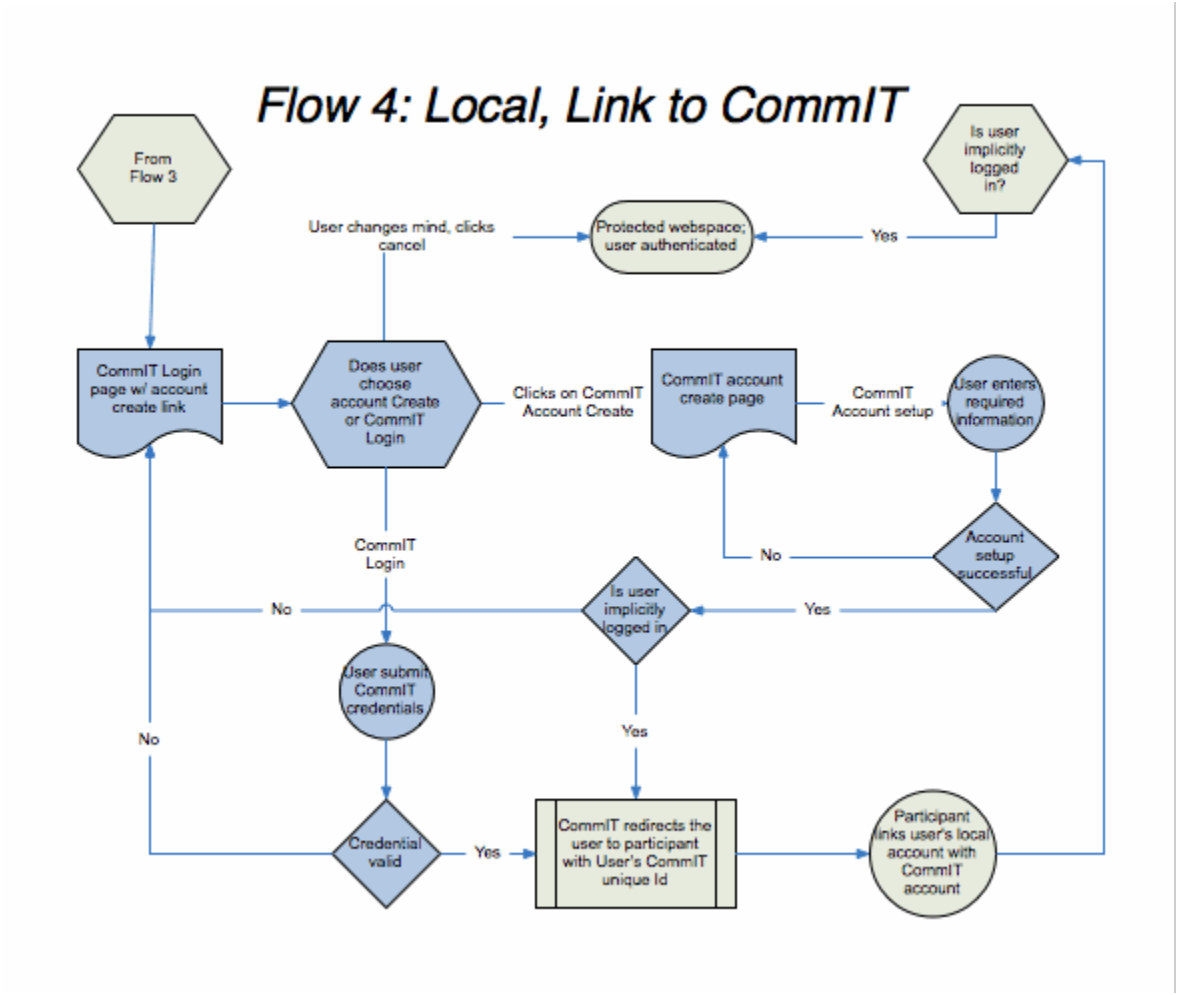
Annie Applicant wants to login to a standardized testing service. The testing service offers to let her login with a local account, or to use a CommIT account. Annie knows that she has a local account with the testing service that she created when she took the standardized test, and clicks on that button. She's directed to the local testing service IdP to authenticate.

After successfully authenticating, the testing service prompts her to create a CommIT account, or to link her testing service account to her existing CommIT account, explaining to her the benefits of doing so. She might also have the option of proceeding without creating an CommIT account.

Annie is convinced, and she clicks to be redirected back to the CommIT IdP. CommIT asks her to either authenticate if she has an existing account, or to create a new account. She either creates an account or uses an existing account. After successfully authenticating, CommIT sends back an assertion describing the authentication, the verification level associated with her account, her CommIT identifier, and optionally a set of attributes. The testing service receives the assertion and associates the unique CommIT identifier with her local account. It then grants her access to the service.

The next time Annie comes back to the testing service, she chooses to authenticate with her CommIT account. She is redirected back to the CommIT IdP. After successfully authenticating, CommIT sends back an assertion describing the authentication, the verification level associated with her account, her CommIT identifier, and optionally a set of attributes. The testing service associates the CommIT identifier with the local account keyed by her CommIT identifier and grants her access to the application.

Start State: A user wants to associate a local account with a CommIT account.
1. The user certainly has a local account.
2. The user may or may not have a CommIT account.
3. The user may be accessing the participating service's website via her CommIT account for the first time.



Successful End State: The user has successfully authenticated to the participating service using principally a local account with an associated CommIT account and identifier.

1. The user certainly (still) has a local account.
2. The user certainly has a CommIT account.
3. The participating service obtains a linkage between the CommIT identifier and a local account.

****

Wireframe UI for This Integration Strategy:

(tbd)