Configurazione EJBCA per l'utilizzo dei WS

1. Dopo aver installato EJBCA, scaricare il certificato superadmin.p12 dal server EJBCA (path: */home/user/ejbca_6_0_3/p12*)

2. Se si vuole cambiare la password del certificato (ad esempio per dare la stessa password ai certificati) si possono utilizzare le seguenti istruzioni:

```
openssl pkcs12 -in my_cert.p12 -out
/tmp/my_cert.pem

openssl pkcs12 -export -in /tmp/my_cert.pem –out
/tmp/my_new_cert.p12

rm -f my_cert.p12 /tmp/my_cert.pem
```

3. Il superadmin così ottenuto va utilizzato all'interno del codice inserendolo nel path */MIUR_PRISMA-2.1-BusinessLayer/src/main/resources/cert/ejbca*
   Il nome va specificato come ***SVCEP_EJBCA_SUPERADMIN*** nel file di properties *services-endpoints.properties* nel rispettivo ambiente in */MIUR_PRISMA-2.1-BusinessLayer/src/main/resources/var-configs-profiles*

4. Ora è necessario aggiungere la CA al truststore java in modo da riconoscerla come affidabile.
   Per fare ciò bisogna innanzitutto ottenere il certificato della CA ed è possibile farlo tramite webui di EJBCA.
   Entrare nel portale EJBCA dell'ambiente da utilizzare e nella sezione Administration -> CA Structure & CRLs scaricare il certificato .pem della root CA.
   Inserire, tramite filezilla, quest'ultimo nella macchina del BL che deve interfacciarsi con EJBCA e lanciare il seguente comando:

```
keytool -keystore cacerts -importcert -file
certificatoDellaCaPrecendentementeImportato
```

   La password del cacerts è *changeit*