

Ventanilla Única Nacional
Componentes de Interoperabilidad
Configuración Security Server
VUN.X-ROAD v6.7
Versión 1.0.2

gob.mx

Índice

Contenido

1. INTEGRACIÓN	4
1.1 OBJETIVO DEL DOCUMENTO.....	4
2. ASPECTOS REQUERIDOS DE SISTEMA OPERATIVO	4
3. PUERTOS REQUERIDOS	4
3.1 CONSIDERACIONES ADICIONALES DE PUERTOS DESPUÉS DE INSTALACIÓN DE SS	4
4. IP PÚBLICA	4
5. SOLICITUD DEL ARCHIVO ANCLA AL COMITÉ DE INTEROPERABILIDAD DE VUN.....	4
6. IMPORTACIÓN DEL ARCHIVO ANCLA SOBRE EL NODO DE SS-XROAD	5
7. CONFIGURACIÓN DEL SS-XROAD	7
8. GENERACIÓN DE LOS CERTIFICADOS	11
9. SOLICITUD DEL ENROLAMIENTO DE LOS CERTIFICADOS AL COMITÉ DE INTEROPERABILIDAD	13
10. IMPORTACIÓN DE LOS CERTIFICADOS FIRMADOS EN EL SS-XROAD	14
11. CONFIGURACIÓN DEL TSA EN EL SS-XROAD	17
12. MONITOREO DE LOS SEMÁFOROS DEL OCSP Y TSA, DESDE EL SS-XROAD	19
13. SOLICITUD DE REGISTRO DEL SS-INSTITUCIÓN EN EL CS-GOB.MX	19
14. PRUEBA DEL SERVICIO DE IOPTRAZABILIDADXROAD DESDE EL SS-XROAD UTILIZANDO LA IP-PUBLICA Y IP-INTERNA.....	20
15. PAYLOAD IOPTRAZABILIDADXROAD → CONSULTARESTATUSTRAMITE (REQUEST,RESPONSE)	22

Colaboradores

Ítem	Nombres y Apellido	Oficina
1.	Jorge Sepúlveda	GOBMX
2.	Viviana Cano	GOBMX
3.	Jaime Benavides	GOBMX
4.	Ricardo Lona	GOBMX
5.	Arturo Silva	GOBMX
6.	Vanessa Vega	GOBMX

1. Integración

1.1 Objetivo del documento

El objetivo del presente documento es describir la configuración de un nuevo nodo de Security Server (SS) VUN.XROAD v6.7 sobre Ubuntu 14.04.5 Server TLS y anclado al Central Server de GOB.MX.

2. Aspectos requeridos de Sistema Operativo

SO	Descripción
Ubuntu Server 14.04.5 TLS	http://releases.ubuntu.com/14.04.5/ubuntu-14.04.5-server-amd64.iso
Usuario	Se debe crear el usuario xroad para la instalación y configuración del SS, y debe tener los privilegios de sudo.

3. Puertos Requeridos

3.1 Consideraciones adicionales de puertos después de instalación de SS

Ejemplo de validación de puertos: `netstat -a | grep 443`

Tabla 1, Puertos Requeridos para IP-publica

Ítem	Entrada/Salida	Protocol	Source
1.	80	TCP	0.0.0.0/0 ::/0
2.	443	TCP	0.0.0.0/0 ::/0
3.	4000	TCP	0.0.0.0/0 ::/0
4.	4001	TCP	0.0.0.0/0 ::/0
5.	5500	TCP	0.0.0.0/0 ::/0
6.	5577	TCP	0.0.0.0/0 ::/0
7.	22	TCP	0.0.0.0/0 ::/0

4. IP Pública

Es requerido para ese equipo donde se instaló el SS-Institución, debe estar vinculado a una IP-PUBLICA estática.

5. Solicitud del archivo Ancla al Comité de Interoperabilidad de VUN

Se debe solicitar el archivo de configuración del anchor.xml y solicitando la visibilidad de la ip-publica estática de la institución donde se instaló el SS a UGD al correo comiteinteroperabilidadxroad@vun.mx, con copia a los siguientes correos.

1. xx000001x@vun.mx
2. xx000002x@vun.mx
3. xx000002x@ugd.gob.mx

6. Importación del Archivo Ancla sobre el Nodo de SS-XRoad

El operador de la institución se autentica con el usuario xroad en su SS.

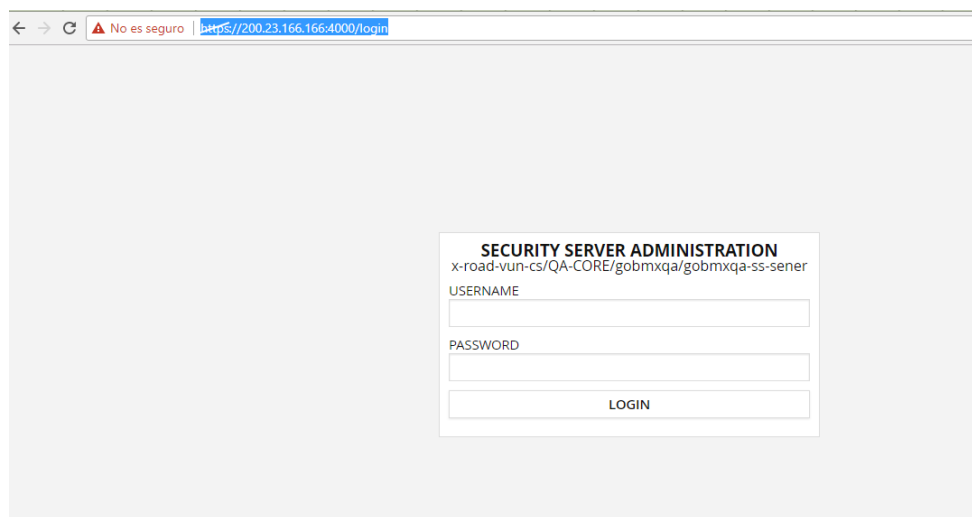


Ilustración 1, Autenticándose con el usuario xroad

Importando el archivo anchor compartido por comité de interoperabilidad de VUN:

[configuration_anchor_x-road-vun-cs_internal.UTC_2017-07-12_22-28-07.xml](#)

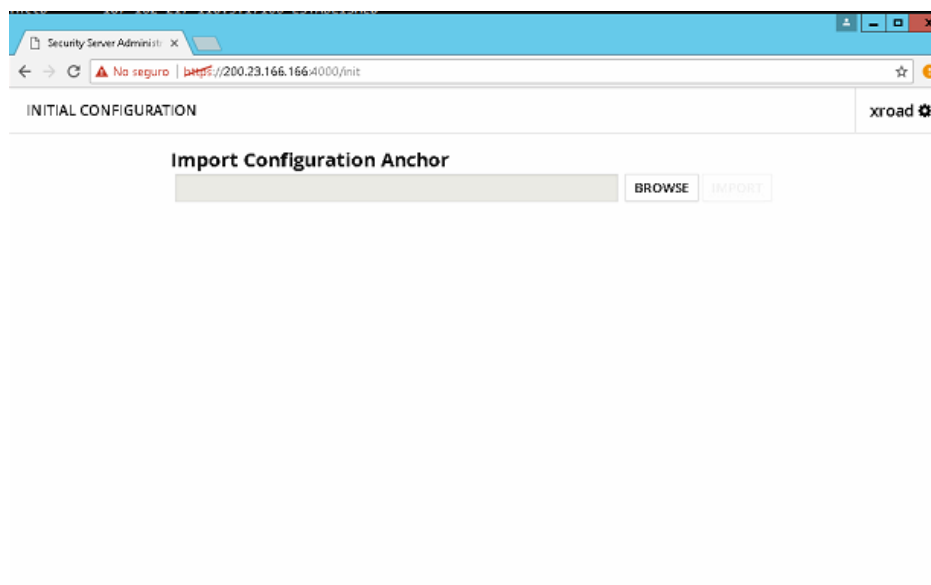


Ilustración 2, El usuario xroad autenticado por primera vez

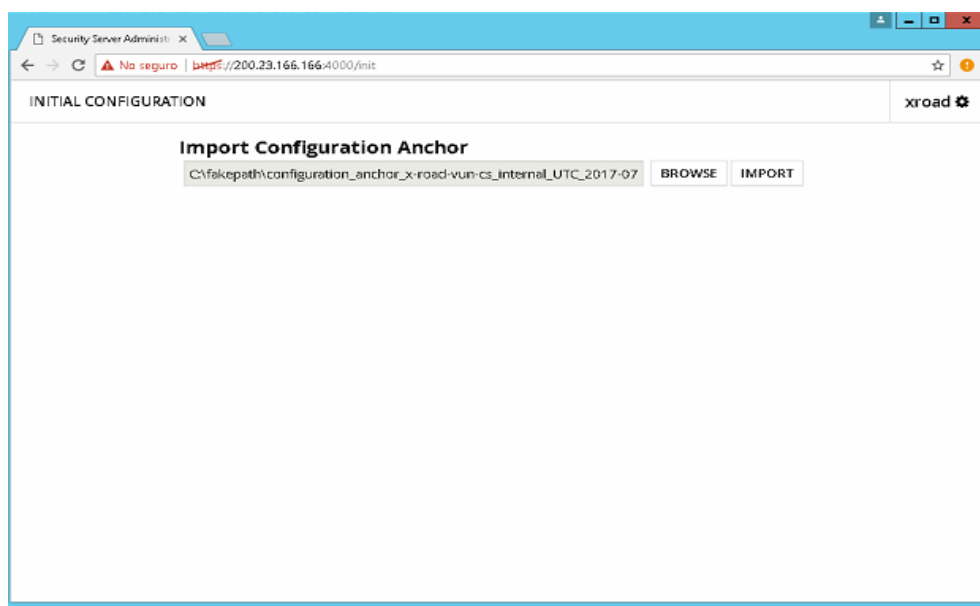


Ilustración 3, Importando el Archivo de ancla

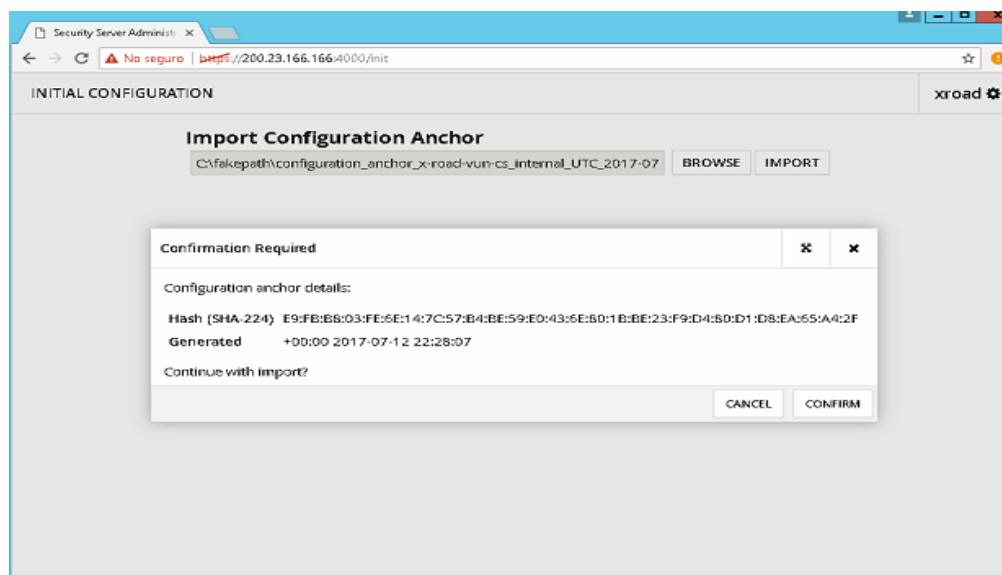


Ilustración 4, Portando el archivo Anchor

7. Configuración del SS-XRoad

Ahora se configura la vinculación del SS-Institución con el SS-GOBMX.

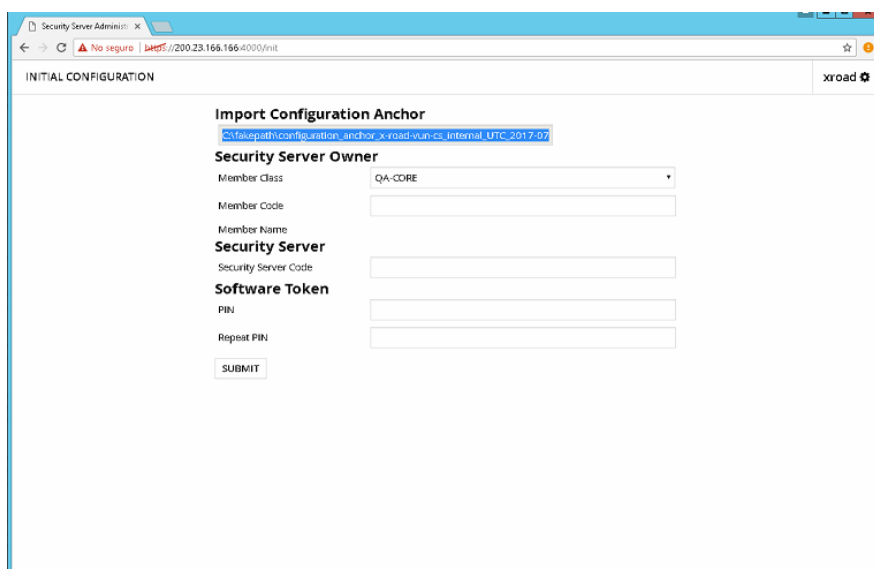


Ilustración 5, Después de cargar el archivo anchor.xml

Member Class: QA-CORE referencia de CS-GOBMX

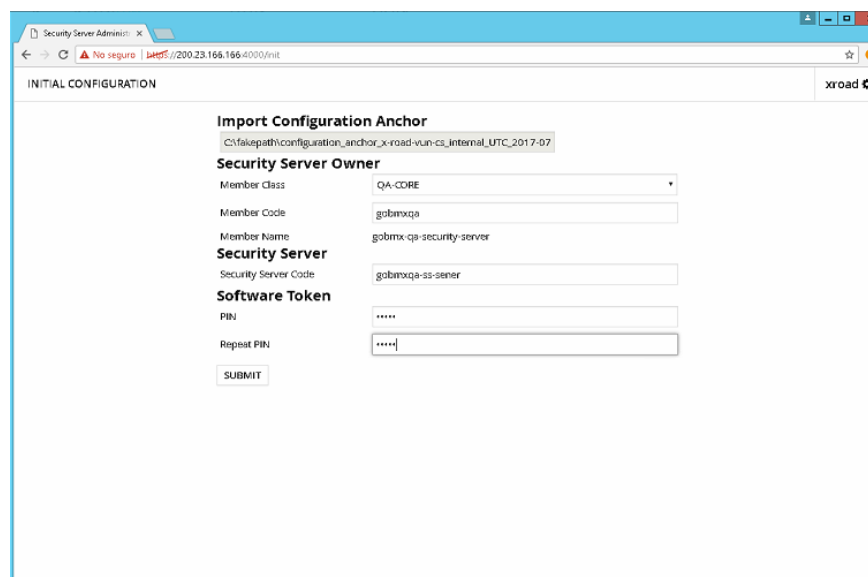
Member Code: gobmxqa → es el SS-GOBMX

Member Name: gobmx-qa-security-server → Nombre del miembro de SS

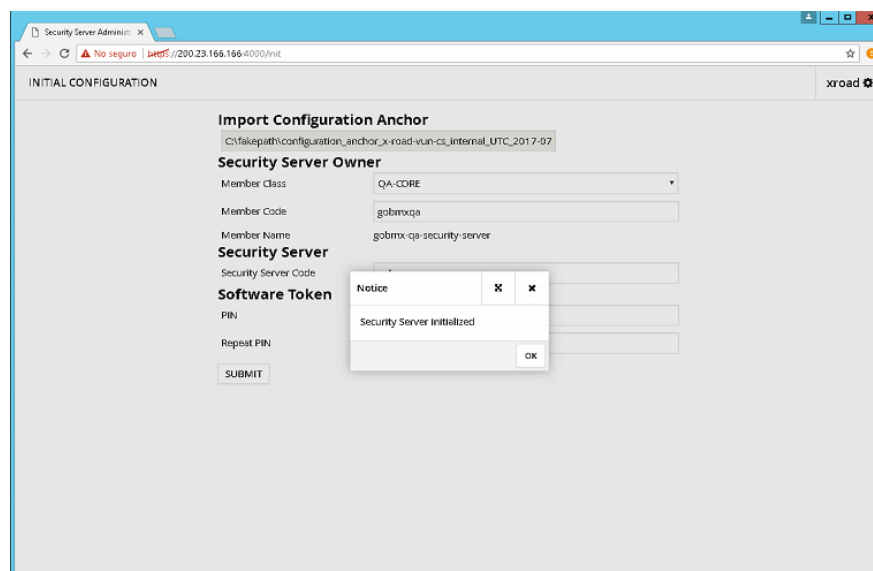
Security Server

Security Server Code: gobmxqa-ss-sener → Referencia del SS-Institución

PIN: un valor alfanumérico.(posteriormente este valor se utiliza para iniciar el SS-Institución).



The screenshot shows the 'Security Server Administration' web interface. The browser address bar indicates a local development environment. The page title is 'INITIAL CONFIGURATION'. The main content area is titled 'Import Configuration Anchor' and shows a file path. Below this, there are sections for 'Security Server Owner', 'Security Server', and 'Software Token'. The 'Security Server Owner' section includes fields for 'Member Class' (QA-CORE), 'Member Code' (gobmxqa), and 'Member Name' (gobmx-qa-security-server). The 'Security Server' section includes a 'Security Server Code' field (gobmxqa-ss-sener). The 'Software Token' section includes 'PIN' and 'Repeat PIN' fields, both containing asterisks. A 'SUBMIT' button is at the bottom.



This screenshot shows the same 'Security Server Administration' web interface as the previous one, but with a 'Notice' dialog box overlaid. The dialog box contains the text 'Security Server Initialized' and an 'OK' button. The background form is slightly dimmed, showing the same configuration fields as before.

Ilustración 6, Configuración Raíz del SS-Institución

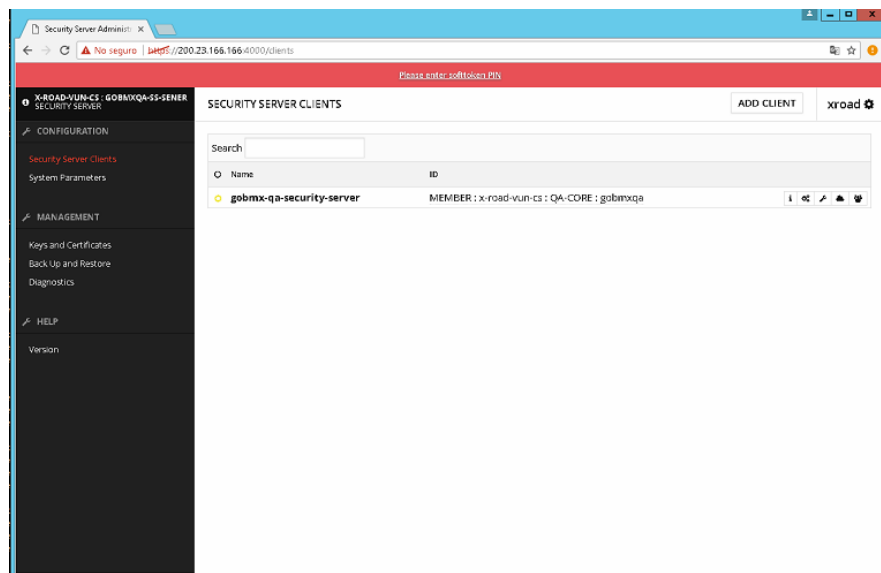


Ilustración 7, Pantalla inicial después de configurar el Anchor

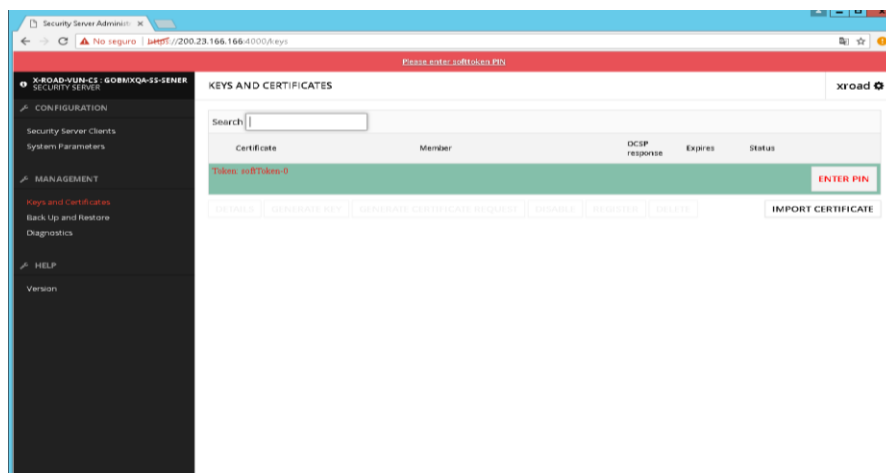


Ilustración 8, Ingresando el PIN

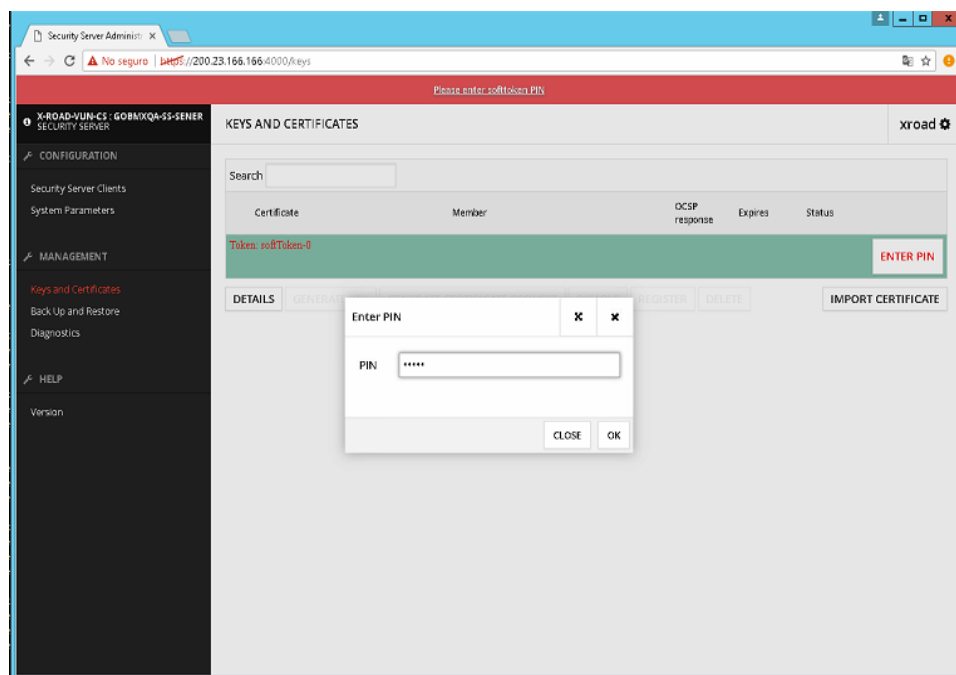


Ilustración 9, Ingresando el PIN

Si todo esta OK, veremos la siguiente ventana lista para generar los certificados.

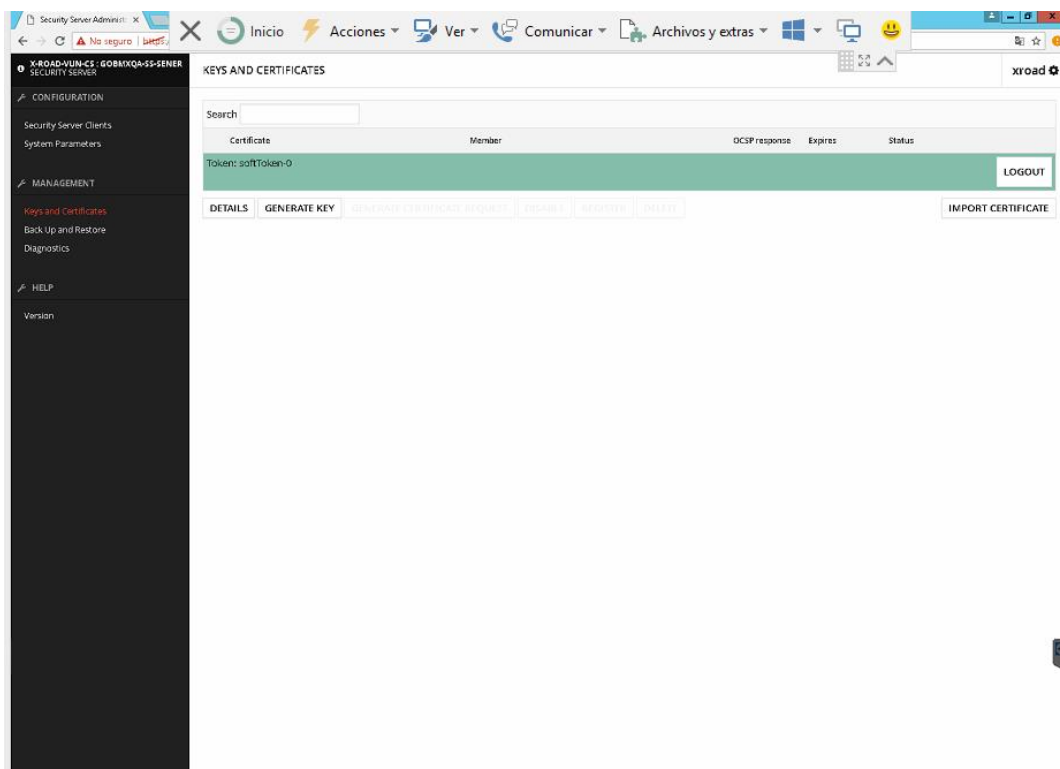


Ilustración 10, PIN Aceptado OK

8. Generación de los Certificados

Nos vamos al menú en **Key and Cetificate** y generamos los certificados de autenticación y uno de firma:

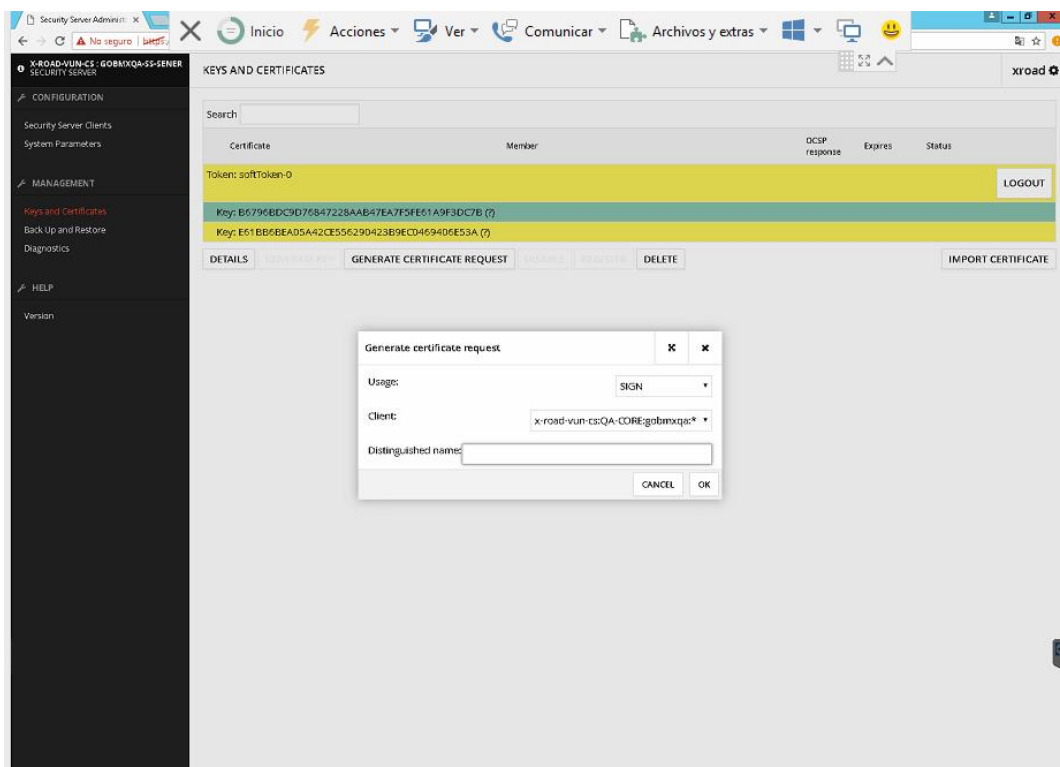


Ilustración 11, Generando el Certificado Request para SIGN

SING: Distinguished name: CN=gobmxqa,SN=x-road-vun-cs/gobmxqa-ss-sener/QA-CORE,O=GOBMX,C=MX

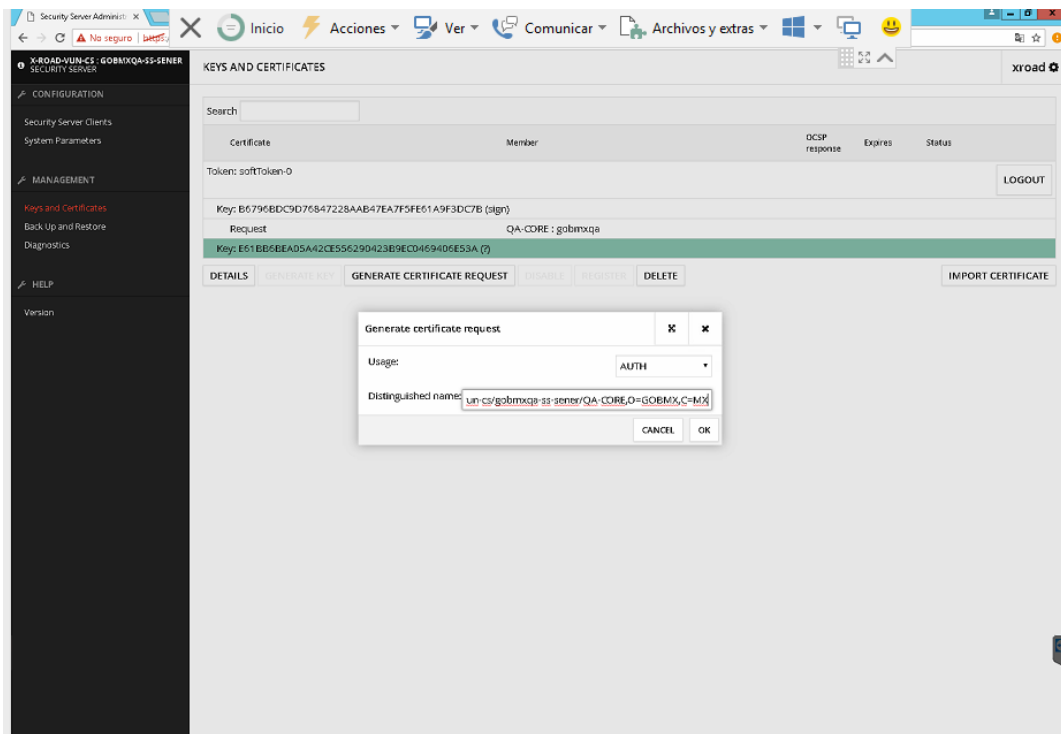


Ilustración 12, Generando el Certificado Request para AUTH

AUTH: Distinguished name: CN=gobmxqa,SN=x-road-vun-cs/gobmxqa-ss-sener/QA-CORE,O=GOBMX,C=MX

NOTA: ambos certificados request generan:

sign_cert_request_20170731_CN_gobmxqa_O_GOBMX_C_MX.p10.

auth_cert_request_20170731_CN_gobmxqa_O_GOBMX_C_MX.p10.

9. Solicitud del enrolamiento de los certificados al comité de Interoperabilidad

La institución una vez generado los certificados request, estos archivos debe enviarlos al comité de interoperabilidad de la VUN y solicitar su enrolamiento, para que sean enrolados y firmados por la CA de GOB.MX.

Este procedimiento genera dos certificados firmados .pem.

Certificado Request	Certificado Firmado
Genera la Institución	Genera la VUN
sign_cert_request_20170731_CN_gobmxqa_O_GOBMX_C_MX.p10	gobmxsignqasener.pem
auth_cert_request_20170731_CN_gobmxqa_O_GOBMX_C_MX.p10	gobmxauthqasener.pem

Luego que el comité de interoperabilidad genere los archivos .pem, son enviados a la institución solicitante

para que continúe con la configuración de su SS-Institución.

10. Importación de los certificados firmados en el SS-XRoad

La institución podrá continuar con la configuración de su SS, importando los certificados firmados .pem, Ir al menú **Keys and Certificates**:

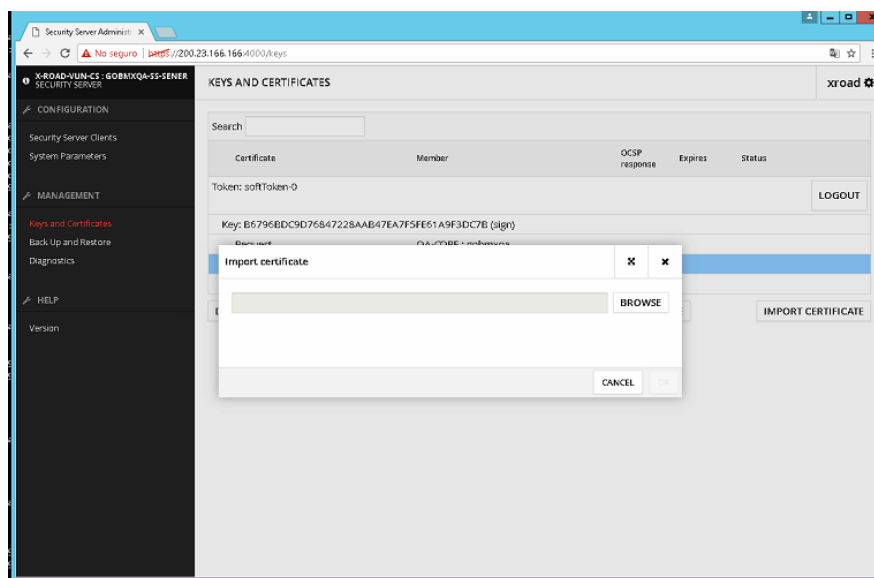


Ilustración 13, Importando los certificados firmados

Ahora primero se importa el certificado de autenticación y luego el de firma.

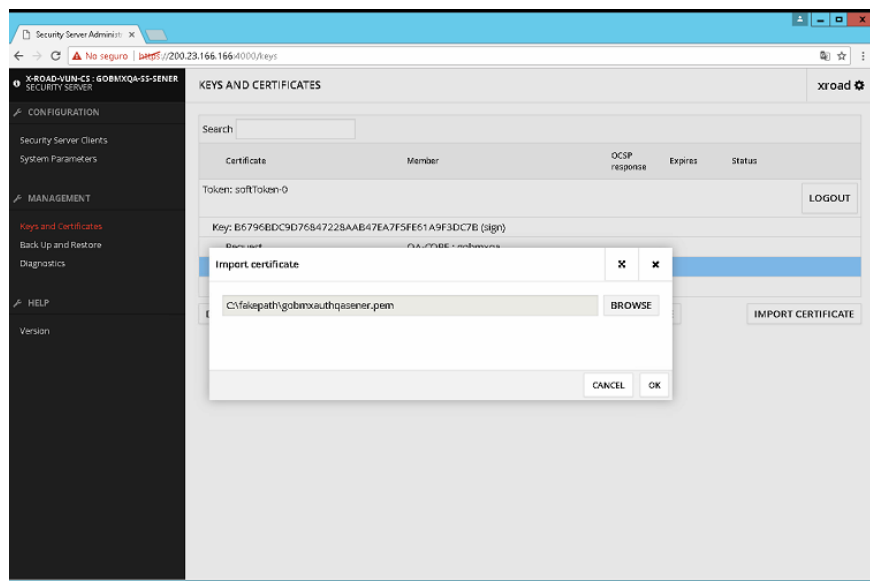


Ilustración 14, Importando Certificados de autenticación

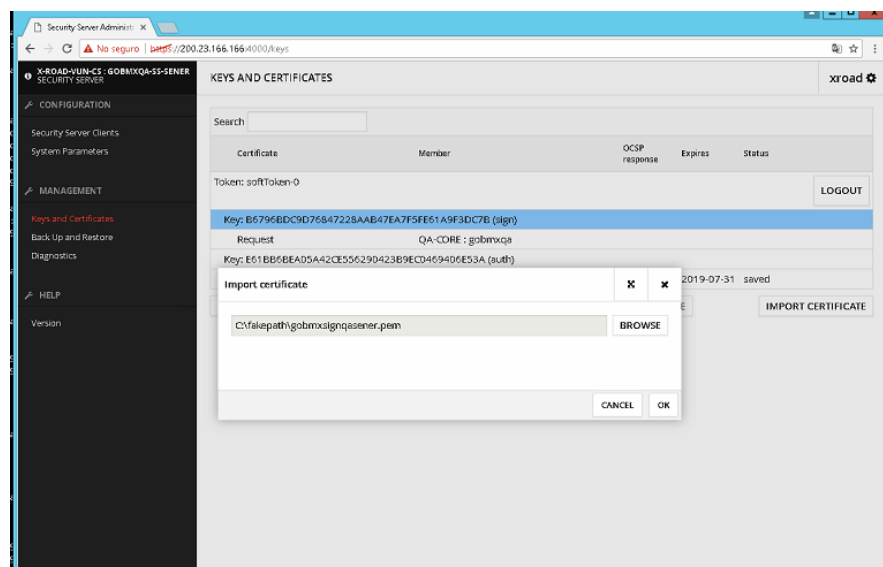


Ilustración 15, Importando el Certificado de Firma

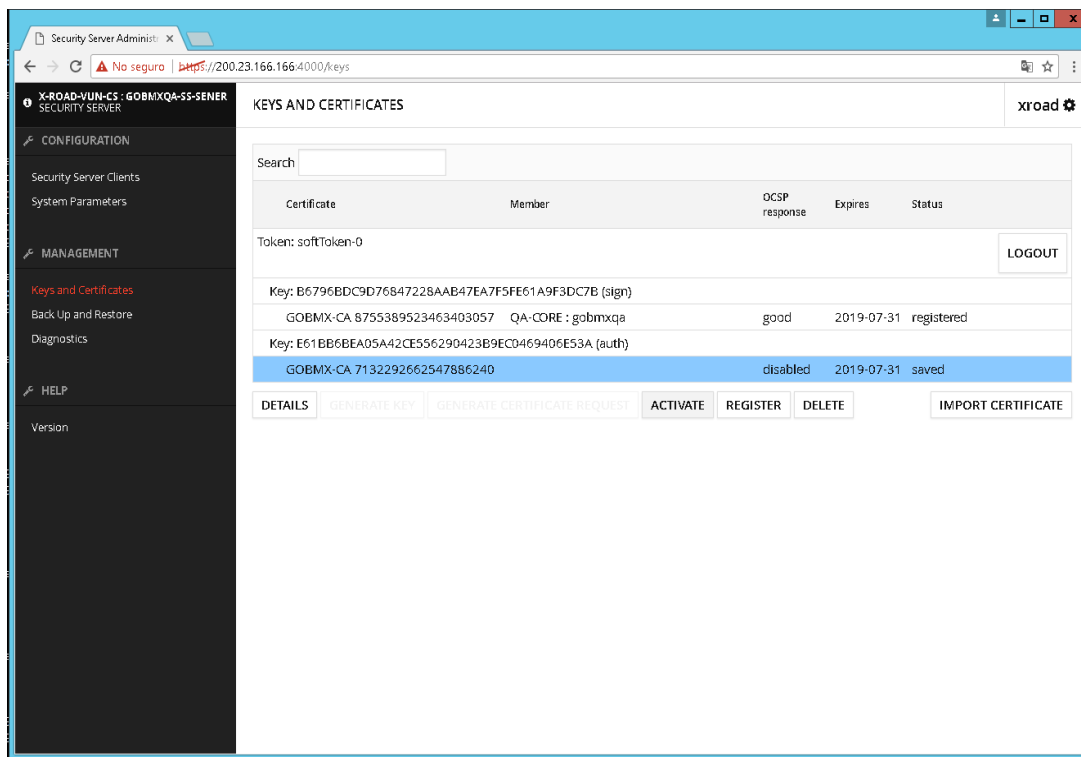


Ilustración 16, Activando el certificado de Autenticación

Y por último se registra el certificado poniendo como parámetro la IP-Pública de la institución que hace referencia a este SS.

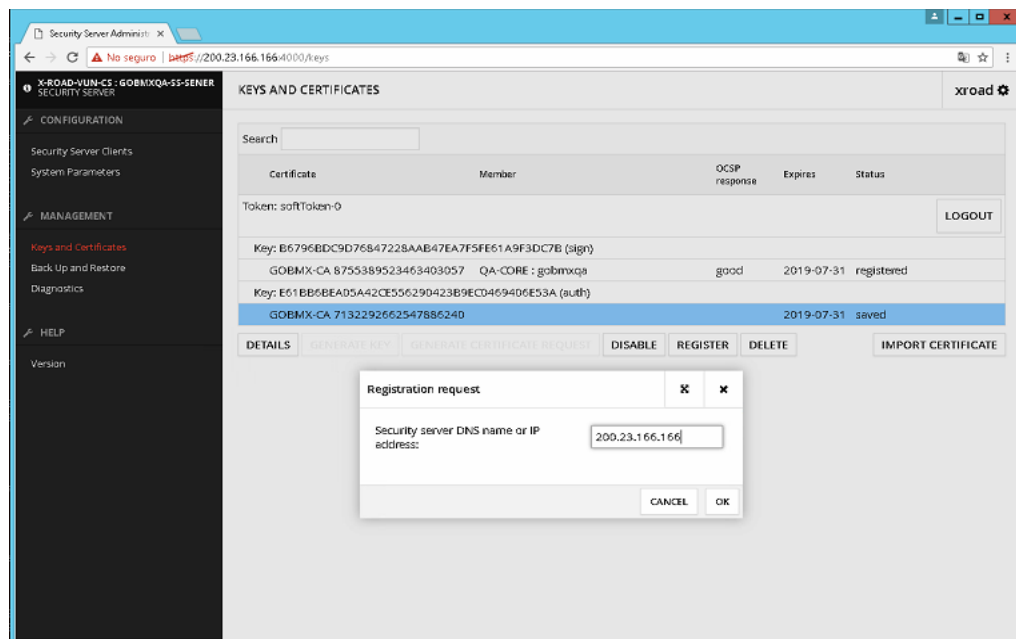


Ilustración 17, Registrando el Certificado de Autenticación con la IP-Pública de la institución

11. Configuración del TSA en el SS-XRoad

Ir a menú de System Parameters, y configurar el TSA.

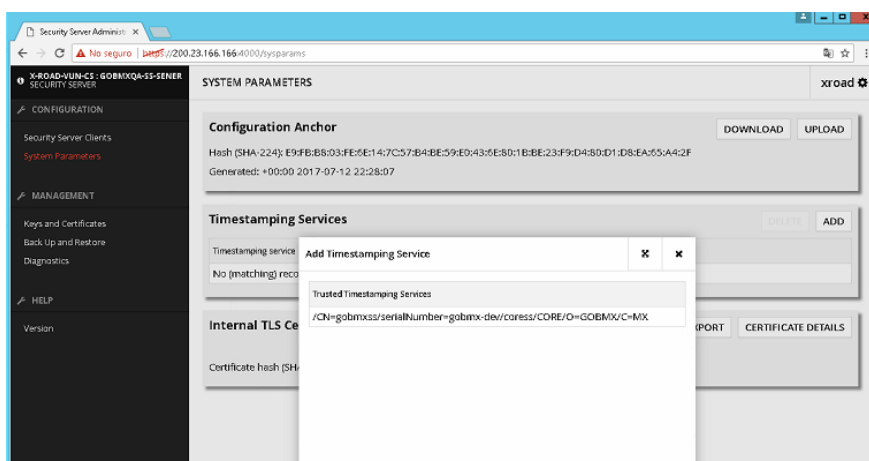


Ilustración 18, Configuración del TSA

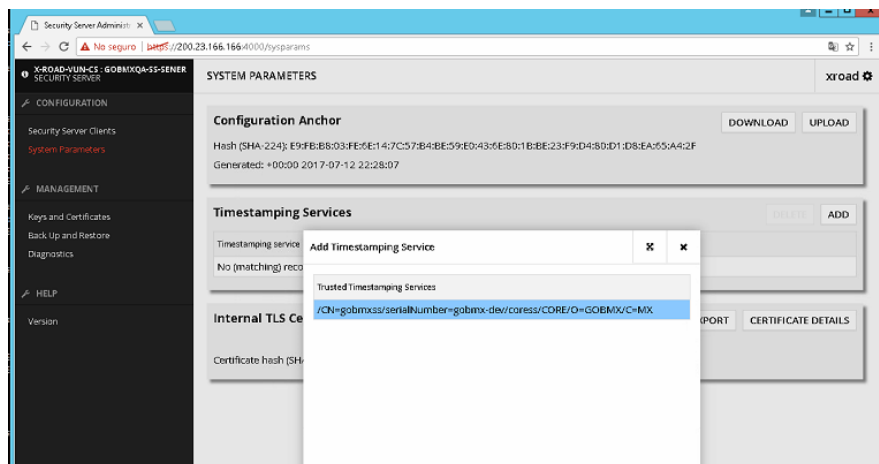


Ilustración 19, Configuración del TSA

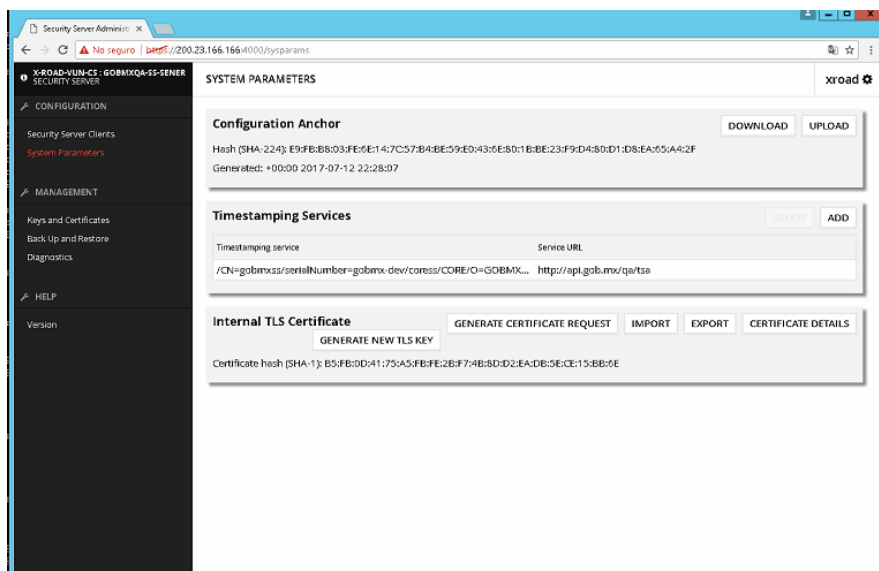


Ilustración 20, TSA configurado en el SS-Institución

12. Monitoreo de los semáforos del OCSP y TSA, desde el SS-XRoad

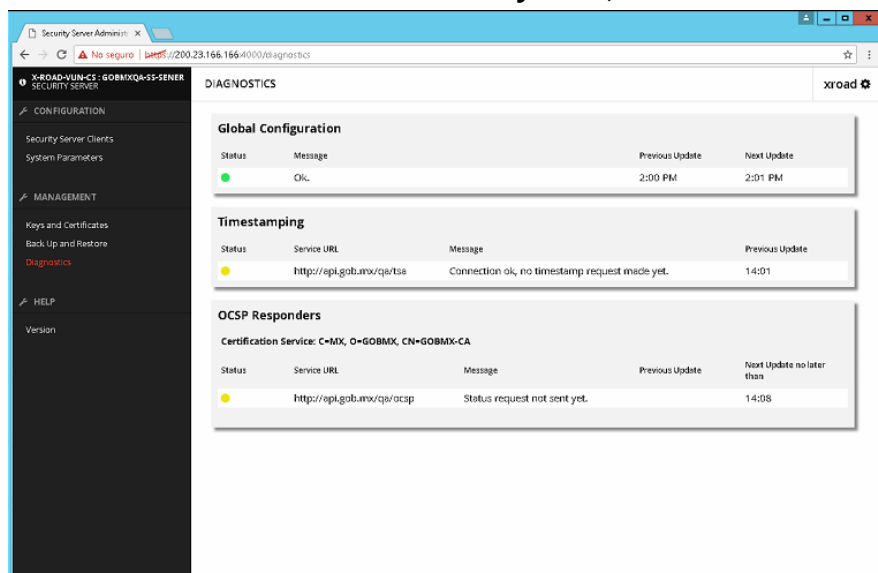


Ilustración 21, Monitoreo de los semáforos configuración global, TSA y OCSP

13. Solicitud de Registro del SS-Institución en el CS-GOB.MX

La institución debe enviar un mail al comited de interoperabilidad solicitando el registro y aprobación del nuevo SS-Institución, y debe enviar el **Security Server Code: gobmxqa-ss-sener** y el archivo de autenticación firmado **gobmxauthqasener.pem**, luego el comité después de registrarlo notificara a la institución que ya está activo y operativo su SS-Institución.

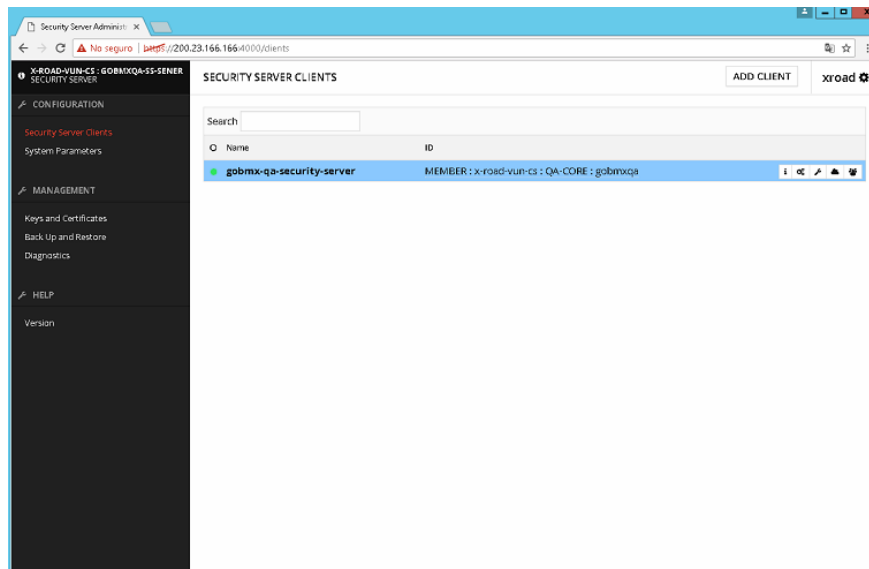


Ilustración 22, SS-Institución Activo

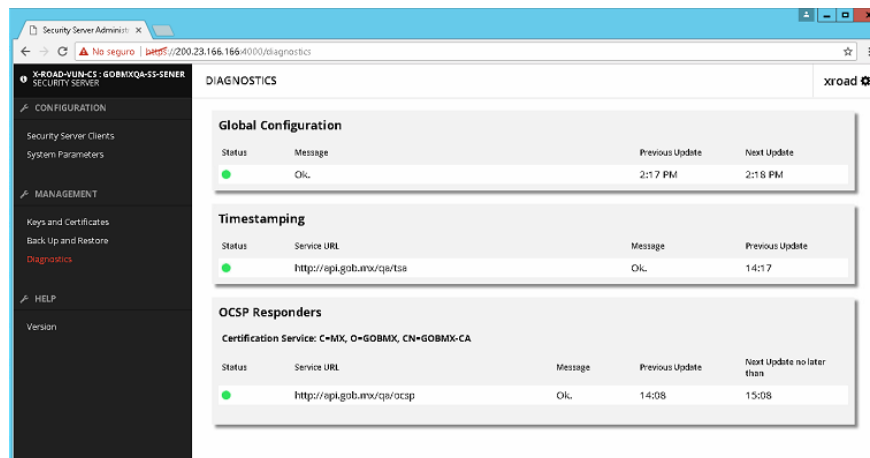


Ilustración 23, Semáforos Configuración Global, TSA y OCSP Ok

Ahora la institución puede operar con el VUN.XRoad.

14. Prueba del Servicio de IOP TrazabilidadXRoad desde el SS-XRoad

utilizando la ip-publica y ip-Interna.

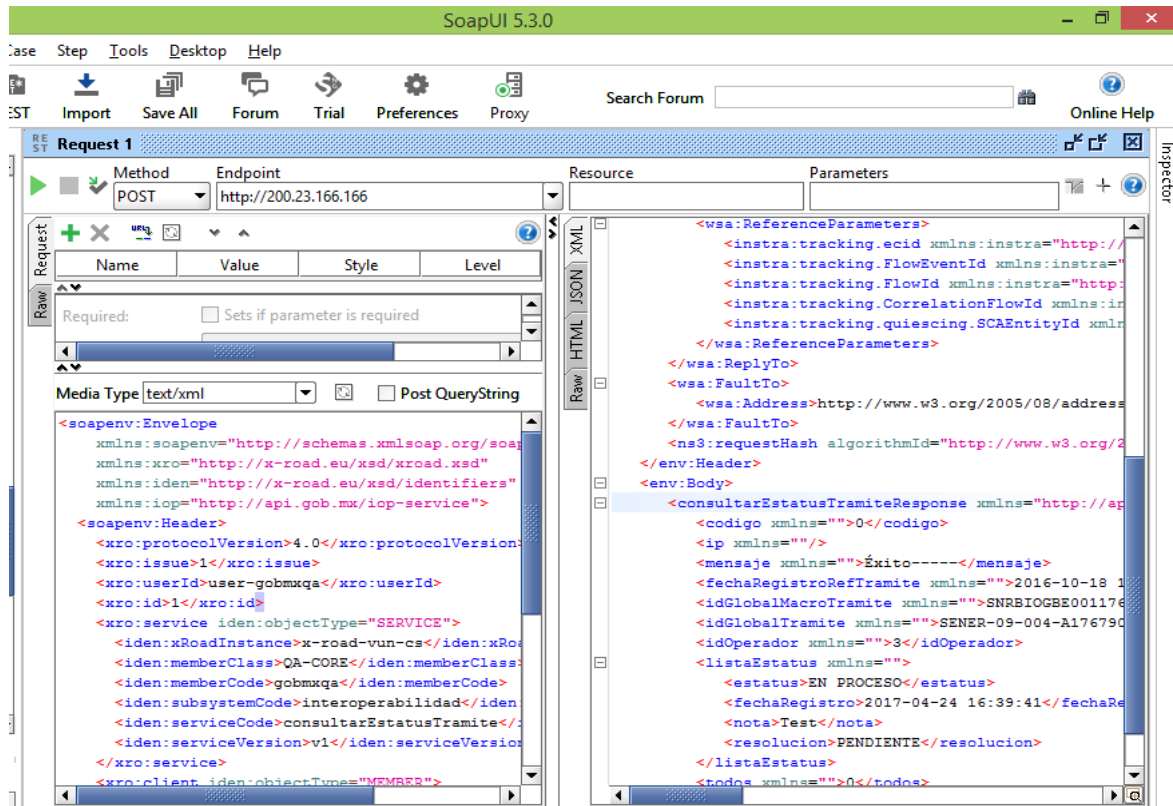


Ilustración 24, Prueba del Servicio de Trazabilidad utilizando la IP-Publica



Método	Consulta el estatus de un Trámite a partir de su IdGlobalTramite
End-Point : Interna	http://192.168.60.3
End-Point : Publico	http://200.23.166.166
Protocolo	WSDL 1.1 y 1.2
Ambiente	VUN-Pre-Productivo
Payload Request – Xroad	
<pre><soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xro="http://x-road.eu/xsd/xroad.xsd" xmlns:iden="http://x-road.eu/xsd/identifiers" xmlns:iop="http://api.gob.mx/iop-service"> <soapenv:Header> <xro:protocolVersion>4.0</xro:protocolVersion> <xro:issue>1</xro:issue></pre>	

```

<xro:userId>user-gobmxqa</xro:userId>
<xro:id>1</xro:id>
<xro:service iden:objectType="SERVICE">
  <iden:xRoadInstance>x-road-vun-cs</iden:xRoadInstance>
  <iden:memberClass>QA-CORE</iden:memberClass>
  <iden:memberCode>gobmxqa</iden:memberCode>
  <iden:subsystemCode>interoperabilidad</iden:subsystemCode>
  <iden:serviceCode>consultarEstatusTramite</iden:serviceCode>
  <iden:serviceVersion>v1</iden:serviceVersion>
</xro:service>
<xro:client iden:objectType="MEMBER">
  <iden:xRoadInstance>x-road-vun-cs</iden:xRoadInstance>
  <iden:memberClass>QA-CORE</iden:memberClass>
  <iden:memberCode>gobmxqa</iden:memberCode>
</xro:client>
</soapenv:Header>
<soapenv:Body>
  <iop:consultarEstatusTramiteRequest>
    <idGlobalTramite>SENER-09-004-A17679000000022</idGlobalTramite>
    <todos>0</todos>
    <idOperador>3</idOperador>
    <ip>127.0.0.1</ip>
  </iop:consultarEstatusTramiteRequest>
</soapenv:Body>
</soapenv:Envelope>

```

Payload Response – XRoad

```

<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing">
  <env:Header>
    <xro:client iden:objectType="MEMBER" xmlns:iden="http://x-road.eu/xsd/identifiers"
xmlns:iop="http://api.gob.mx/iop-service" xmlns:xro="http://x-road.eu/xsd/xroad.xsd">
      <iden:xRoadInstance>x-road-vun-cs</iden:xRoadInstance>
      <iden:memberClass>QA-CORE</iden:memberClass>
      <iden:memberCode>gobmxqa</iden:memberCode>
    </xro:client>
    <xro:service iden:objectType="SERVICE" xmlns:iden="http://x-road.eu/xsd/identifiers"
xmlns:iop="http://api.gob.mx/iop-service" xmlns:xro="http://x-road.eu/xsd/xroad.xsd">
      <iden:xRoadInstance>x-road-vun-cs</iden:xRoadInstance>
      <iden:memberClass>QA-CORE</iden:memberClass>
      <iden:memberCode>gobmxqa</iden:memberCode>
      <iden:subsystemCode>interoperabilidad</iden:subsystemCode>
      <iden:serviceCode>consultarEstatusTramite</iden:serviceCode>
      <iden:serviceVersion>v1</iden:serviceVersion>
    </xro:service>
    <xro:id xmlns:iden="http://x-road.eu/xsd/identifiers" xmlns:iop="http://api.gob.mx/iop-service"
xmlns:xro="http://x-road.eu/xsd/xroad.xsd">1</xro:id>

```

```

<xro:userId xmlns:iden="http://x-road.eu/xsd/identifiers" xmlns:iop="http://api.gob.mx/iop-service"
xmlns:xro="http://x-road.eu/xsd/xroad.xsd">user-gobmxqa</xro:userId>
<xro:issue xmlns:iden="http://x-road.eu/xsd/identifiers" xmlns:iop="http://api.gob.mx/iop-service"
xmlns:xro="http://x-road.eu/xsd/xroad.xsd">1</xro:issue>
<xro:protocolVersion xmlns:iden="http://x-road.eu/xsd/identifiers" xmlns:iop="http://api.gob.mx/iop-
service" xmlns:xro="http://x-road.eu/xsd/xroad.xsd">4.0</xro:protocolVersion>
<wsa:MessageID>urn:eb3d9069-7624-11e7-a0c6-00144ffa98a4</wsa:MessageID>
<wsa:ReplyTo>
<wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
<wsa:ReferenceParameters>
<instra:tracking.ecid
xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">MEjJp1IZ000000000</instra:tracking.ecid>
<instra:tracking.FlowEventId
xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">558214</instra:tracking.FlowEventId>
<instra:tracking.FlowId
xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">366631</instra:tracking.FlowId>
<instra:tracking.CorrelationFlowId
xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">0000LqQ5HOUF^6O_yhw0yW1PMying0001be</instr
a:tracking.CorrelationFlowId>
<instra:tracking.quiescing.SCAEntityId
xmlns:instra="http://xmlns.oracle.com/sca/tracking/1.0">50042</instra:tracking.quiescing.SCAEntityId>
</wsa:ReferenceParameters>
</wsa:ReplyTo>
<wsa:FaultTo>
<wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
</wsa:FaultTo>
<ns3:requestHash algorithmId="http://www.w3.org/2001/04/xmlenc#sha512" xmlns:ns3="http://x-
road.eu/xsd/xroad.xsd">FSMUOmHJoqMcIXw9orG7mWnxkzYKQG6qEesyoY1JbdM/AyWNiLpLAmwpVN
ZD2+cQLVdrLaPtddRfNBdFCbEB2A==</ns3:requestHash>
</env:Header>
<env:Body>
<consultarEstatusTramiteResponse xmlns="http://api.gob.mx/iop-service">
<codigo xmlns="">0</codigo>
<ip xmlns=""/>
<mensaje xmlns="">Éxito----</mensaje>
<fechaRegistroRefTramite xmlns="">2016-10-18 14:10:51</fechaRegistroRefTramite>
<idGlobalMacroTramite xmlns="">SNRBIOGBE00117679000000022</idGlobalMacroTramite>
<idGlobalTramite xmlns="">SENER-09-004-A17679000000022</idGlobalTramite>
<idOperador xmlns="">3</idOperador>
<listaEstatus xmlns="">
<estatus>EN PROCESO</estatus>
<fechaRegistro>2017-04-24 16:39:41</fechaRegistro>
<nota>Test</nota>
<resolucion>PENDIENTE</resolucion>
</listaEstatus>
<todos xmlns="">0</todos>

```



```
</consultarEstatusTramiteResponse>  
</env:Body>  
</env:Envelope>
```