Shibboleth Functional Requirements Document

http://datascience.iq.harvard.edu/blog/try-out-single-sign-shibboleth-40-beta provides a high-level view of the initial Shibboleth support that was shipped with Beta 7, which is more or less the "First Time User Log In" user story described below. This document is an attempt to clarify the complete set of functional requirements for Dataverse 4.0. The "Not in Scope" section at the end covers features that are planned for future releases.

Mockups

https://iqssharvard.mybalsamiq.com/projects/updatedloginwithshibbolethii-dataverse40/grid

First Time User Log In: GONE THROUGH QA

Dataverse users should be able to...

- Click "Log In" to see if their institution is listed or not. If their institution is not listed and they think it should be, they should be able to get further instructions on who to contact to get their institution listed.
- Select their institution and click "Continue".
- Arrive at their institution's login page and attempt to log in.
- Given successful login to their institution's login page (and receipt on the Dataverse side of required Shibboleth attributes), read "Terms of Use" (consistent with builtin accounts per https://github.com/IQSS/dataverse/issues/972) and either click "Accept Terms" or "Cancel"

Institutional Identity Updates: DONE

On successful login with one's institution...

- The first and last name should be updated in Dataverse.
- The email address should be updated in Dataverse.
- The name of institution provided by the Identity Provider updated in "affiliation" in Dataverse: https://github.com/IQSS/dataverse/issues/1497

Log out

- Clicking "Log Out" is not enough for Shibboleth users. After clicking "Log Out", they will be presented with a popup with an OK button saying that they must close their browsers to finish logging out. As an alternative, perhaps we could have a short timeout (10 minutes or fewer) configured between the Dataverse SP and each of the Identity Provider (IdP).

Conversion from Migrated Builtin Account to Shibboleth

https://github.com/IQSS/dataverse/issues/796
https://github.com/IQSS/dataverse/issues/1387

~~Users who have builtin accounts that have been migrated from DVN 3.x should be able to...~~

- ~~Convert their local account to a Shibboleth account~~

When a Shibboleth user logs in for the first time and a matching email address is found in the system, they will be shown the matching username, prompted for their "builtin" password, and given the choice between cancelling or agreeing to the account conversion and terms of use. They won't be prompted to pick a "useridentifier".

If no matching email address is found, a new Shibboleth account will be created (after they agree to terms of use). We recognize that this could lead to duplicate accounts when the email address in Dataverse differs from the email address that is provided by the institution's identity provider.

Shibboleth groups

Users with the "superuser" boolean set to "true" should be able to...

- Create institution-wide Shibboleth groups: https://github.com/IQSS/dataverse/issues/1401

Shibboleth configuration and management

People who install Dataverse should be able to...

- Read documentation to know what software to install and how to configure Apache.
- Enable Shibboleth login, which is off by default. (At the moment this is accomplished with `curl -X PUT -d yes http://localhost:8080/api/s/settings/:ShibEnabled`)
- Configure the attribute to use as a unique identifier for users (i.e. "eppn", could be a list). https://github.com/IQSS/dataverse/issues/1422
- Edit an XML file to add or remove institutions from a list.

Dealing with Identity Provider Quirks

- For example, Eleni has two "givenName" attributes: Eleni and Elleni

Not in Scope/Deferred

- Disambiguation of users with the same name ("all users should have a username").
- On first Shib login, prompting users for a username/password to convert a builtin account when no matching email address was found.
- Storing the "position" received from Shibboleth (e.g. "staff;student"). See https://github.com/IQSS/dataverse/issues/1444#issuecomment-74134694
- Conversion from Shibboleth Account to Builtin Account
- Automatically add a shib group when a user from a new institution first logs in https://github.com/IQSS/dataverse/issues/1403
- Future: Create Shibboleth groups that are defined by regular expressions that match incoming Shibboleth attributes. https://github.com/IQSS/dataverse/issues/1515

High-level summary of Shibboleth Features that Shipped with Dataverse 4.0

Dataverse 4.0 shipped with support for the following Shibboleth features:

- Multiple Identity Providers (#794)
- Institution-wide Shibboleth groups (#1401)
- Automatic population of users' affiliation in their profiles (#1497)
- Conversion of "builtin" accounts to Shibboleth accounts (#796)