Sakai Authentication

March 2005 Version 1.1

Please direct questions or comments about this document to:
Glenn R. Golden, ggolden@umich.edu

Authentication is a Sakai kernel service that has the responsibility of authenticating end users. A package of "evidence" is collected that represents information provided by the end user. This is validated against the authentication "database". A valid authentication produces an end user id (UUID) to be considered the authorized end user.

Authentication API is implemented by one of many different components. Authentication is likely to be tied into a Sakai integrator's enterprise systems, so we expect many different forms of Authentication components for Sakai.

There are also going to be many forms of Authentication evidence. This will often take the form of a user identification and a password. Another form of evidence will be the "remote user" from a web server that is participating with a container based single-sign-on system, which we have chosen to trust for our authentication. Evidence can also take the form of a public certificate, a thumbprint, or any other sort of information that is used to authentication a user.

Authentication is a lonely API. There are going to be very few clients of the API.

The Authentication API is defined in the Sakai `kernel` module, in the `authentication` project.