Data Portal Version 3

Authentication and Authorization Web Service

Author: **Michael Doherty**

Doc version: **0.1**

Date: **March 2003**

1. DESCRIPTION

The Authentication and Authorization web service is the primary security mechanism in the CCLRC Data Portal. Any user or outside service must first authenticate themselves with this service. A username and pass phrase must be provided to retrieve a Globus Security Infrastructure (GSI) certificate from a MyProxy server. The advantage of this method is that once the user has loaded a certificate into the MyProxy server, the Data Portal can retrieve a proxy certificate and act on their behalf. The user can therefore use any web browser to invoke the Data Portal, with the knowledge that certificate based security is being used internally. Further to this it negates the requirement for a user to carry around their private key.

2. WEB SERVICES OFFERED

2.1 int login (String userName, String password)

This is the main method of the AuthCtl (Authentication Control) class and is the only method presented as a web service. The userName and password are in fact used to interrogate the MyProxy server and obtain a proxy certificate for the user. The int returned by this method is in fact the Session Id, which is used by the internally by the Data Portal to maintain session state control.

If either of the userName or password details are incorrect, or there is no valid MyProxy account matching these, then a Session Id of –1 is returned to indicate a failure to authenticate.

2.2 Services that use the Authentication and Authorization service

2.2.1 The following services call the Authentication and Authorization service:

- Web Interface uses **login(userName, password)**
- Outside Service use **login(userName, password)**

2.2.2 Services that the Authentication and Authorization service calls

- Calls the MyProxy server to validate a user and obtain a delegate proxy certificate
- Calls the Lookup Service to get the end points for all facilities
- Calls the Access Control Service for each facility in turn per user login
- Calls the Session Manager Service to obtain a session id.

3. INTERNAL METHODS

The main class of this service is AuthCtl. Two other classes are used to access the MyProxy Server: DelegateProxy and PortalProxy. The methods of all these classes are described below:

3.1 public class AuthCtl

3.1.1 public static void getMyConfig()

This method reads the "authent.config" in the WEB-INF directory file and obtains all parameters relevant to this module. These are:

- my_proxy_server_name = The name of the MyProxy Server your system uses
- my_proxy_server_dn = The Distinguished Name of the MyProxy Server
- my_proxy_server_port = The IP Port number of the MyProxy Server
- delegate_proxy_lifetime = The default lifetime of delegated certificates
- portal_cert_filename = The location and name of the Data Portal certificate
- portal_private_key_filename = The location and name of the Data Portal private key file
- ca_cert_filename = The e-Science Certification Authority certificate (who signed the Data Portal certificate).
- uddi_lookup_service = The name of the UDDI server where all Data Portal web services are registered

3.1.2 private X509Certificate idCheck(String userName, String userPassword)

This method is passed the userName and userPassword as supplied to the login method. This method first of all obtains the actual Data Portal proxy certificate from the My Proxy server and then obtains the users proxy certificate, given those supplied.

3.1.3 private String[] lookupFacility()

This method obtains a list of Access Control Service End Points from the Lookup Web Service and stores them into a string array. The lookup service location is specified by

uddi_lookup_service = The name of the UDDI server where all Data Portal web services are registered

This is located in the "authent.conf" file in the WEB-INF directory.

3.1.4 private org.w3c.dom.Element buildAccess(String userName, String[] facilityEndPoints)

This method queries all the end points obtained from the lookupFacility service using the username and password supplied to the Authentication and Authorization web service. It builds up an XML document that merges the access control information that each user has at all facilities. This XML document is eventually passed to the Session Manager.

3.1.5 private int getSessionId(String userName, org.w3c.dom.Element facilityAccess)

This method sends the username and XML document describing access control (see above) to the Session Manager. The Session Manager then returns a valid session id for this user.

3.2 public abstract class PortalProxy

3.2.1 public static GlobusProxy getPortalProxy()

This method calls the createPortalProxy() (see below) with no arguments. It exists purely for exception handling

3.2.2 private static void createPortalProxy()

This method reads the Data Portals server certificate and private key from a file on Data Portals files system and uses these in combination with the Data Portal Private Key pass phrase to create a server proxy certificate for the data portal to use. The Private key location and certificate location are specified by the configuration properties:

- portal_cert_filename = The location and name of the Data Portal certificate
- portal_private_key_filename = The location and name of the Data Portal private key file
- ca_cert_filename = The e-Science Certification Authority certificate (who signed the Data Portal certificate).

These are located in the "authent.conf" file in the WEB-INF directory.

3.3 public abstract class DelegateProxy

3.3.1 public static GlobusProxy getProxy(String aUsername, String aPassPhrase, GlobusProxy thePortalProxy)

This class is passes the username and password originally supplied to the Authentication and Authorization service and contacts the MyProxy Server using the Data Portal GSI certificate. It returns the users proxy certificate, which may then be

used by the Data Portal. The address of the MyProxy server and Data Portal distinguished name are specified by the following parameters:

- my_proxy_server_name = The name of the MyProxy Server your system uses
- my_proxy_server_dn = The Distinguished Name of the MyProxy Server
- my_proxy_server_port = The IP Port number of the MyProxy Server

These are located in the "authent.conf" file in the WEB-INF directory.

3.4 public class Config

3.4.1 public static String getContextPath()

This class obtains the location of the WEB-INF directory on the host system. This is used to locate the "authent.config" file which contains local configuration parameters relevant to this web service.

3.5 Code Walkthrough

The following diagram (Figure 1) shows how each of the above documented methods is used in sequence:

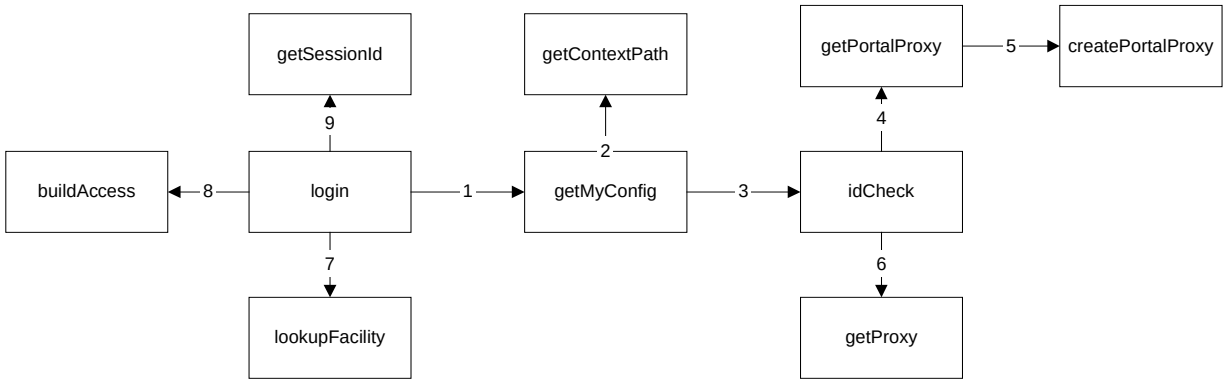

Figure 1. Code Walkthrough

4. USE CASES

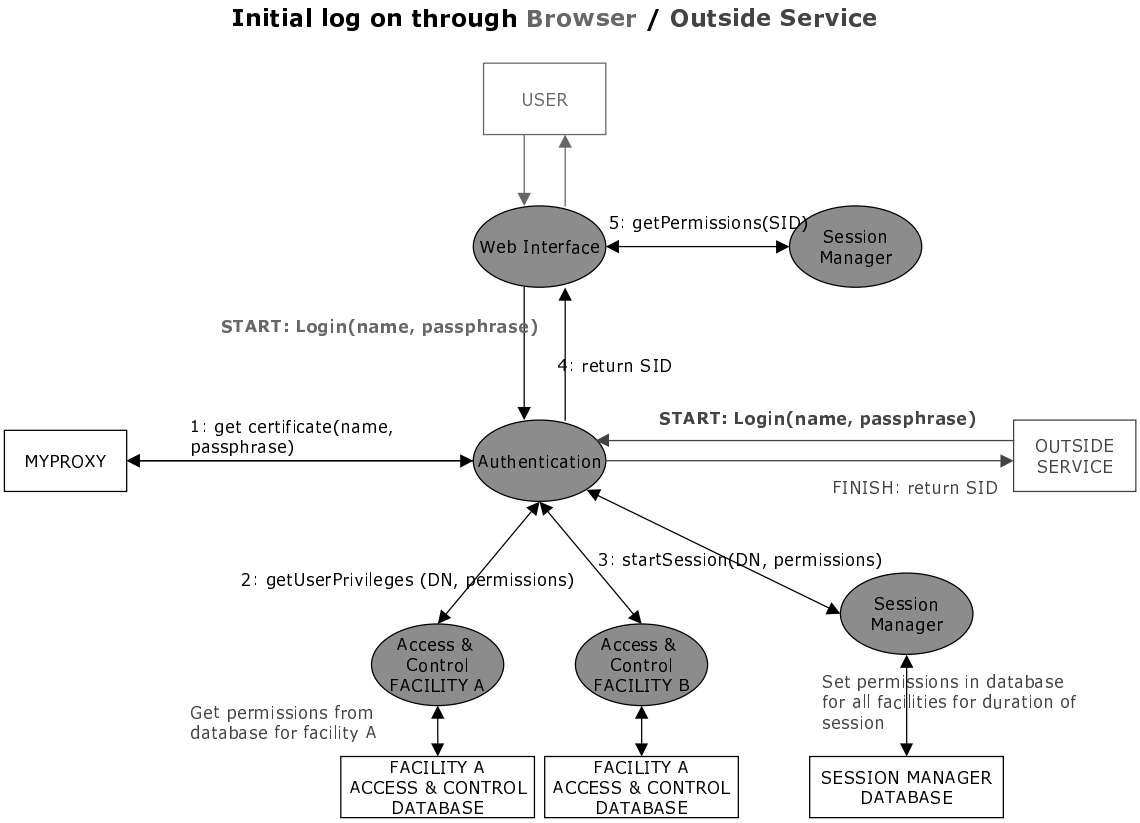

Figure 2 Authentication & Authorisation

4.1 Login through Browser

User logs in using a standard web browser. The Web Interface calls the Authentication and Authorization service to obtain a certificate from the MyProxy server. The Authentication and Authorization service then requests the user's permissions from each facilities Access Control service (one per facility) and these are collated. Finally it calls startSession() on the Session Manager, sending the collated information and receives a new session identifier. This is expanded in Figure 1.0.

4.2 Login through Outside Service

If an Outside Service has requested the login on behalf of a user or application, the Authentication And Authorization service behaves in the same way.