

## Evidencias Interoperabilidad XRoad Julio 2017

**gob.mx**

A large, dark gray triangle occupies the bottom-left portion of the page, pointing towards the bottom-right corner.

## Índice

<b>1</b>	<b>Objetivo. ....</b>	<b>3</b>
<b>2</b>	<b>Evidencias. ....</b>	<b>3</b>

## 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

- 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/>

- En el menú izquierdo acciendo a la opción de Add End Entity



The screenshot shows the EJBCA Administration interface. On the left is a navigation menu with categories: Home, CA Functions, RA Functions (highlighted), Supervision Functions, System Functions, and System Configuration. Under RA Functions, 'Add End Entity' is selected. The main content area displays a welcome message for SuperAdmin, the node hostname (xroad3), and the server time (2017-07-11 22:48:58+00:00). It also features two status tables: 'CA health state' and 'Publish queue status'.

CA Name	CA Service	CRL Status
GOBMX-CA	✓	⚠
ManagementCA	✓	⚠

Publisher	Length
GOBMX-OCSP-PUBLISHER	22

Version : EJBCA 6.2.0 (r19221)  
Using exportable cryptography

Made by PrimeKey Solutions AB, 2002-2014.

3. Deberá aparecer una forma como la siguiente:

The screenshot shows the EJBCA Administration web interface. The browser address bar indicates the URL is https://10.20.37.221:8443/ejbca/adminweb/. The page title is "EJBCA Administration". The left sidebar contains a navigation menu with sections: Home, CA Functions, RA Functions, Supervision Functions, System Functions, and System Configuration. The main content area is titled "Add End Entity". It contains a form with several sections: "End Entity Profile" (with a dropdown menu set to "GOBMX-TSA-EP" and a "Required" checkbox checked), "Username" (with a text input field and a "Required" checkbox checked), "Password (or Enrollment Code)" (with a text input field and a "Required" checkbox checked), "Confirm Password" (with a text input field), "E-mail address" (with a text input field and an "@" symbol), "Subject DN Attributes" (with fields for "CN, Common name", "C, Country (ISO 3166)", "O, Organization", and "serialNumber, Serial number (in DN)", each with a "Required" checkbox checked), and "Main certificate data" (with fields for "Certificate Profile" (set to "GOBMX-TSA"), "CA" (set to "GOBMX-CA"), and "Token" (set to "User Generated"), each with a "Required" checkbox checked). At the bottom of the form are "Add" and "Reset" buttons. The footer of the page states "Made by PrimeKey Solutions AB, 2002-2014."

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 configurar 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 haciendo hover sobre el icono de información en el menú del lado izquierdo de la consola del x-road security server

**X-ROAD-VUN-CS : GOBMXQASS**  
SECURITY SERVER

**SECURITY SERVER CLIENTS** ADD CLIENT ubuntu

Search

Name	ID
gobmx-qa-security-server	MEMBER : x-road-vun-cs : QA-CORE : gobmxqa
gobmx-qa-security-server	SUBSYSTEM : x-road-vun-cs : QA-CORE : gobmxqa : interoperabilidad

**MANAGEMENT**

- Keys and Certificates
- Back Up and Restore
- Diagnostics

**HELP**

- Version

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

Main certificate data	
Certificate Profile	GOBMX-TSA
CA	GOBMX-CA
Token	User Generated
<span>Add</span> <span>Reset</span>	

- Dar click en el botón Add

Búsqueda de entidades de usuario

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

**EJBCA**  
PKI BY PRIMEKEY *Administration*

Home

**CA Functions**

- CA Activation
- CA Structure & CRLs
- Certificate Profiles
- Certification Authorities
- Crypto Tokens
- Publishers

**RA Functions**

- Add End Entity
- End Entity Profiles
- Search End Entities**
- User Data Sources

**Supervision Functions**

- Approve Actions
- View Log

**System Functions**

- Administrator Roles
- Internal Key Bindings
- Services

**System Configuration**

- CMP Configuration
- SCEP Configuration
- System Configuration

**My Preferences**

- Public Web
- Documentation
- Logout

Search end entities with certificates expiring within  Days

Select	Username	CA	CN	OU	O (organization)	Status	
<input type="checkbox"/>	gobmxauth	GOBMX-CA	gobmxss		GOBMX	New	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>
<input type="checkbox"/>	gobmxauthqa	GOBMX-CA	gobmxqa		GOBMX	Generated	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>
<input type="checkbox"/>	gobmxauthqaamazon	GOBMX-CA	gobmxqa		GOBMX	Generated	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>
<input type="checkbox"/>	gobmxocsp	GOBMX-CA	gobmxss			New	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>
<input type="checkbox"/>	gobmxsign	GOBMX-CA	gobmxss		GOBMX	New	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>
<input type="checkbox"/>	gobmxsignqa	GOBMX-CA	gobmxqa		GOBMX	Generated	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>
<input type="checkbox"/>	gobmxsignqaamazon	GOBMX-CA	gobmxqa		GOBMX	Generated	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>

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

Search end entity with username

Search end entity with Certificate SN (hex)

Search end entities with status

Search end entities with certificates expiring within  Days

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

Select	Username	CA	CN	OU	O (organization)	Status	
<input type="checkbox"/>	gobmxauth	GOBMX-CA	gobmxss		GOBMX	New	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>
<input type="checkbox"/>	gobmxauthqa	GOBMX-CA	gobmxqa		GOBMX	Generated	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>
<input type="checkbox"/>	gobmxauthqaamazon	GOBMX-CA	gobmxqa		GOBMX	Generated	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>
<input type="checkbox"/>	gobmxocsp	GOBMX-CA	gobmxss			New	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>
<input type="checkbox"/>	gobmxsign	GOBMX-CA	gobmxss		GOBMX	New	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>
<input type="checkbox"/>	gobmxsignqa	GOBMX-CA	gobmxqa		GOBMX	Generated	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>
<input type="checkbox"/>	gobmxsignqaamazon	GOBMX-CA	gobmxqa		GOBMX	Generated	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>

## 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 correspondiente a esa entidad final

Search end entities with certificates expiring within  Days

Select	Username	CA	CN	OU	O (organization)	Status	
<input type="checkbox"/>	gobmxauth	GOBMX-CA	gobmxss		GOBMX	New	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>
<input type="checkbox"/>	gobmxauthqa	GOBMX-CA	gobmxqa		GOBMX	Generated	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>
<input type="checkbox"/>	gobmxauthqaamazon	GOBMX-CA	gobmxqa		GOBMX	Generated	<a href="#">View End Entity</a> <a href="#">Edit End Entity</a> <a href="#">View Certificates</a> <a href="#">View History</a>

### Edit End Entity

<b>End Entity Profile</b>	GOBMX-AUTH-EP	Required
Status	Generated <input type="button" value="Save"/>	
<b>Username</b>	gobmxauthqaamazon	<input checked="" type="checkbox"/>
Password (or Enrollment Code)	<input type="text"/>	<input checked="" type="checkbox"/>
Confirm Password	<input type="text"/>	
Maximum number of failed login attempts	<input type="radio"/> <input type="text"/> <input checked="" type="radio"/> Unlimited	
Remaining login attempts	<input type="text"/> <input type="checkbox"/> Reset login attempts	
E-mail address	<input type="text"/> @ <input type="text"/>	<input type="checkbox"/>
<b>Subject DN</b>		
CN, Common name	gobmxqa	<input checked="" type="checkbox"/>
C, Country (ISO 3166)	MX	<input type="checkbox"/>
O, Organization	GOBMX	<input type="checkbox"/>
serialNumber, Serial number (in DN)	x-road-vun-cs/gobmxqass-amazon/QA-CORE	<input type="checkbox"/>
<b>Main certificate data</b>		
Certificate Profile	GOBMX-AUTH <input type="button" value="↓"/>	<input checked="" type="checkbox"/>
CA	GOBMX-CA <input type="button" value="↓"/>	<input checked="" type="checkbox"/>
Token	User Generated <input type="button" value="↓"/>	<input checked="" type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>		

- 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

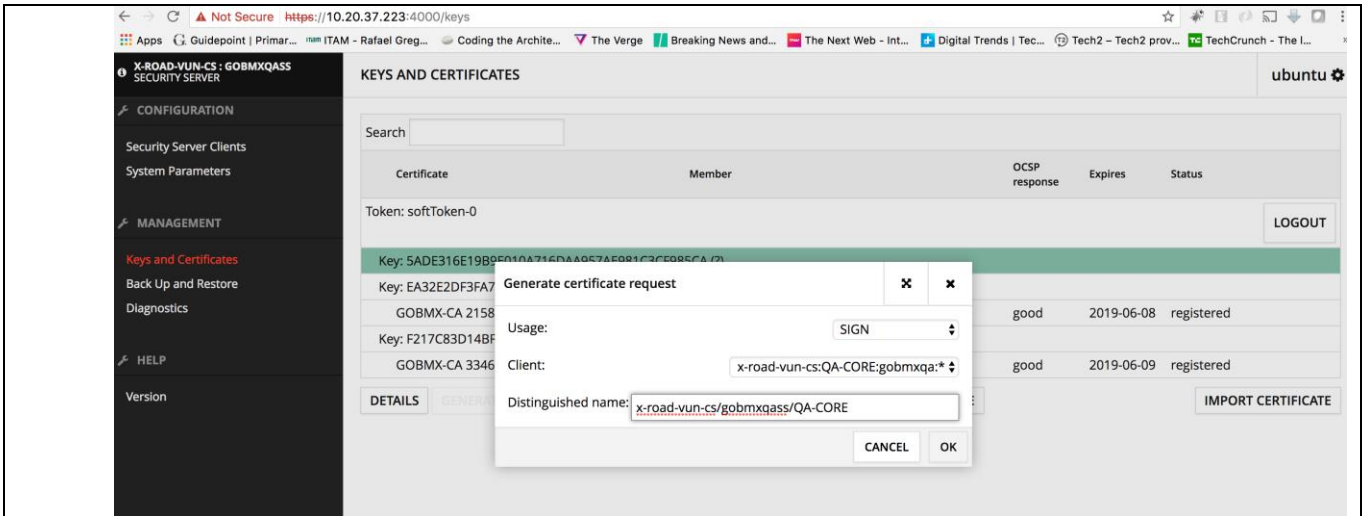
### EJBCA/X-Road

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

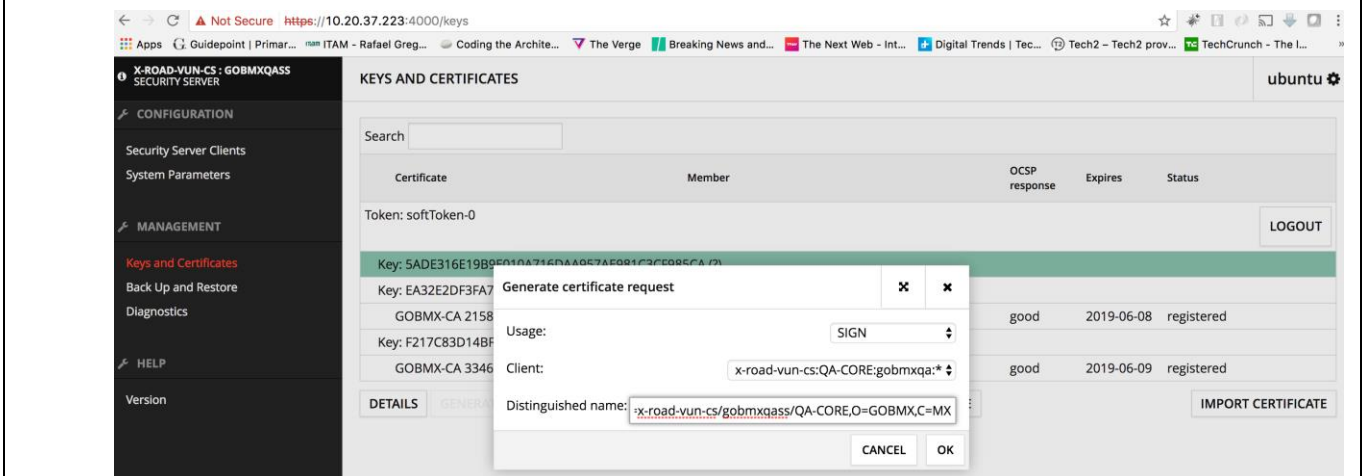
3. Teniendo seleccionada la nueva llave dar click en GENERATE CERTIFICATE REQUEST a lo que desplegará la siguiente forma



- En el campo Distinguished Name se deberá poner una nomenclatura similar a la cadena de serial number que se puso 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



- 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
- Ahora se debe de proceder a acceder a liga de la consola pública de EJBCA

<http://10.20.37.221:8080/ejbca/>

**EJBCA**  
PKI BY PRIMEKEY

**Enroll**

- Create Browser Certificate
- Create Certificate from CSR
- Create Keystore
- Create CV certificate

**Register**

- Request Registration

**Retrieve**

- Fetch CA Certificates
- Fetch CA CRLs
- List User's Certificates
- Fetch User's Latest Certificate

**Inspect**

- Inspect certificate/CSR
- Check Certificate Status

**Miscellaneous**

- Administration
- Documentation

**Welcome to the public EJBCA pages**

**Enroll**

- Create Browser Certificate - Install a certificate in your web browser. This certificate may be exportable depending on browser and browser settings.
- Create Certificate from CSR - Send a PKCS#10 certificate request generated by your server, and receive a certificate that can be installed on the server. Consult your server documentation.
- Create Keystore - Create a server generated keystore in PEM, PKCS#12 or JKS format and save to your disc. This keystore can be installed in a server, browser or in other applications.
- Create CV Certificate - Used for EU EAC ePassport PKI. Send a CVC certificate request generated by an Inspection System, and receive a CV certificate. Note: this can not be used for regular certificates, CV certificates are completely different.

**Retrieve**

- Fetch CA Certificates - Browse and download CA certificates.
- Fetch CA CRLs - Download Certificate Revocation Lists.
- Fetch User's Latest Certificate - Download the last issued certificate for a user for whom you know the certificate Distinguished Name.

**Inspect**

- Inspect certificate/CSR - Inspect a dump of a CSR or a certificate. This gives an output of a CVC or ASN.1 dump, suitable for technical inspection and debugging.

**Miscellaneous**

- List User's Certificates - List certificates for a user for whom you know the certificate Distinguished Name.

- En el menú izquierdo dar click en la opción de Create certificate from CSR a lo que desplegará la siguiente forma

**Certificate enrollment from a CSR**

Please give your username and enrollment code, select a PEM- or DER-formatted certification request file (CSR) for upload, or paste a PEM-formatted request into the field below and click OK to fetch your certificate.

A PEM-formatted request is a BASE64 encoded certificate request starting with  
-----BEGIN CERTIFICATE REQUEST-----  
and ending with  
-----END CERTIFICATE REQUEST-----

**Enroll**

Username

Enrollment code

Request file  No file chosen

or pasted request

Result type

- 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

## Certificate enrollment from a CSR

Please give your username and enrollment code, select a PEM- or DER-formatted certification request file (CSR) for upload, or paste a PEM-formatted request into the field below and click OK to fetch your certificate.

A PEM-formatted request is a BASE64 encoded certificate request starting with

-----BEGIN CERTIFICATE REQUEST-----

and ending with

-----END CERTIFICATE REQUEST-----

Enroll

Username

gobmxsignqa

Enrollment code

.....

Request file

Choose File

sign\_cert\_r...MX\_C\_MX.p10

or pasted request

Result type

PEM - certificate only

OK

- Dar click en Ok, esto deberá generar un certificado en forma PEM firmado con la llave que se generó en el security server
- En x-road security server volver 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

The screenshot shows the X-Road Security Server interface. The left sidebar contains navigation links: CONFIGURATION, Security Server Clients, System Parameters, MANAGEMENT, Keys and Certificates (highlighted), Back Up and Restore, Diagnostics, HELP, and Version. The main content area is titled 'KEYS AND CERTIFICATES' and features a search bar and a table of certificates. A modal window titled 'Import certificate' is open, displaying a file path 'C:\fakepath\gobmxauth\_2.pem' and a 'BROWSE' button. The table in the background has columns for Certificate, Member, OSCP response, Expires, and Status, with rows showing certificates for '2019-06-08' and '2019-06-09'.

11. Al dar click en OK el certificado se importará. Posteriormente después de algunos minutos el x-road security server mandará una solicitud al ocsf 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>