1.2 Configuring Apache Web Server to use Shibboleth

Configuring Apache http-server 2.x

If Shibboleth is installed with yum or apt-get, the Apache module mod_shib will be installed and activated. What you need to do next is to determine how the actual service should be protected:

1. If the entire site should be protected by shibboleth, or
2. is there only a part (path) of the site that need to be protected by shibboleth, while the rest should be accessible without IdP login. In the example below we are protecting the relative path /myprotectedSP:

In your <VirtualHost> you add a <Location> tag for what you want to protect (found in /etc/httpd/conf.d/shib.conf):

```
<Location /myprotectedSP>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
  Require valid-user
</Location>
```

If the entire site should be protected, you write `<Location /> instead of "<Location /myprotectedSP>"`

Handling logins by the Service/Application protected by Shibboleth

The login information from the Identity Provider (user name and other attributes that comes with the assertion) are set as HTTP environment variables by the Apache module. If the Service/Application only wants to know that the user successfully logged in, nothing special has to be done. Shibboleth and mod_shib takes care of that before handling the user over to the Service/Application. If the Service/Application needs to have the attributes sent by the Identity Provider, it needs to be able to read the HTTP environment variables produced by mod_shib.

HTTP environment or HTTP headers

Some Services/Applications can't read HTTP environment variables out of the box, e.g. applications written in php. But those applications can read HTTP headers. You can tell Apache that it should deliver the attributes as HTTP headers (it is done in the configuration file /etc/httpd/conf.d/shib.conf):

```
ShibUseHeaders On
```