Integrating EJBCA and OpenSSO

EJBCA is an Enterprise PKI Certificate Authority issuing certificates to users, servers and devices. In an organization certificate can be used for strong authentication. EJBCA is based on standard such as X.509 and OCSP.

OpenSSO provides core identity services to simplify the implementation of transparent single sign-on (SSO). OpenSSO provides authentication and authorization services based on standards such as SAML and XACML.

Contents

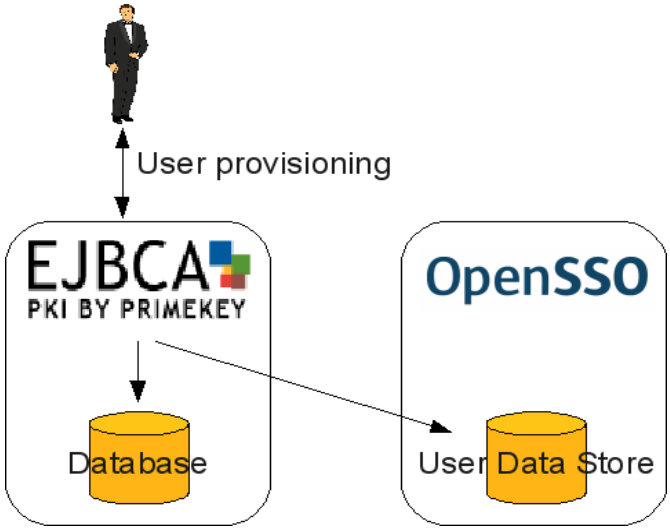
Integration goal

The goal of this integration description is to demonstrate creating users issuing certificate to those users, and using those certificates to authenticate the user with OpenSSO. Doing all this with only adding the user once in EJBCA, issuing the certificate.

- Issue a digital certificate to a user using EJBCA.
- Immediately use this certificate for single sign-on and and authorization with OpenSSO.

Deployment Architecture

In this integration guide the deployment architecture is a simple one where user provisioning is made in EJBCA.



Installation prerequisites

To perform the steps in this simplified guide we have made default installations of EJBCA and OpenSSO in the same JBoss application server. In order to be able to use OpenSSO for certificate authentication the CA certificate from EJBCA must be installed in the Java trust store of the system:

- In the EJBCA administration console go to *Basic Functions*.
- For the default CA, *AdminCA1*, select the link *Download binary/to IE* and save the certificate in the file system as *AdminCA1.cacert.crt*.
- Open a command line windows where the certificate was saved and enter the command:
  - `keytool -import -keystore $JAVA_HOME/jre/lib/security/cacerts -file`

```
AdminCA1.cacert.crt
```

Example on Ubuntu Linux:

```
sudo keytool -import -keystore /usr/lib/jvm/java-6-openjdk/jre/lib/security/cacerts
-file AdminCA1.cacert.crt
```

After performing this step, your application server must be restarted.

Configuring OpenSSO

Install OpenSSO

This is not an installation guide for OpenSSO, hence we will only cover the configuration for the actual integration. To make the basic setup of OpenSSO you can follow the installation instructions of the product.

There are two configuration option you set during installation that is important to remember for the integration:

- Hostname and port of the OpenSSO User Data Store LDAP server, usually something like *ds.domain.com* and *50389*.
- Login and password to the OpenSSO User Data Store, could be something like *cn=Directory Manager* and the same password as *amadmin*.
- The Root Suffix of the LDAP tree in the User Data Store, usually something like *dc=opensso,dc=company,dc=com*.

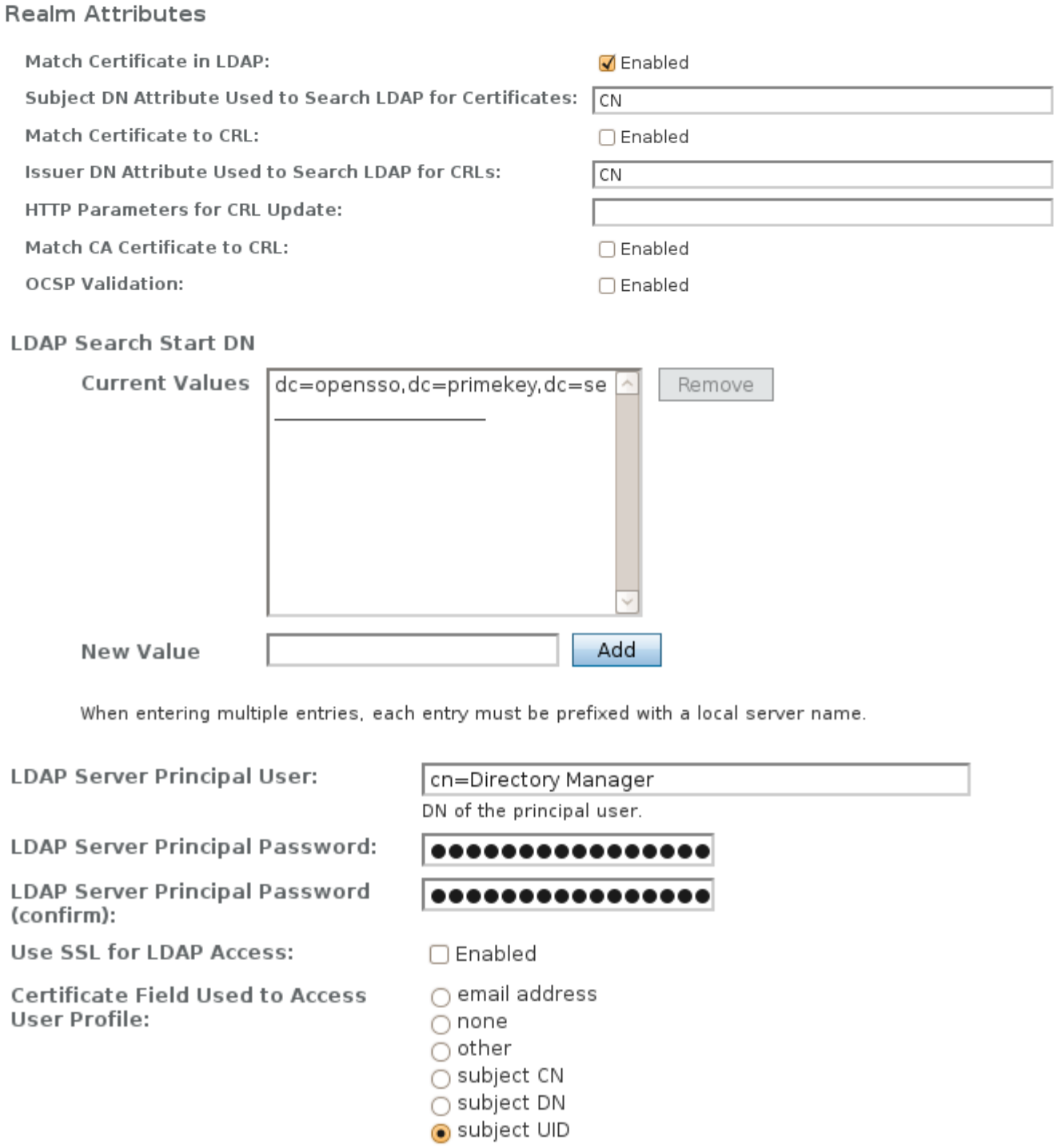
Configure the Certificate authentication module

Since we will use certificates for stronger authentication we need the Certificate authentication module enabled in OpenSSL.

- Log in to the administration console as *amadmin*.
- Go to *Access Control, '/ (Top Level Realm)'* and finally *Authentication*.
- Under *Module Instances*, click *New*.
- Select *Certificate* as type and enter *Certificate* as name. Click *OK*.
- Click on *Certificate* under *Module Instances* to configure the module.
    - Match Certificate in LDAP: Enabled
    - LDAP Search Start DN: Use Root Suffix of the LDAP tree, *dc=opensso,dc=company,dc=com*
    - LDAP Server Principal User: Use login to the User Data Store, c*n=Directory Manager*

- LDAP Server Principal Password: Use login to the User Data Store
- Certificate Field Used to Access User Profile: Use *Subject UID*

- Click *Save*



Configuring EJBCA

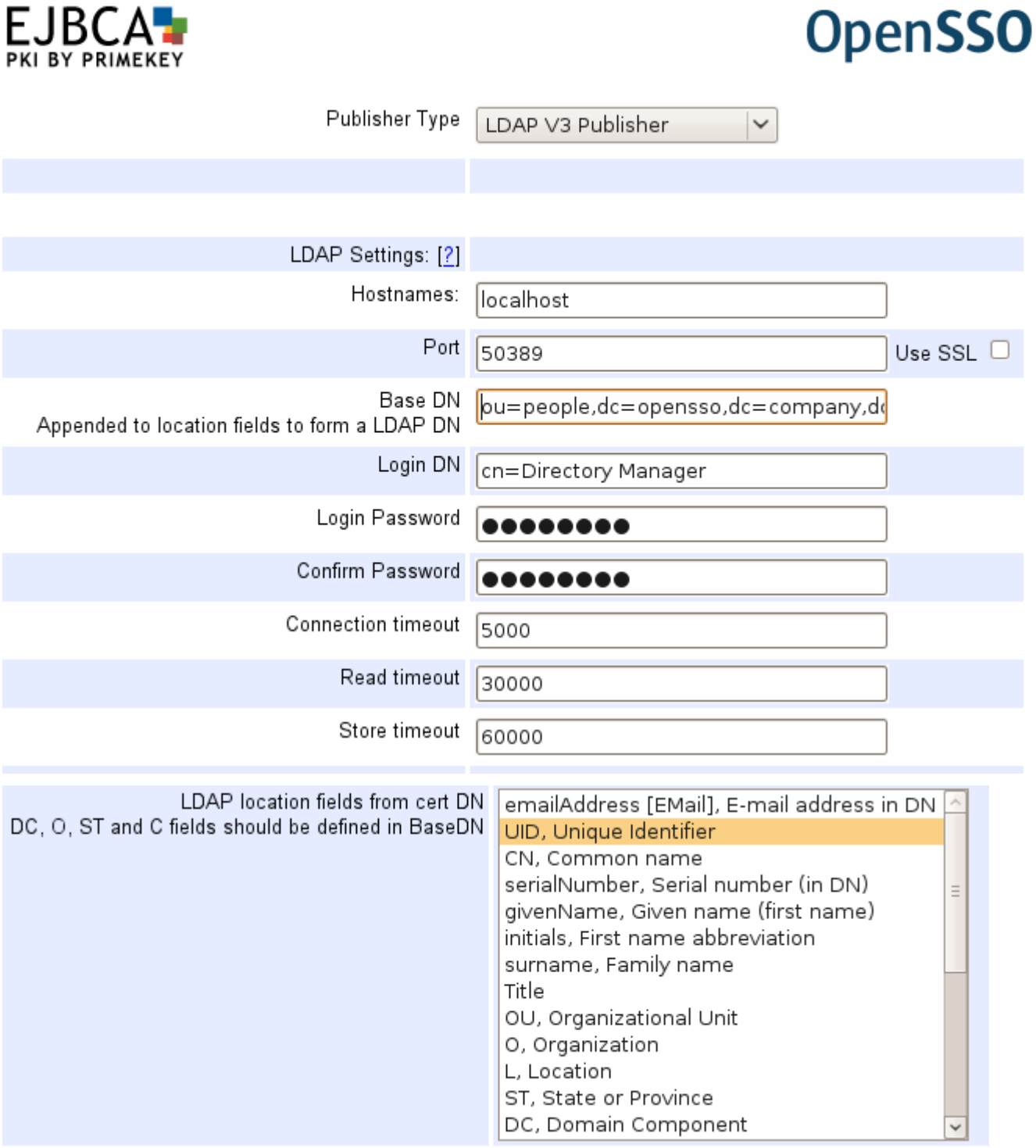
Install OpenSSO

This is not an installation guide for EJBCA, hence we will only cover the configuration for the actual integration. To make the basic setup of EJBCA you can follow the installation instructions of the product.

Creating the LDAP publisher

We will use a regular LDAP publisher to publish user data and issued certificates from EJBCA to OpenSSO when certificates are issued.

- Login to the EJBCA administration console and click on *Edit Publishers*.
- Add a new publisher called *OpenSSOPublisher*. Select the publisher and click *Edit Publisher*.
- Hostname and port: Use the hostname and port of the OpenSSO User Data Store, *ds.domain.com* and *50389*. Uncheck *Use SSL*.
- Base DN: Use Root Suffix prepended with *ou=people*, *ou=people*, *dc=opensso,dc=company,dc=com*. This is the tree where default users are stored in OpenSSO. Adapt this is you have configured something else in you User Data Store.
- Login DN and password: Use the same as LDAP Server Principal User in the OpenSSO configuration, *cn=Directory Manager*.
- Login Password: Use login to the User Data Store
- LDAP location fields from cert DN: Use *UID, Unique Identifier*
- Click *Save and Test Connection*, it should say *Connection Tested Successfully*



Create the certificate profile

We will use a certificate profile to control that all certificates issued using this profile is published to OpenSSO.

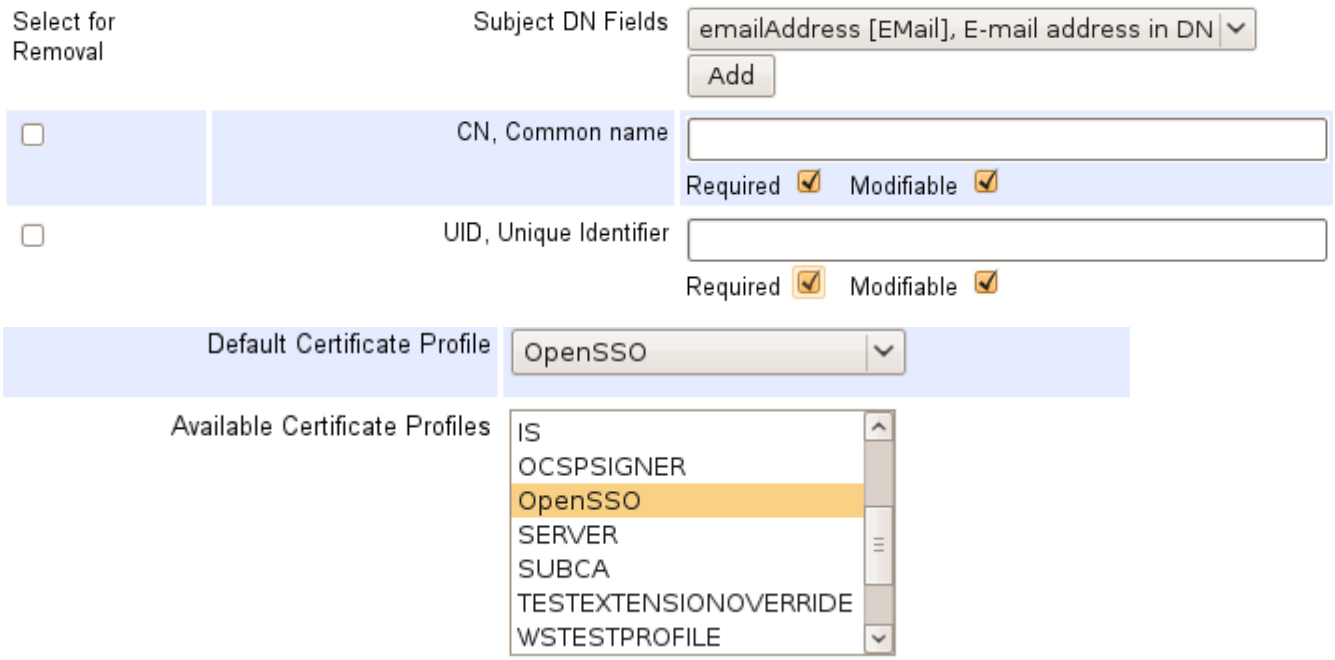
- Click on *Edit Certificate Profiles*

- Add a new certificate profile called *OpenSSO* by typing *OpenSSO* in the input field, selecting *ENDUSER* in the list and clickin on *Use selected as* templet (this saves us a few clicks later).
- Select *OpenSSO* and click *Edit Certificate Profile*.
- Go down almost to the bottom of the page and select *OpenSSOPublisher*. Click *Save*.

Create the end entity profile

We will use an end entity profile to control which user attributes are registered when we add the user.

- Click on *Edit End Entity Profiles*
- Add a new end entity profile called *OpenSSO*. Select the profile and click *Edit End Entity Profile*.
- Select *UID* in *Subject DN Fields* and click *Add*.
- Select *OpenSSO* as both *Default Certificate Profile* and *Available Certificate Profiles*.
- Click *Save*.



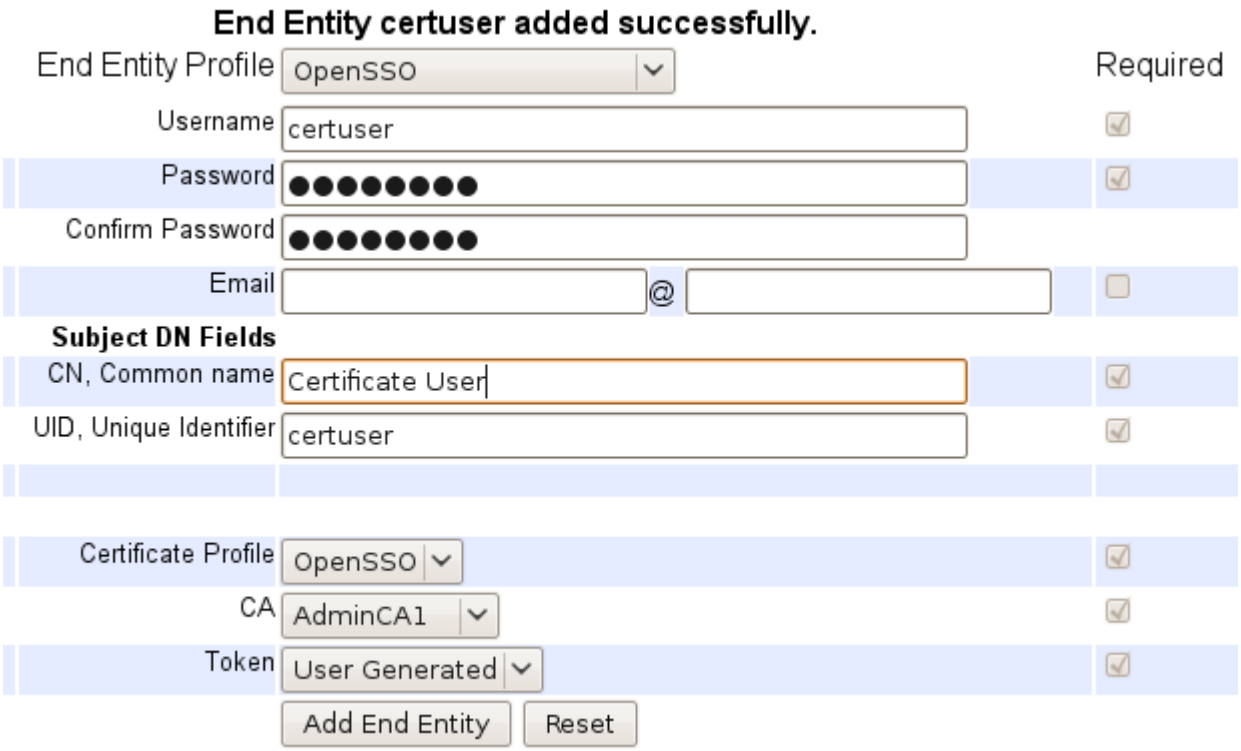
Creating the user

When the user is added in EJBCA, a username and password is created. Using this username and password the user can enroll for a certificate, using a regular web browser. When the certificate is issued to the user, it is also published to the OpenSSO User Data Store so it can be used by OpenSSO.

Adding the user in EJBCA

This step will add the user in EJBCA's user database. During this step the user is issued a username and password. In different organizations this can be done in thousands of different ways, the step shown here is only one example.

- In the EJBCA aministration console go to *Add End Entity*.
- Select *OpenSSO* as end entity profile in the drop-down.
- Username: certuser
- Password: certuser
- CN: Certificate User
- UID: certuser
- Click *Add End Entity*



Issuing the certificate

Using the username and password registered above we can now enroll for a certificate in our web browser. In this example we will use FireFox, but Internet Explorer works just as well.

- Go to the EJBCA Public Web, there is a link from the administration console.
- Click *Create Browser Certificate.*
- Username: certuser
- Password: certuser
- On the next page click *OK* to get the certificate issued and installed in your browser.

Using the certificate for authentication in OpenSSO

The new user has now been created in EJBCA and in the OpenSSO User Data Store. You can view the user in OpenSSO.

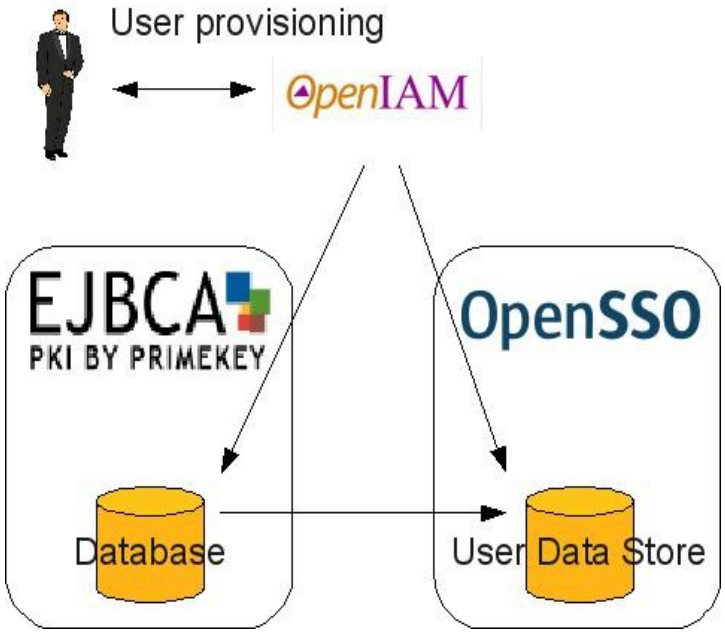
- In the OpenSSO administration console go to *Subjects.* You should see *Certificate User* in the user list.

Next we want to test if the user can be authenticated in OpenSSO and the certificate is located.

- Close down the browser, in order for the EJBCA administrator to be logged out.
- Start the browser again and go to the OpenSSO administration console login. Edit the login URL to use SSL with client certificate authentication and the *Certificate* login module: https://localhost:8443/opensso/UI/Login?module=Certificate

Other Deployment Architectures

In a larger deployment neither EJBCA or OpenSSO is designed to do user provisioning. In such an installation a separate provisioning product would typically be used, or even several different ones.



More information

For more information and documentation about EJBCA, visit http://www.ejbca.org/.

Form information about support and maintenance subscriptions and training for EJBCA, visit http://www.primekey.se/.

For more information and documentation about OpenSSO, visit http://opensso.dev.java.net/