Evidencias Interoperabilidad XRoad Julio 2017

gob.mx

gob.mx

Índice

Control de versiones del documento

Versión	Fecha	Descripción de la actualización	Elaborado por
1.0	10/07/2017	Elaboración de las evidencias correspondientes a la instalación y configuración de servicios relacionados al sistema X-Road, EJBCA.	Leví Durán Torres

1 Objetivo.

Este documento está destinado a dar una representación gráfica de los elementos que soportan la instalación y configuración de servicios relacionados al sistema X-Road.

2 Evidencias.

1. Evidencia: Configuración de entidades finales en EJBCA

EJBCA

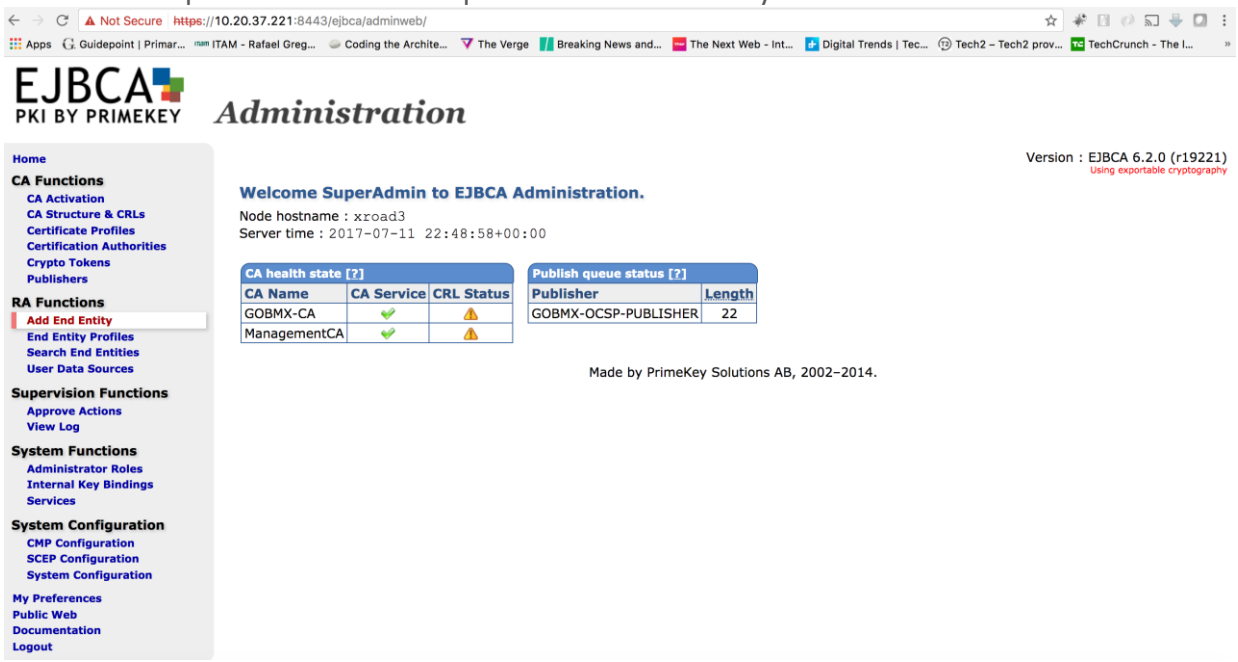
A continuación se mencionan las instrucciones para poder configurar usuarios (entidades finales) dentro la consola de administración de EJBCA

Alta

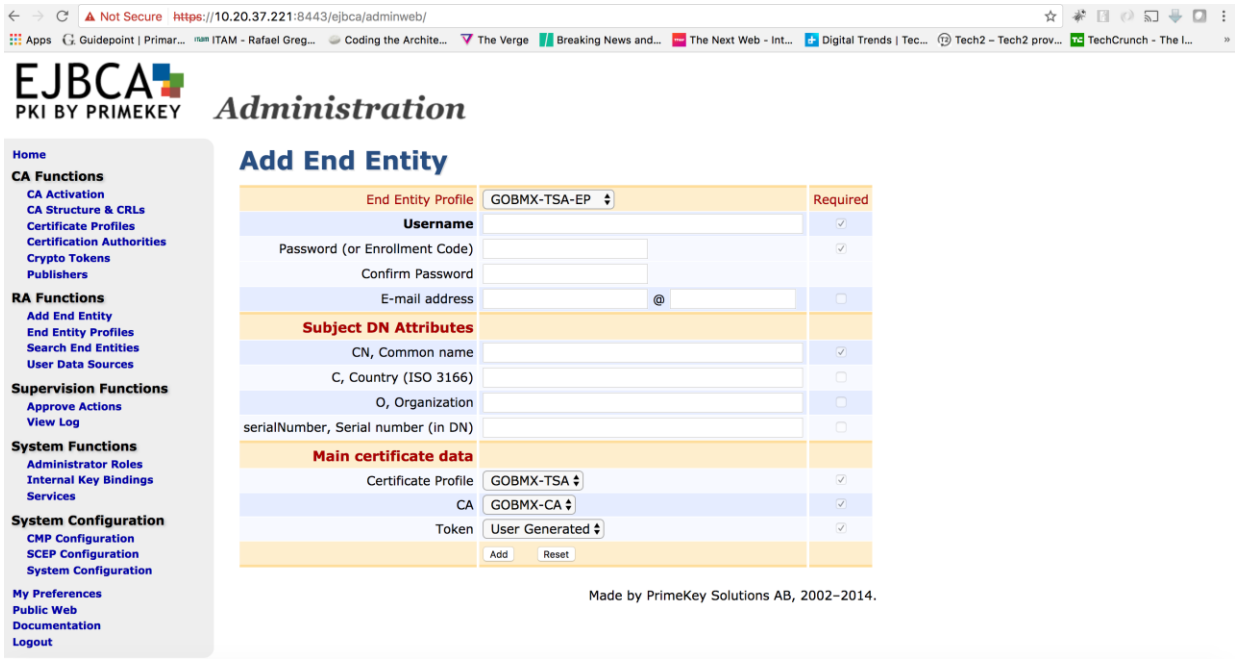
1. Para dar de alta una entidad final dentro de EJBCA primero hay que acceder a la url de la consola de administración de EJBCA (asegurarse de tener el certificado de admin para EJBCA desde la máquina donde se quiera acceder a la consola, este se encuentra en la ruta /home/user/ejbca_ce_6_x_x/p12/superadmin.p12 del servidor EJBCA)

   https://10.20.37.221:8443/ejbca/adminweb/

2. En el menú izquierdo acceder a la opción de Add End Entity



3. Deberá aparecer una forma como la siguiente:



4. Indicar los valores deseados para Certificate Profile, CA y End Entity Profile deseado, para el caso del ambiente de pruebas xroad elegir

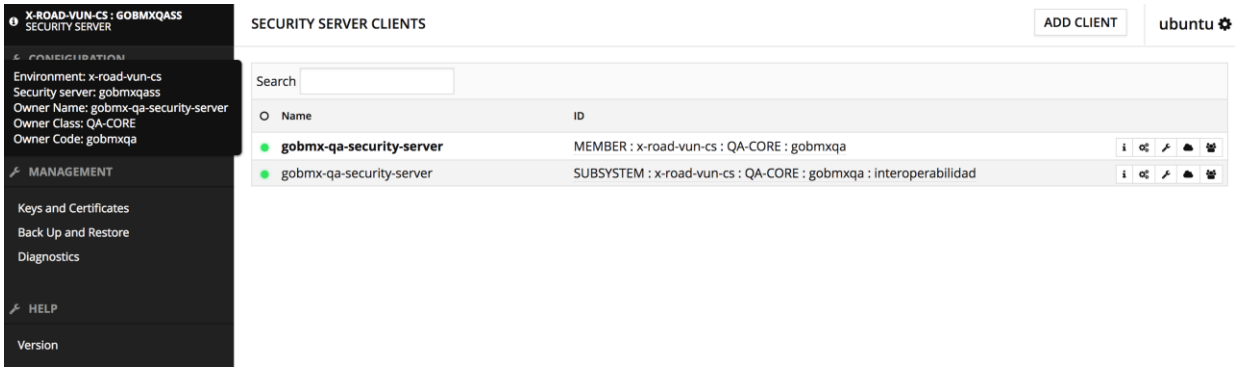
   End Entity Profile: GOBMX-AUTH-EP
   Certificate Profile: GOBMX-AUTH
   CA: GOBMX-CA

   También se debe de elegir un username así como un password

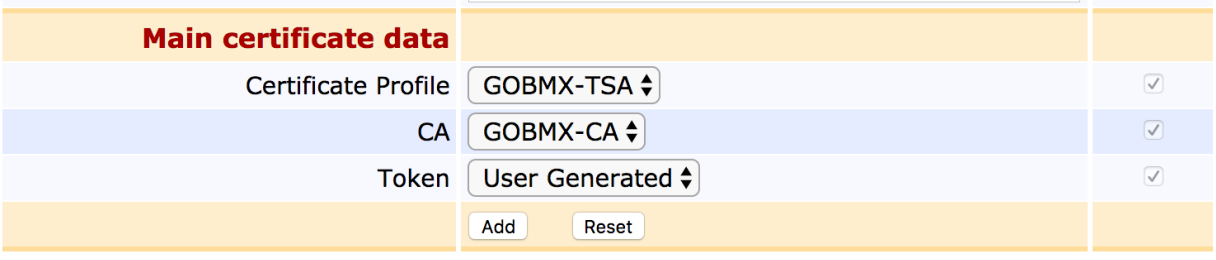
5. Para el caso de los campos CN (common name),C (country),O (organization), serialNumber
   CN: a elegir
   C: MX
   O: GOBMX
   SN: Utilizar la siguiente nomenclatura para certificados x-road
   {ambiente x-road}/{nombre security server}/{owner class}

Nota: Para el caso en que se requiera dar de alta nuevas dependencias dentro del ambiente de pruebas de x-road gobmx se recomienda que por cada security server que se necesite configuar se tomen los usuarios existentes de gobmxsignqa y gobmxauthqa (para certificado de sign y auth respectivamente) para generar los certificados y solo se cambie el valor del serial number. Específicamente solo se requiere cambiar el campo de {security server} de acuerdo a la nomenclatura antes mencionada con el nombre del security server que se esté configurando en el momento. De esta forma se evita la creación de dos entidades finales por cada dependencia.

Los datos para el serial number se pueden obtener hacienda hover sobre el icono de información en el menú del lado izquierdo de la consola del x-road security server



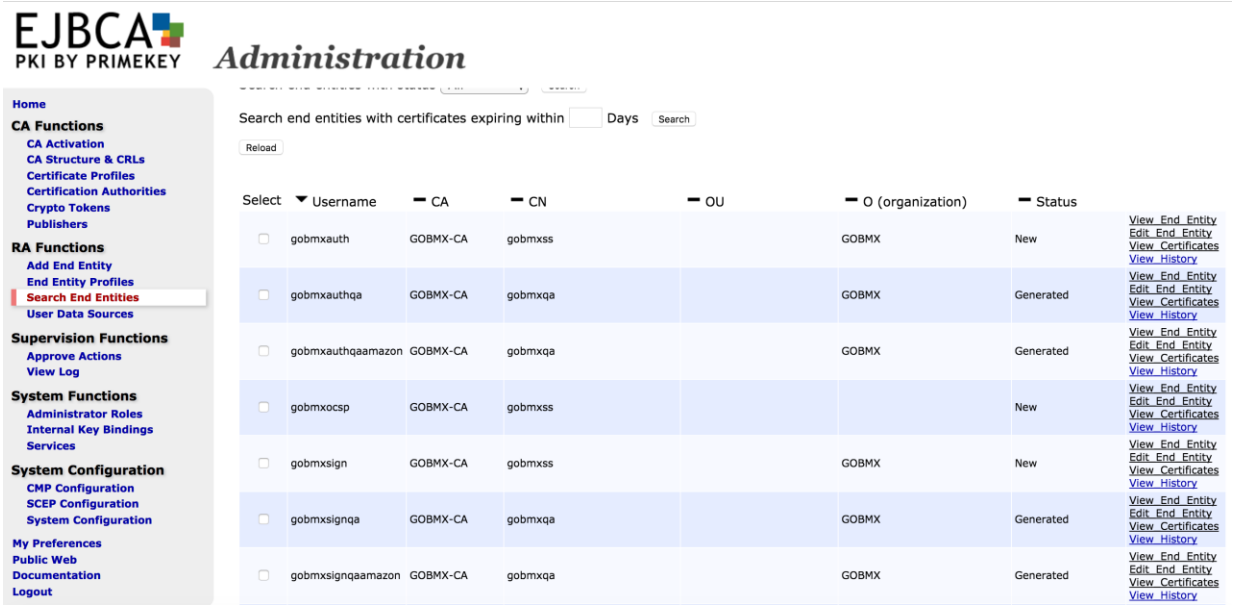
6. Asegurarse que dentro de la forma de alta de end entity esté habilitada la opción de User Generated en el campo de Token



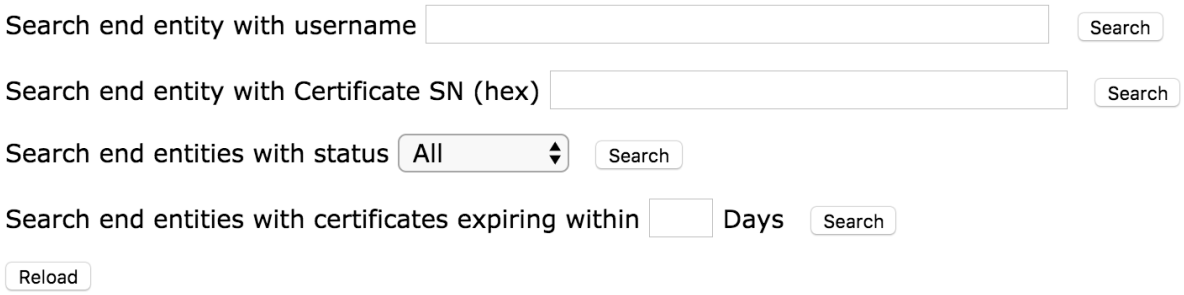
7. Dar click en el botón Add

Búsqueda de entidades de usuario

1. En el menú izquierdo acceder a la opción Search End Entities



2. Para obtener todas las entidades finales existentes elegir la opción de All en el campo de Search end entities with status



3. Dar click en Reload para que se desplieguen los resultados de la búsqueda

Select	Username	CA	CN	OU	O (organization)	Status	
☐	gobmxauth	GOBMX-CA	gobmxss		GOBMX	New	View End Entity Edit End Entity View Certificates View History
☐	gobmxauthqa	GOBMX-CA	gobmxqa		GOBMX	Generated	View End Entity Edit End Entity View Certificates View History
☐	gobmxauthqaamazon	GOBMX-CA	gobmxqa		GOBMX	Generated	View End Entity Edit End Entity View Certificates View History
☐	gobmxocsp	GOBMX-CA	gobmxss			New	View End Entity Edit End Entity View Certificates View History
☐	gobmxsign	GOBMX-CA	gobmxss		GOBMX	New	View End Entity Edit End Entity View Certificates View History
☐	gobmxsignqa	GOBMX-CA	gobmxqa		GOBMX	Generated	View End Entity Edit End Entity View Certificates View History
☐	gobmxsignqaamazon	GOBMX-CA	gobmxqa		GOBMX	Generated	View End Entity Edit End Entity View Certificates View History

Edición de entidades

1. Primero se deberá realizar una búsqueda como se describió en la sección anterior
2. Al obtener los resultados dar click sobre la opción de Edit End Entity la entidad final que se quiera editar, aparecerá la siguiente forma con la información correpondiente a esa entidad final

Search end entities with certificates expiring within Days Search

Reload

Select	Username	CA	CN	OU	O (organization)	Status	
☐	gobmxauth	GOBMX-CA	gobmxss		GOBMX	New	View End Entity Edit End Entity View Certificates View History
☐	gobmxauthqa	GOBMX-CA	gobmxqa		GOBMX	Generated	View End Entity Edit End Entity View Certificates View History
☐	gobmxauthqaamazon	GOBMX-CA	gobmxqa		GOBMX	Generated	View End Entity Edit End Entity View Certificates View History

Edit End Entity

End Entity Profile	GOBMX-AUTH-EP	Required
Status	Generated Save	
Username	**gobmxauthqaamazon**	☑
Password (or Enrollment Code)		☑
Confirm Password		
Maximum number of failed login attempts	○ ○ Unlimited	
Remaining login attempts	☐ Reset login attempts	
E-mail address	@	☐
Subject DN		
CN, Common name	gobmxqa	☑
C, Country (ISO 3166)	MX	☐
O, Organization	GOBMX	☐
serialNumber, Serial number (in DN)	x-road-vun-cs/gobmxqass-amazon/QA-CORE	☐
Main certificate data		
Certificate Profile	GOBMX-AUTH	☑
CA	GOBMX-CA	☑
Token	User Generated	☑
	Save Close	

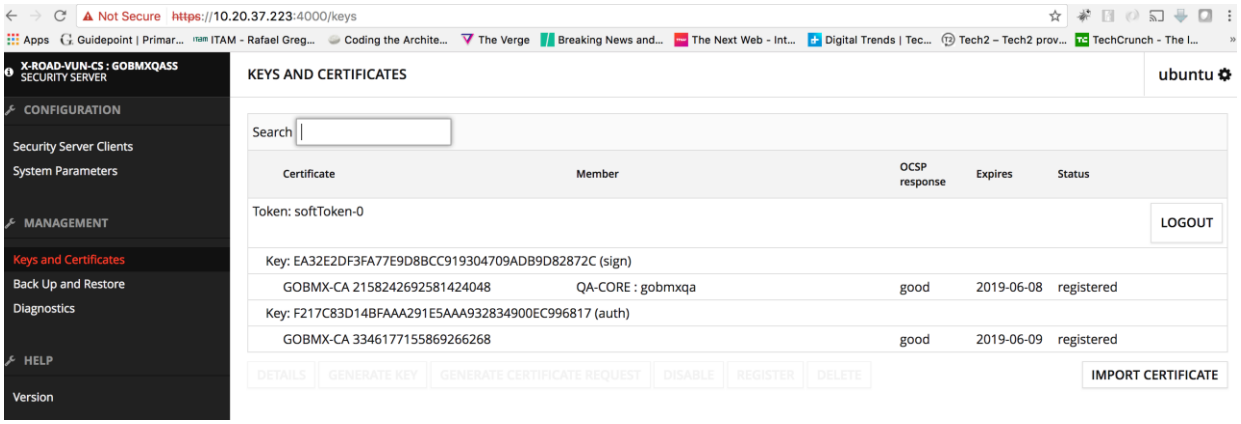
3. Realizar los cambios requeridos (la forma volverá a pedir un password) y dar click en Save

2. Evidencia: Generación de certificados firmados desde EJBCA/ gestión de certificados desde X-Road

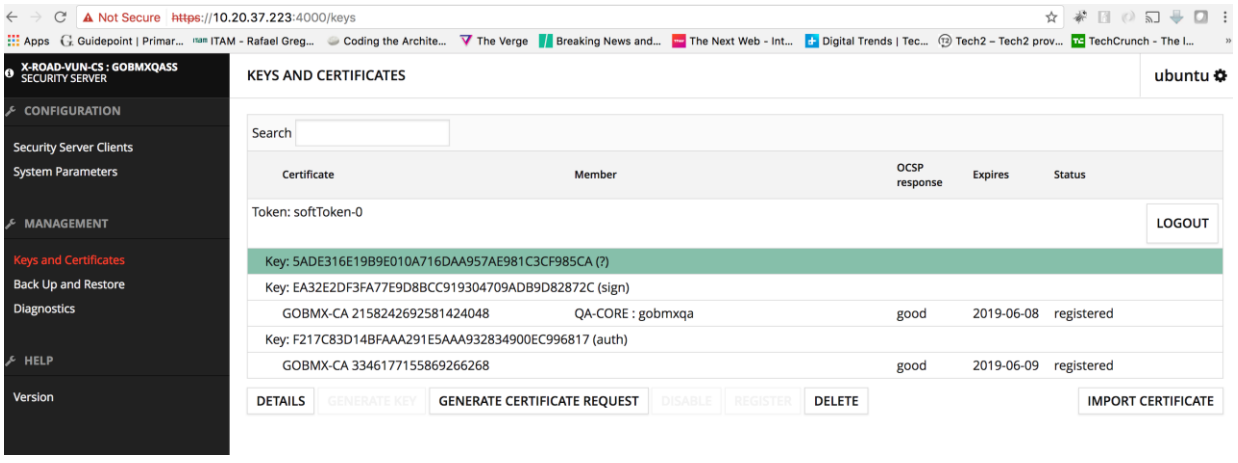
EJBCA/X-Road

A continuación se mencionan las instrucciones para poder configurar usuarios (entidades finales) dentro la consola de administración de EJBCA

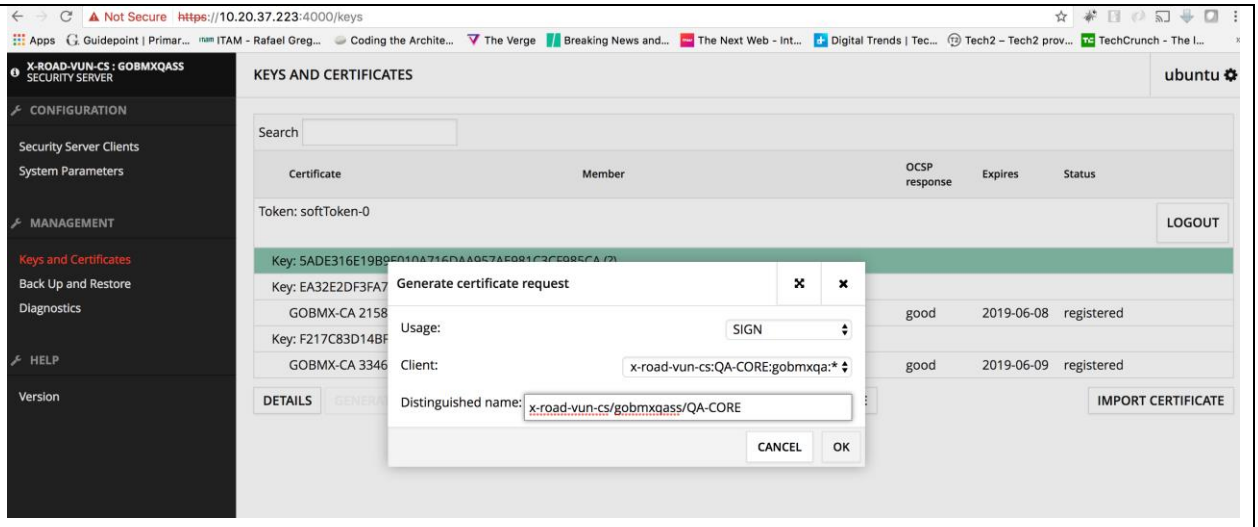
1. Para generar certificados para x-road primero se debe generar un CSR desde el x-road security server. Para eso después de firmarse dentro la consola web de x-road se debe elegir la opción de Keys and Certificates en el menú izquierdo lo cual desplegará la siguiente pantalla



2. Para generar un CSR el cual no se tiene asociado todavía algún certificado se debe dar click en Generate Key para crear una llave nueva



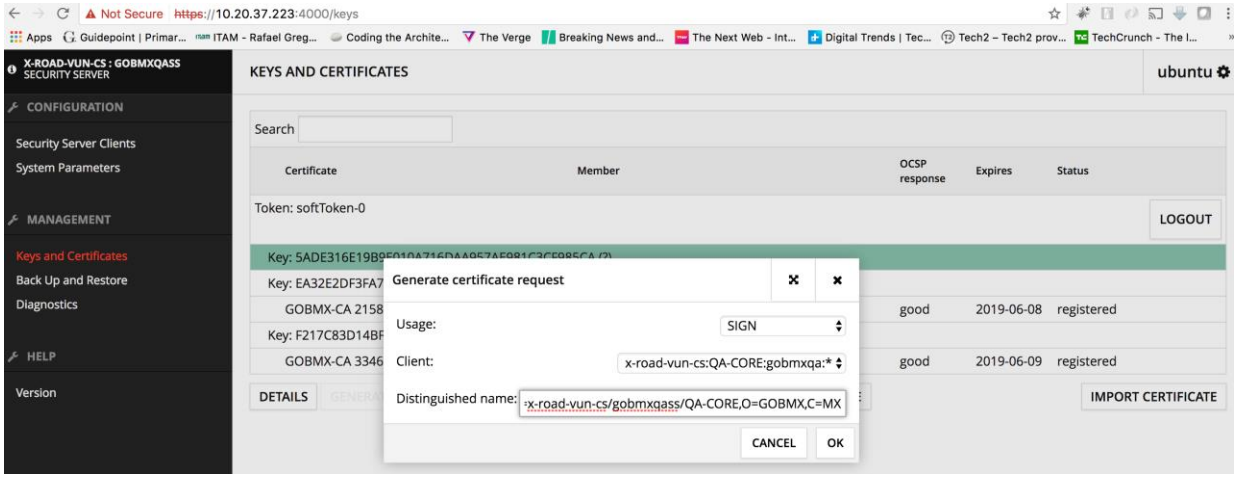
3. Teniendo seleccionada la nueva llave dar click en GENERATE CERTIFICATE REQUEST a lo que desplegará la siguiente forma



4. En el campo Distinguished Name se deberá poner una nomenclatura similar a la cadena de serial number que se pusó al dar de alta una nueva entidad final con las siguiente diferencia

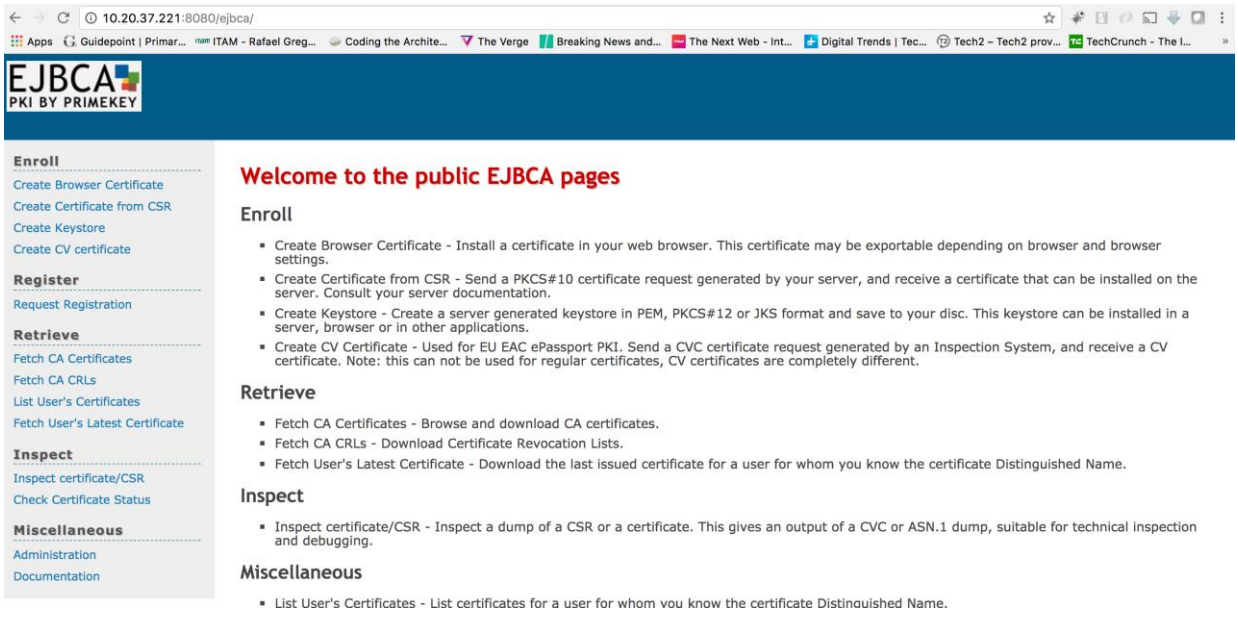
   CN=gobmxqa,SN=x-road-vun-cs/gobmxqass/QA-CORE,O=GOBMX,C=MX

   Nota:En este caso el valor que cambiaría con respecto al ambiente de X-Road gobmx sería el de “gobmxqass” por el nombre del security server en donde se esté realizando la generación del CSR

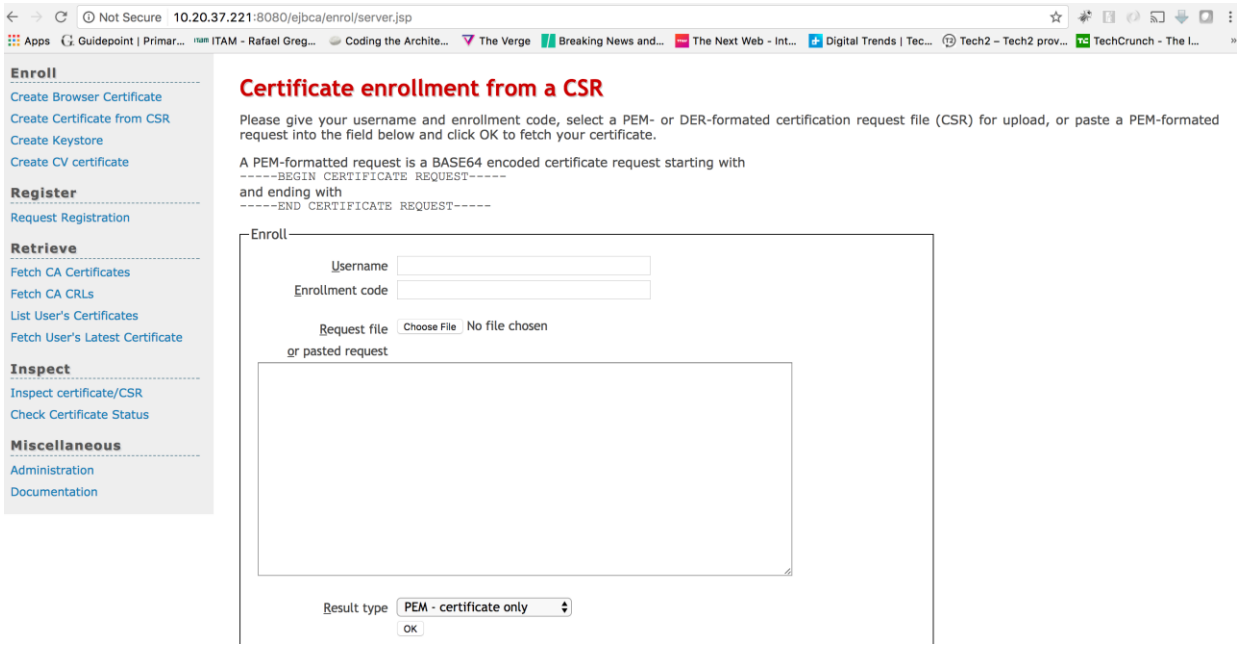


5. Dar click en OK, esto generará el CSR que se descargará de forma automática. Nota: este paso se deberá realizar dos veces, primero para el certificado de sign y después para el certificado de auth
6. Ahora se debe de proceder a acceder a liga de la consola pública de EJBCA

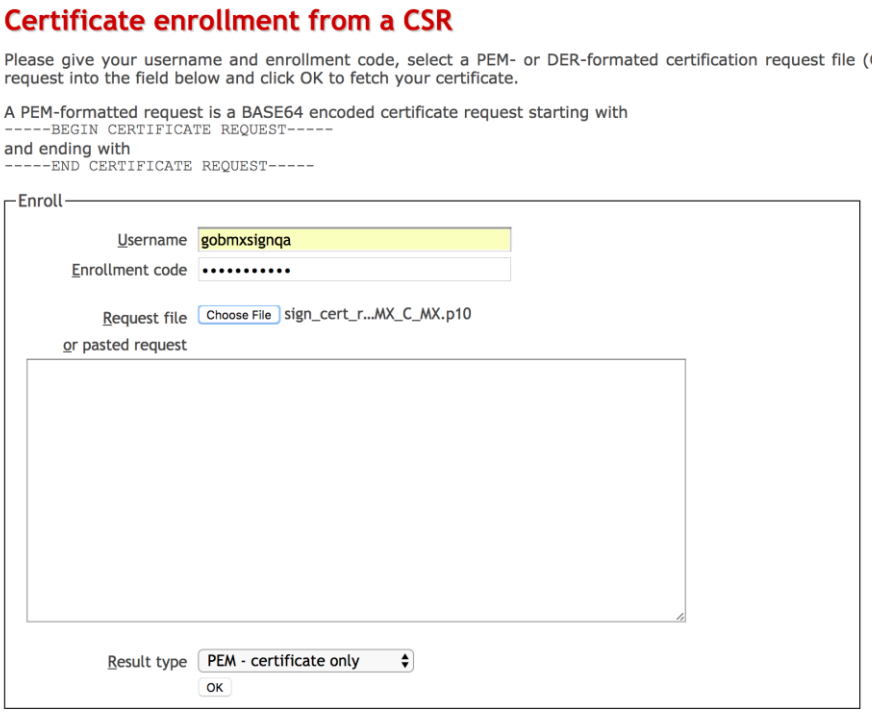
http://10.20.37.221:8080/ejbca/



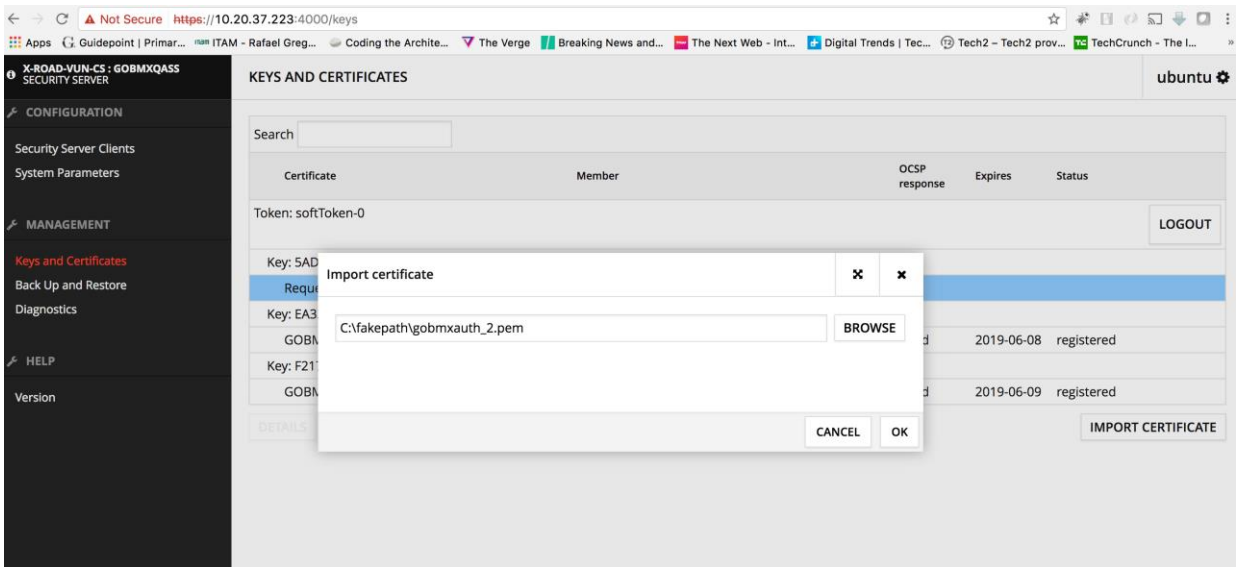
7. En el menú izquiero dar click en la opción de Create certificate from CSR a lo que desplegará la siguiente forma



8. En los campos de Username y Enrollment code poner el username y password de la entidad final correspondiente (gobmxsignqa para certificados sign y gobmxauthqa para certificados auth/ pass letme1n1234). También se debe seleccionar el CSR generado anteriormente en el security server



9. Dar click en Ok, esto deberá generar un certificado en forma PEM firmado con la llave que se generó en el security server
10. En x-road security server vovler a la sección de Keys and Certificates y seleccionar el CSR que se creó. Dar click en IMPORT CERTIFICATE, elegir el certificado que se generó desde la consola pública de EJBCA



11. Al dar click en OK el certificado se importará. Posteriormente después de algunos minutos el x-road security server mandará una solicitud al ocsp de EJBCA para validar la vigencia del certificado a lo cual se debe reportar el status del mismo como good

---

Ligas relacionadas:

https://github.com/GOBMX/xroad-source
https://www.ejbca.org/docs/installation.html
https://www.ejbca.org/docs/installation-ocsp.html