Doc notes

Shibboleth Authorization setup and coding

Our app acts as a Shibboleth service provider (sp) and talks to a Shibboleth identity provider (idp) server to authenticate the user. All communication to the identity provider is handled via the user’s browser by using redirects.

Steps:

Configure settings in Yii App config file config/main.php:

// the next two set up the type of user authentication we are using

'useShibboleth'=>**true**, // true if using shibboleth authentication

'useLocalLogin'=>**true**, // true if using local authentication

// the entity id for this app as registered with the Shibboleth //identity provider (authentication server):

'idName'=>'base.phpfogapp.com/baseapp',

// the xml tag used by the identity provider to identify the

//users email address which is where we get their cuzId:

'userEmailTag'=>'urn:oid:1.3.6.1.4.1.5923.1.1.1.6',

// the url our app uses to access the Shibboleth identity provider:

// We get this from the identity providers xml metadata file.

// (provided by Jeffrey Crawford

'idProviderUrl'=>'https://test-idp.ucsc.edu:444/idp/profile/SAML2/Redirect/SSO',

// this is the public key x509 certificate for th eidentity provider

// so we can validate their response.

// We get this from the identiy providers xml metadata file. 'idpPubCert'=><<<CERTIFICATE

We generate the xml metadata that describes our app as a service provider by calling the app with the parameters: ‘?r=login/metadata’. For example: <http://base.phpfogapp.com/baseapp/index.php?r=login/metadata>

We provide the service provider (sp) metadata to Jeffrey Crawford. He sets us up account for our app in Shibboleth identity provider (idp). The only essential item we provide is our entity ID (app name.) We could use the same account for multiple apps if we have them use the same entity Id.

We are currently using the identity provider at 'https://test-idp.ucsc.edu:444/idp/profile/SAML2/Redirect/SSO'

Note for our code we need to use the idp url that ends in/SAML2/Redirect/SSO there are other urls with other bindings for the same identity provider but those are not configured correctly for our code.

Our code picks the cruzId of the logged on user from the xml sent by the identity provider. Our code is dependent on the xml format and tagging of the response from the identity provider. If updates to the identity provider change this then we will have to update our code. Tag names we are dependent on are placed in a config file for easy access and update.

We use the onelogin php-saml open source library from: <http://support.onelogin.com/entries/268420-saml-toolkit-for-php>