Delegation Issuing Service (DIS) Client Installation Guide

Document History

Version	Date	Comments
0.1	9 September 2005	First draft by Wensheng
0.2	12 September 2005	Updated by Tuan Anh
0.3	14 September 2005	Reviewed by David
1.0	15 September 2005	First public release
1.1	1 July 2006	Updated with Acceptance Tests for issuing attributes
1.2	24 July 2006	Update the installation instructions
1.3	26 July 2006	Updated with Acceptance Tests for revocation attributes
1.4	14 August 2006	Fix some inconsistencies after validating by Romain
1.5	3 October 2006	Add the SearchRequestor parameter, change the parameters in the configuration file using Permis standard parameters.
1.6	24 October 2006	Add instruction for using policy stored in a file
1.7	24 October 2006	Add support for java 1.5
1.8	22 February 2007	Add support for Tomat 5.5
1.9	23 April 2007	Add support for Apache 2.2
2.0	12 August 2008	Using PERMIS v5 policies and Apache http server on Windows (by Linying)
2.1	25 March 2009	Updated the authentication of tomcat, DIS installation

		instruction, instruction for apache2.2 (by Kaniz)
2.2	17 February 2010	Revised and updated by Kaniz
2.3	16 April 2010	Updated by Mark
2.5	26 October 2010	Install guide rewritten and separated into its own document
2.5.2	2 November 2010	Java installation explained more fully. Tomcat native library installation corrected. Default DIS configuration file inserted.
2.5.4	5 November 2010	Addressed feedback from Kaniz
2.5.5	26 May 2011	Added alternative <FilesMatch> for PHP files. Updated screenshots for DIS Web UI. Refreshed formatting. Added table of contents. Added missing information from old document version.
2.5.6	13 July 2011	Client installation guide revised, updated and separated into its own document.
2.5.7	23 August 2011	Addressed received feedback

Contents

Introduction

The Delegation Issuing Service (DIS) is a web service for issuing attribute certificates on behalf of privilege holders who wish to delegate their privileges to their peers and subordinates. The DIS web service is accessed by DIS web service client applications through SOAP calls. A DIS client application may be the end user (e.g. when an application wants to delegate privileges to another application) or may be directly connected to a human user via an appropriate user interface, or may be a trusted server acting as a proxy between human users and the DIS (e.g. the Apache client that we provide in this release).

For demonstration purposes, we have written a client application in PHP that acts as a trusted proxy running on an Apache server. It invokes the DIS web service server, via SOAP calls. The human end users access the Apache proxy via a standard web browser, and are authenticated to Apache using their usernames and passwords that are stored in the local LDAP server.

This document describes the installation steps of the DIS PHP client application.

In this user guide, we assume that you have the DIS Web Service installed according to the DIS Service installation guide. The examples presented in this document assumes that the Tomcat server holding the DIS Web service and the Apache server for the PHP client are running on the same computer (thus the use of localhost throughout the guide), although you may run them in different computers.

System Requirements

- An Apache HTTP Server configured with SSL, PHP, LDAP and Proxy
- A LDAP server that holds user login credentials that Apache can read

A publicly available demo of the Delegation Issuing Service client is available at https://sec.cs.kent.ac.uk/dis.html. Trying out this demo will give users a better understanding of what they are trying to build.

Software Contents

The software is available from http://sec.cs.kent.ac.uk/permis/downloads/Level3/DIS.shtml.

Inside `disInterface_x_x_x.zip` there is a directory called `clientSide`, which contains the following files:

- **disClientPHP/…**

  The DIS Web User Interface files.

The `clientSide` directory also contains a subdirectory called `disClientKeystore`, which contains the following files, used in the example installation below:

- **cacert.pem**

  Apache CA certificate file, used by the Apache server.
- **httpd-cert-key.pem**

  Apache proxy SSL public key certificate and private key file, used by the Apache proxy.
- **httpd-cert.p12**

  This is the same SSL certificate in pkcs12 format. Its password is “dis123”. This will be used by java client of DIS.
- **httpd-cert.pem**

  Apache SSL public key certificate, used by the Apache server.
- **httpd-key.pem**

  Apache SSL private key, used by the Apache server.

Example Installation of the DIS Web User Interface

This example installation follows on from the DIS Web Service installation guide and has been tested with the following software versions:

- Apache HTTP Server 2.2.19
- PHP 5.3.6

A general knowledge of UNIX commands is required to follow this example installation.

Step 0: Directory for holding the installation.

To keep things simple, we will use the same directory used for installing the DIS web service.

Copy the contents extracted from the disInterface_x_x_x.zip file to your dis directory.

Execute the following command:

```
cp –r /path/to/clientSide ~/dis
```

Step 1: Install Apache HTTP Server

Apache HTTP Server is required for hosting the DIS Web User Interface.

Download the Apache source from http://httpd.apache.org/ to `~/dis`. Extract the downloaded file to the same location. Execute the following commands there:

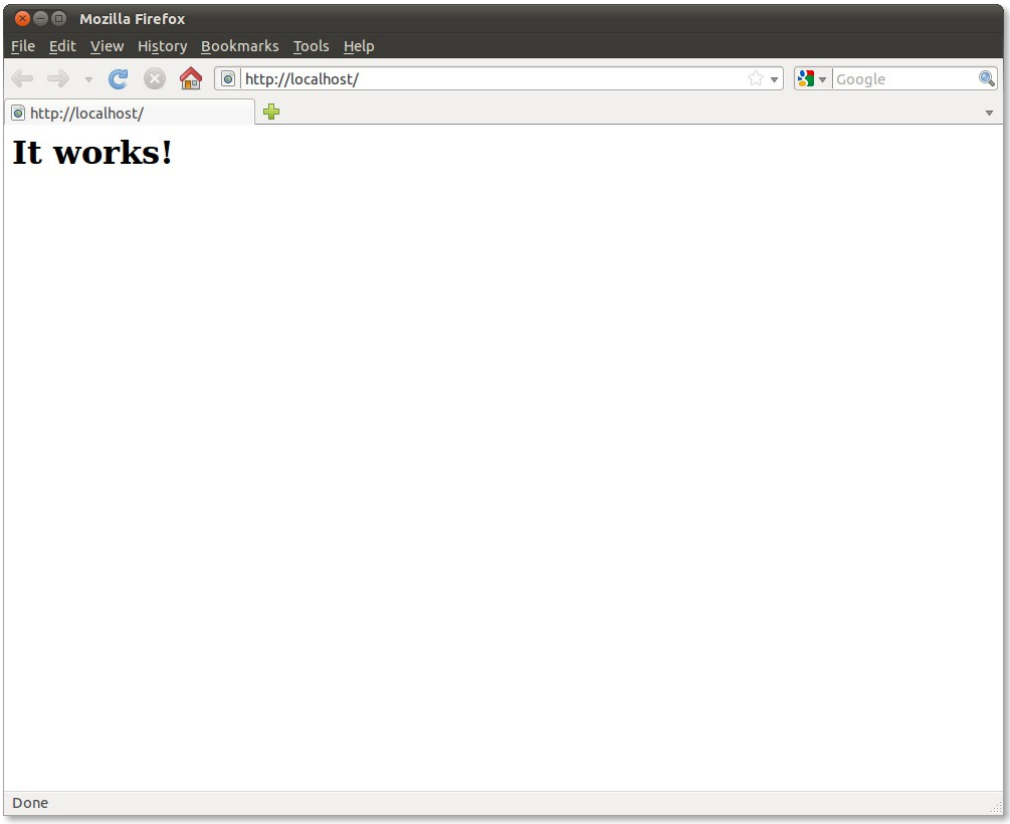
```
1. ./configure --enable-authnz-ldap --enable-proxy --enable-proxy-http
   --enable-so --enable-ssl --enable-unique-id --enable-mods-shared=all
   --enable-ldap --with-ldap --with-ldap-
   include=/home/user/dis/openldap/include --with-ldap-
   lib=/home/user/dis/openldap/lib --prefix=/home/user/dis/apache2.2
2. make
3. make install
```

Apache should now be installed to `~/dis/apache2.2`.

We will now test Apach works. Start Apache by executing:

```
sudo ~/dis/apache2.2/bin/apachectl -k start
```

Go to http://localhost in a web browser. “It works!” should be displayed.



Step 2: Install PHP

PHP is required for producing the dynamic web pages of the DIS Web User Interface.

Download the PHP 5 source from http://www.php.net/ to `~/dis`. Extract the downloaded file to the same location. Execute the following commands there:

```
1. sudo apt-get install libxml2-dev
2. ./configure --prefix=/home/user/dis/php --enable-soap --with-
   apxs2=/home/user/dis/apache2.2/bin/apxs --with-openssl --with-
   ldap=/home/user/dis/openldap
3. make
4. make install
```

PHP should now be installed.

We now need to make Apache parse .php files as PHP. Append the following[1] to `/home/user/dis/apache2.2/conf/httpd.conf`:

```
<FilesMatch \.php$>
    SetHandler application/x-httpd-php
</FilesMatch>
```

[1] If this does not work, try “AddHandler php5-script php” instead of “SetHandler application/x-httpd-php”.

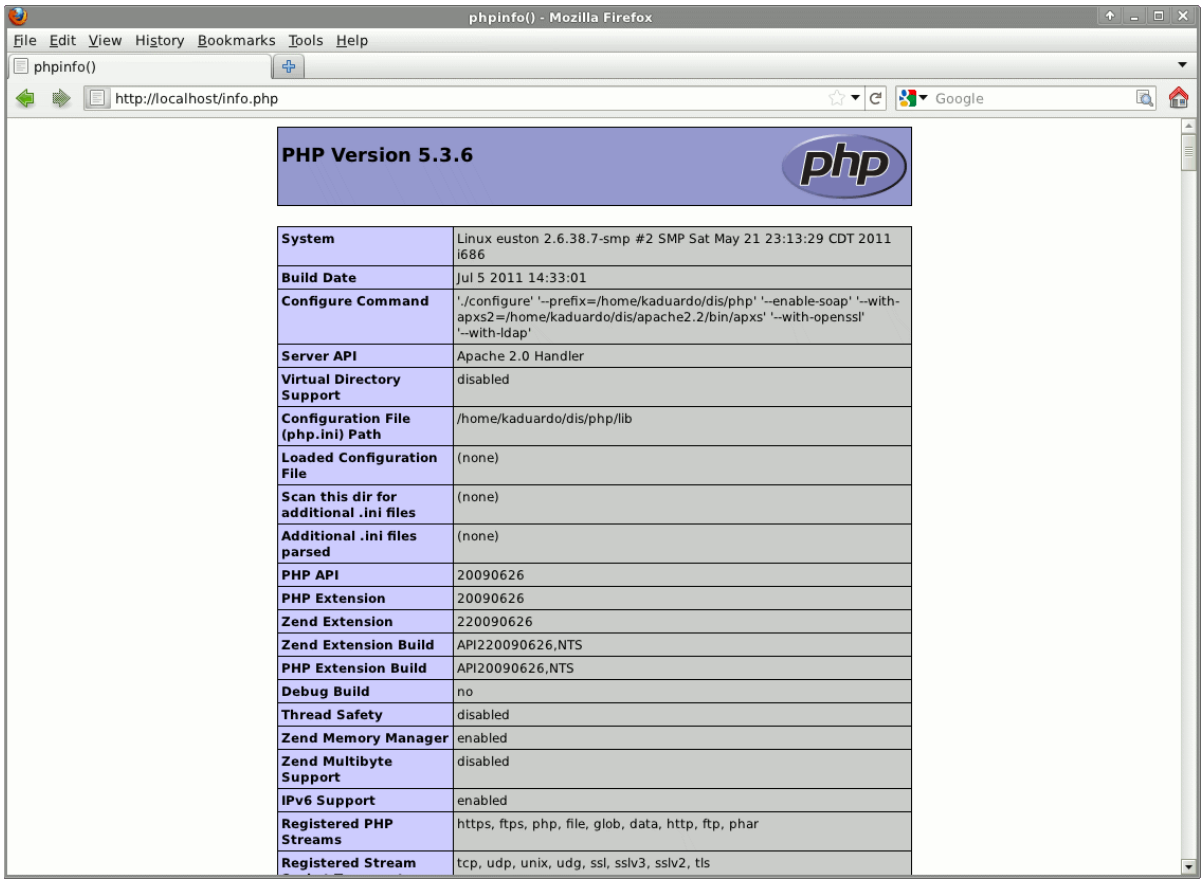
We will now test PHP works. Create a file `info.php` in `/usr/local/apache2.2/htdocs` with the following contents:

```
<?php phpinfo(); ?>
```

Restart Apache by executing:

```
sudo /usr/local/apache2.2/bin/apachectl -k restart
```

Go to http://localhost/info.php. Information about this PHP's configuration should be displayed.



Step 3: Enable SSL on Apache HTTP Server

In `~/dis/apache2.2/conf/httpd.conf` uncomment the following line:

```
Include conf/extra/httpd-ssl.conf
```

Append the following to `~/dis/apache2.2/conf/extra/httpd-ssl.conf`:

```
ProxyRequests Off
<Proxy>
    Order allow,deny
    Allow from all
</Proxy>
```

Execute the following commands:

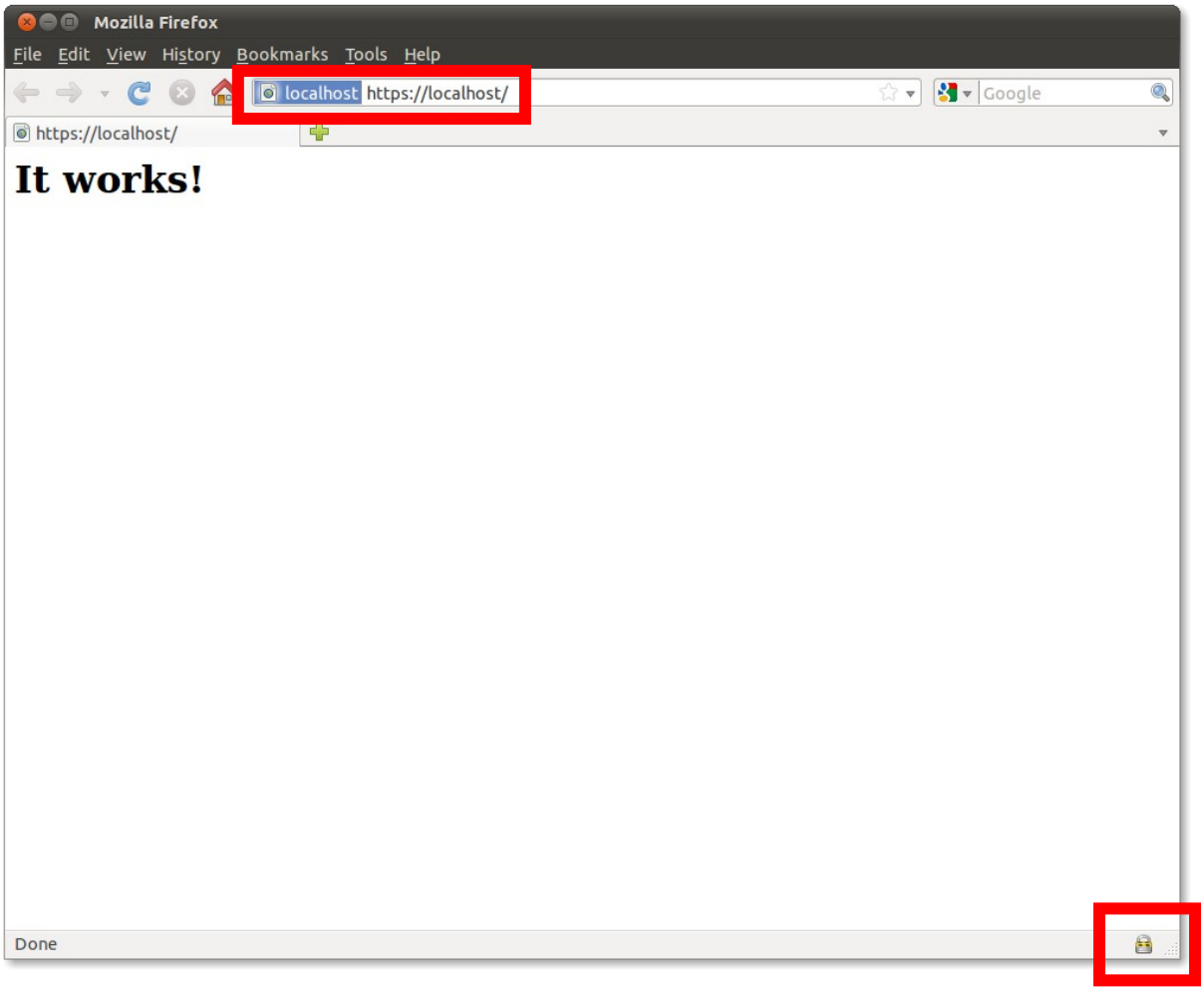
```
1. mkdir ~/dis/apache2.2/conf/ssl.crt
2. mkdir ~/dis/apache2.2/conf/ssl.key
3. cd ~/dis/clientSide/disClientKeystore
4. cp httpd-cert.pem cacert.pem httpd-cert-key.pem
   ~/dis/apache2.2/conf/ssl.crt/
5. cp httpd-key.pem ~/dis/apache2.2/conf/ssl.key/
```

Append the following to `~/dis/apache2.2/conf/extra/httpd-ssl.conf`:

```
ProxyPass /disproxy https://localhost:8443/axis2/services/DIS
SSLProxyEngine on
SSLProxyCipherSuite RC4-MD5:RC4-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA
SSLCertificateFile /home/user/dis/apache2.2/conf/ssl.crt/httpd-cert.pem
SSLCertificateKeyFile /home/user/dis/apache2.2/conf/ssl.key/httpd-key.pem
SSLCACertificateFile /home/user/dis/apache2.2/conf/ssl.crt/cacert.pem
```

Ensure any other directives for `SSLCertificateFile`, `SSLCertificateKeyFile` and `SSLCACertificateFile` in `~/dis/apache2.2/conf/extra/httpd-ssl.conf` are commented out. This enables server authentication.

We will now test server authentication. Restart Apache and go to https://localhost in a web browser. After accepting the server's certificate, the "It works!" should be displayed.



Step 4: Allow the Apache HTTP Server to act as a DIS trusted proxy

This is required for allowing it to act as a trusted proxy to the DIS Web Service. Apache will present its SSL certificate to the DIS Web Service, which will check if the subject DN in the certificate is configured as a trusted proxy.

Append the following to `~/dis/apache2.2/conf/extra/httpd-ssl.conf`:

```
SSLProxyCACertificateFile
/home/user/dis/apache2.2/conf/ssl.crt/cacert.pem

SSLProxyMachineCertificateFile
/home/user/dis/apache2.2/conf/ssl.crt/httpd-cert-key.pem

<Directory /home/user/dis/apache2.2/htdocs/disproxy>

    Order allow,deny

    Allow from localhost

</Directory>
```

Step 5: Enable LDAP authentication on Apache HTTP Server

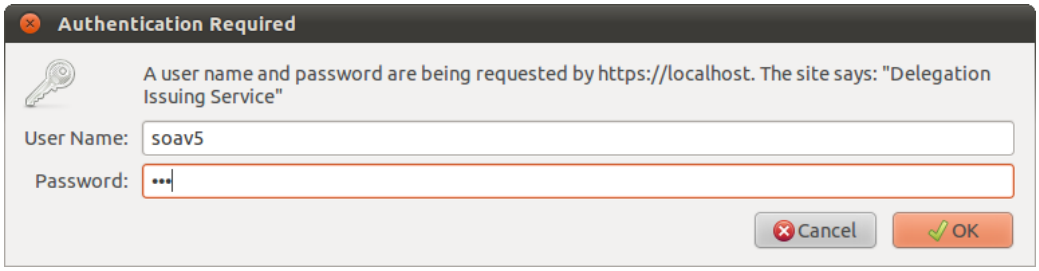
LDAP authentication on Apache is required for authenticating users of the DIS Web User Interface.

Make the directory `~/dis/apache2.2/htdocs/dis`. Append the following to `~/dis/apache2.2/conf/extra/httpd-ssl.conf`:

```
<Directory /home/user/dis/apache2.2/htdocs/dis>

    AuthName "Delegation Issuing Service"

    AuthType Basic

    AuthBasicProvider ldap

    AuthzLDAPAuthoritative off

    AuthLDAPURL ldap://localhost:389/c=gb?uid

    require valid-user

    AllowOverride FileInfo AuthConfig Limit

    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec

    <Limit GET POST OPTIONS>

        Order allow,deny

        Allow from all

    </Limit>

</Directory>
```

This enables LDAP authentication.

We will now test LDAP authentication. Restart Apache and go to https://localhost/dis in a web browser. After entering userid “soav5” and password “soa”, “Index of /dis” should be displayed.



Step 6: Install the DIS Web User Interface

To install the DIS Web User Interface, execute the following commands.

```
1. cd ~/dis/clientSide/disClientPHP
2. cp –r * ~/dis/apache2.2/htdocs
```

Next edit `~/dis/apache2.2/htdocs/dis/proxysigning.cfg`. The default configuration file is shown below.

```
ldapserver localhost
search c=gb
ServiceLocation https://127.0.0.1/disproxy
role Student
role Staff
role Professor
role Researcher
role Admin
type permisRole
key uid
Wsdl https://localhost:8443/axis2/services/DIS?wsdl
Wsdlcert /home/user/dis/apache2.2/conf/ssl.crt/httpd-cert-key.pem
```

Each parameter is defined below. For this example installation `Wsdlcert` is the only parameter that should need to be adjusted.

- **ldapserver**

  The LDAP server that holds the attribute certificates. This server will be queried for users that can be delegates.

- **search**

  The LDAP search root for the aforementioned query.

- **ServiceLocation**

The address of the DIS service proxy on Apache.

- **roleValue**

  The delegatable role values displayed to users. The roleValue parameter can be repeated as many times as necessary, for multiple role values.

- **roleType**

  The role type of the role values mentioned in the above parameter(s).

- **key**

  The name of the LDAP username attribute, i.e. the attribute in the AuthLDAPURL directive from the previous step. This is used to find the distinguished name of logged in users, so the DIS knows who sent a delegation request.

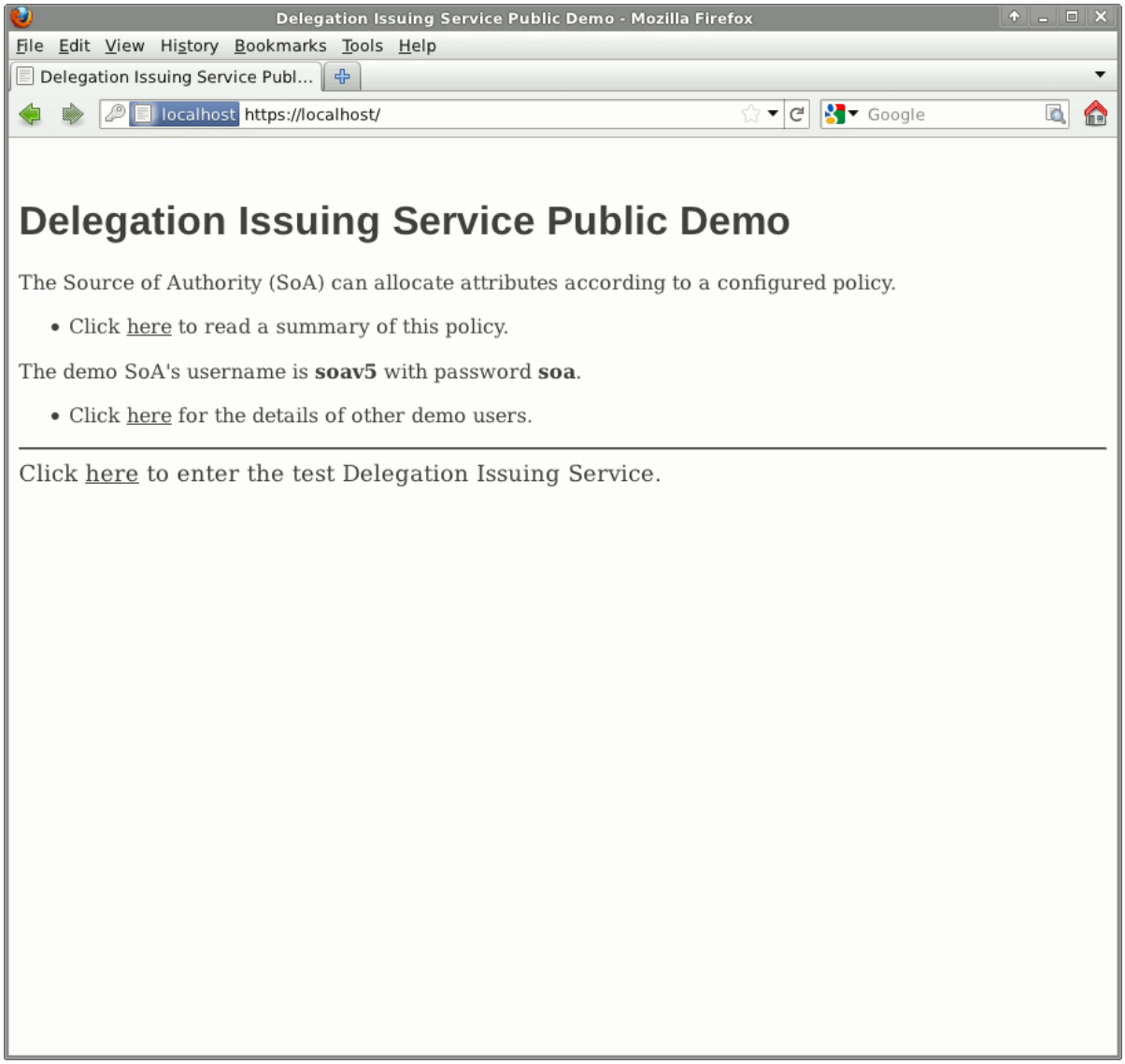
- **Wsdl**

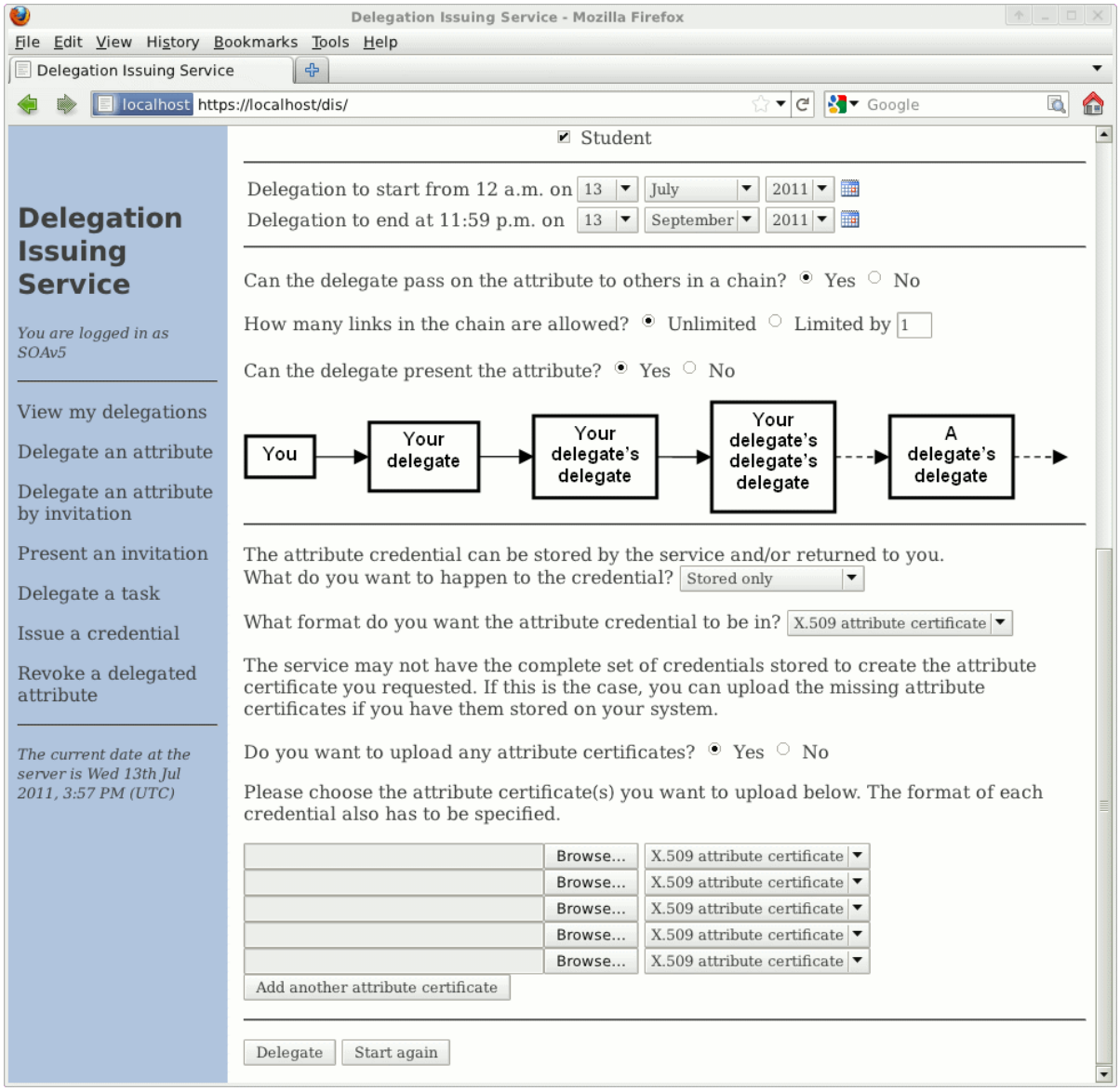
  The URL of the DIS Web Service's WSDL

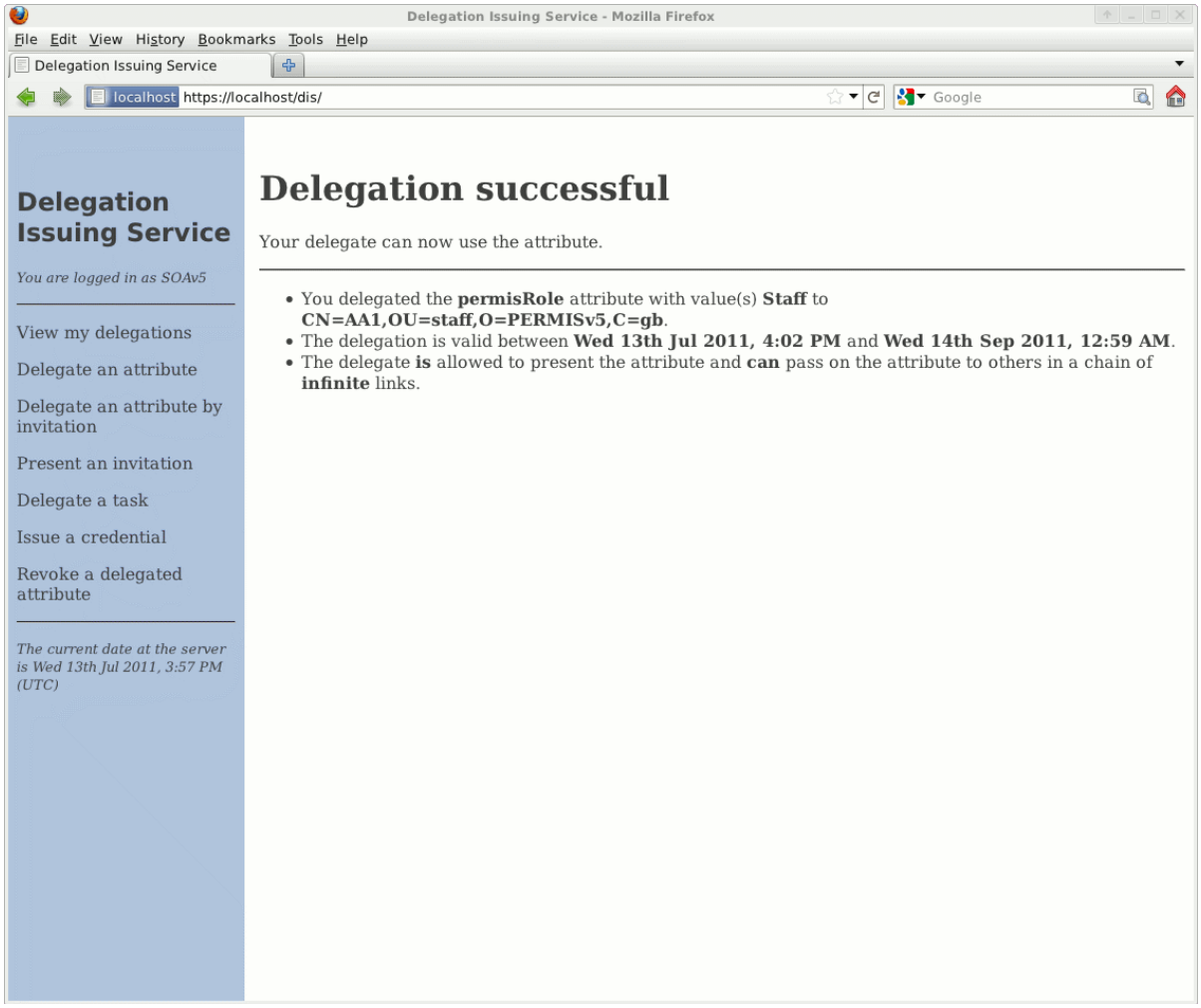
- **Wsdlcert**

  The path of the certificate to present to get the above WSDL.

We will now test the DIS Web User Interface. Go to https://localhost/ in a web browser. The DIS welcome page should be displayed. Click the link to enter the DIS. Valid delegation requests should now be accepted by the DIS.


Delegation Issuing Service Public Demo - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Delegation Issuing Service Publ...
localhost https://localhost/
Google
Delegation Issuing Service Public Demo
The Source of Authority (SoA) can allocate attributes according to a configured policy.
Click here to read a summary of this policy.
The demo SoA's username is soav5 with password soa.
Click here for the details of other demo users.
Click here to enter the test Delegation Issuing Service.


Delegation Issuing Service - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Delegation Issuing Service
localhost https://localhost/dis/
Google
Delegation Issuing Service
You are logged in as SOAv5
View my delegations
Delegate an attribute
Delegate an attribute by invitation
Present an invitation
Delegate a task
Issue a credential
Revoke a delegated attribute
The current date at the server is Wed 13th Jul 2011, 3:57 PM (UTC)
Student
Delegation to start from 12 a.m. on 13 July 2011
Delegation to end at 11:59 p.m. on 13 September 2011
Can the delegate pass on the attribute to others in a chain? Yes No
How many links in the chain are allowed? Unlimited Limited by 1
Can the delegate present the attribute? Yes No
You
Your delegate
Your delegate's delegate
Your delegate's delegate's delegate
A delegate's delegate
The attribute credential can be stored by the service and/or returned to you.
What do you want to happen to the credential? Stored only
What format do you want the attribute credential to be in? X.509 attribute certificate
The service may not have the complete set of credentials stored to create the attribute certificate you requested. If this is the case, you can upload the missing attribute certificates if you have them stored on your system.
Do you want to upload any attribute certificates? Yes No
Please choose the attribute certificate(s) you want to upload below. The format of each credential also has to be specified.
Browse... X.509 attribute certificate
Add another attribute certificate
Delegate
Start again


Delegation Issuing Service - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Delegation Issuing Service
localhost https://localhost/dis/
Google
Delegation Issuing Service
You are logged in as SOAv5
View my delegations
Delegate an attribute
Delegate an attribute by invitation
Present an invitation
Delegate a task
Issue a credential
Revoke a delegated attribute
The current date at the server is Wed 13th Jul 2011, 3:57 PM (UTC)
Delegation successful
Your delegate can now use the attribute.
• You delegated the permisRole attribute with value(s) Staff to CN=AA1,OU=staff,O=PERMISv5,C=gb.
• The delegation is valid between Wed 13th Jul 2011, 4:02 PM and Wed 14th Sep 2011, 12:59 AM.
• The delegate is allowed to present the attribute and can pass on the attribute to others in a chain of infinite links.