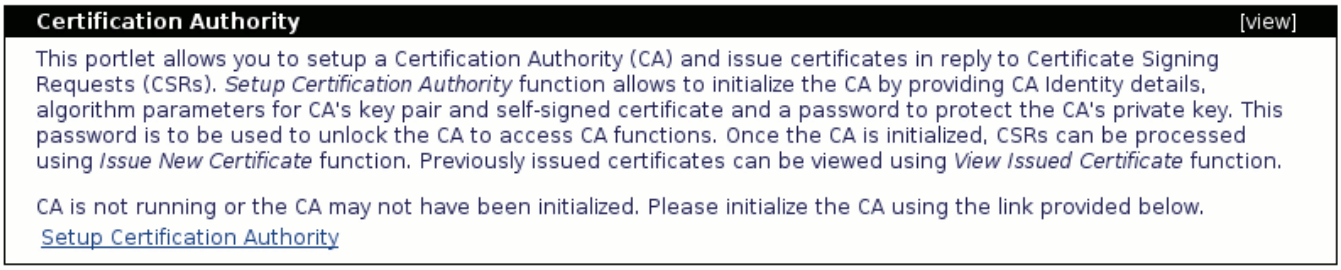
Certification Authority

{scrollbar}

This release of Apache Geronimo allows you to define your own Certification Authority (CA) and issue certificates in reply to Certificate Signing Requests (CSR). The Certification Authority portlet is avaiable by clicking **Certificate Authority** on the left menu in the Geronimo Administration Console.

Configuring a Certification Authority

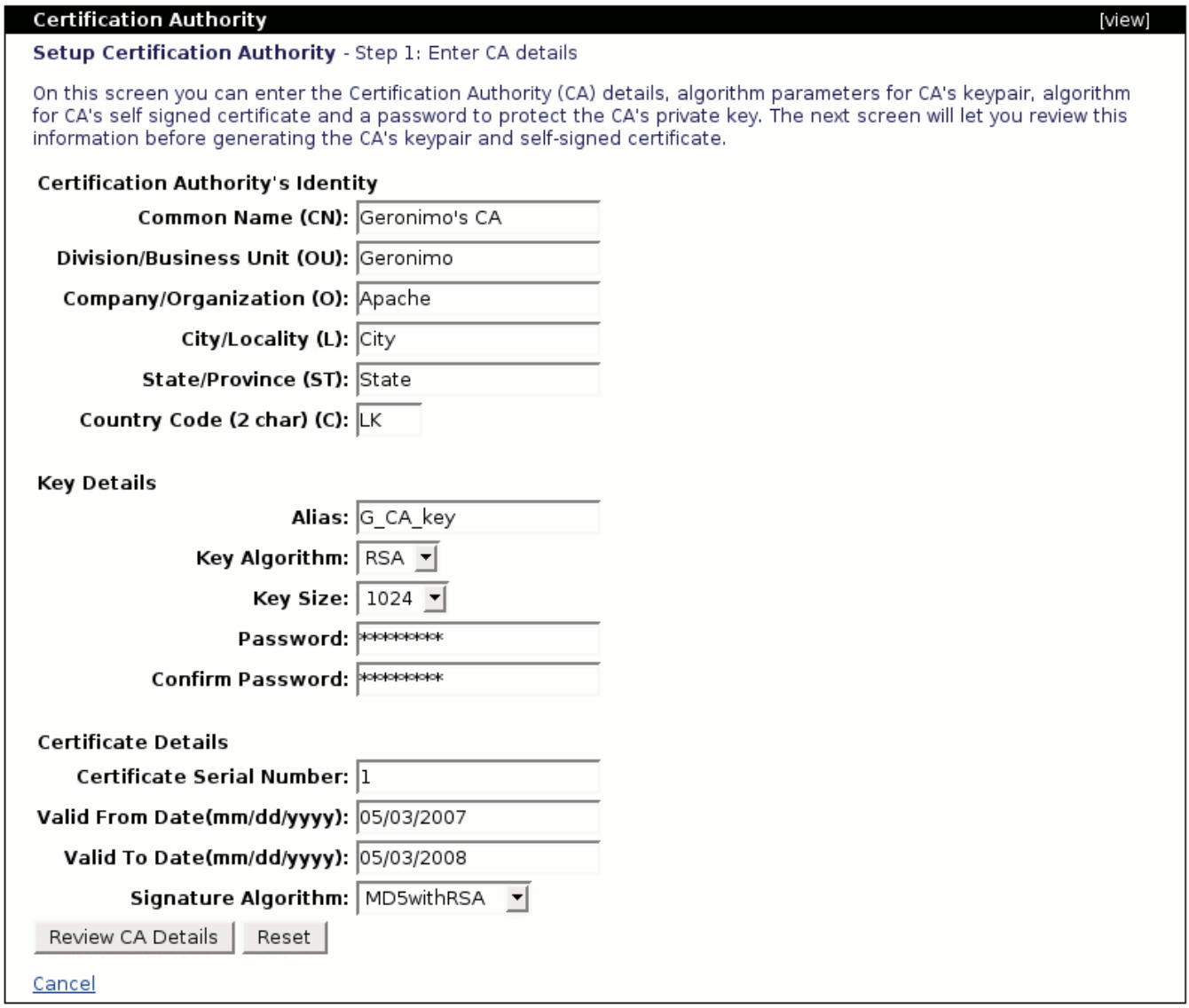
The first time you call this porlet the CA is not yet configured so you will see a screen similar to this one.



Click on **Setup Certification Authority** to configure Geronimo as a CA.

This process is somewhat similar to defining keystores and certificates as covered in the Administering certificates, this is in the sense that you should be prepared to provide similar type of information.

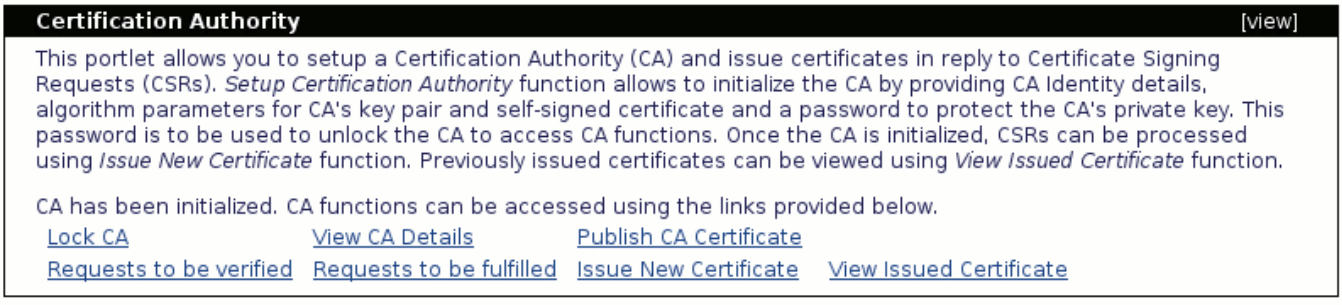
The first step is defining the Certification Authority details as illustrated in the following image. The information entered in this form will be used to create the Certification Authority and respective self-signed key pairs.



This is an "information gathering" step, at this point you are not creating any certificates yet. Click on **Review CA Details** and then on **Setup Certification Authority**.

Once created you will see a confirmation message **CA Setup is successful!** along with the details for the certificate you just created.

Next time you access the **Certification Authority** portlet you should see the the CA you just created. From this portlet now you can manage CSRs, review and issue certificates.



Signing certificate requests

The Certificate Properties File Realm section cover in great detail how to create a new keystore and certificate and how to create a CSR and then import the CA's reply. In this section we will focus on how the CA manages and signs the client CSR.

We will start from the point where you generate the CSR, here is the example we used for the Certificate Properties File Realm section.