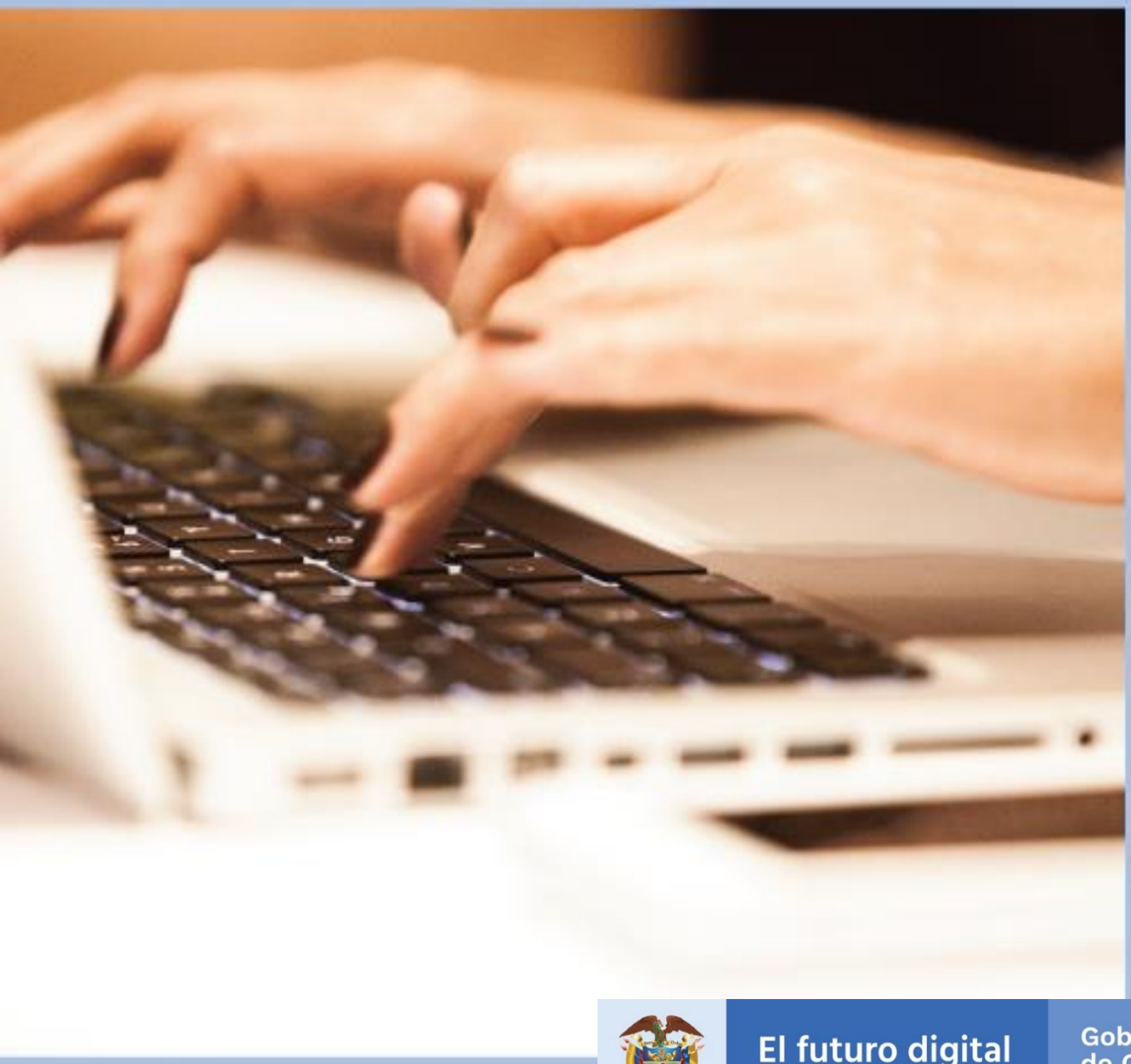


El futuro digital es de todos

Gobierno de Colombia
MinTIC

Guía Despliegue Servidor de Seguridad Plataforma de Interoperabilidad

CONTROL DE VERSIONES

Versión	Fecha de aprobación	Descripción
1.0	11/06/2019	Documento para despliegue Ambientes de Desarrollo
1.1	10/12/2019	Alineación con el Marco de interoperabilidad

1 INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), de acuerdo con la Ley 1341 de 2009, desarrolla políticas y planes enfocados a las Tecnologías de la Información y las Comunicaciones que constituyen un componente vital para el crecimiento y desarrollo del sector, con el fin de brindar acceso a toda la población, en el marco de la expansión y diversificación de las TIC.

En consecuencia, MinTIC ha establecido la necesidad de garantizar la transformación digital de los trámites y servicios mediante el modelo de los Servicios Ciudadanos Digitales (SCD), para enfrentar los retos que imponen los entornos digitales entre ellos:

a) Interoperabilidad, mejorando las condiciones de intercambio de información.
b) Autenticación Digital, mitigando los riesgos en la suplantación de la identidad y transformando al Estado colombiano para que funcione como una sola institución que le brinde a los ciudadanos información oportuna, trámites ágiles y mejores servicios. Las entidades públicas deben estar interconectadas y operar de manera articulada como un único gran sistema.
c) Carpeta Ciudadana Digital, permitiendo la visualización de los datos que las entidades públicas tienen de cada ciudadano o empresa.

De otra parte, la Agencia Nacional Digital - AND como articulador de los SCD adelanta la implementación del servicio de interoperabilidad de los Servicios Ciudadanos Digitales – SCD, por medio de la herramienta X-ROAD.

A continuación, se enuncian las características que se requieren las entidades para el hacer uso del servidor de seguridad que permitirá ajustar los servicios web y poder integrarlos a la plataforma de interoperabilidad del estado colombiano.

2 INTEROPERABILIDAD

La interoperabilidad es "la capacidad de las organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio para interactuar hacia objetivos mutuamente beneficiosos, con el propósito de facilitar la entrega de servicios Digitales A Ciudadanos, empresas y a otras entidades, mediante el intercambio de datos entre sus sistemas TIC". Esta es la definición de Interoperabilidad acogida para el Gobierno Digital.

2.1 Marco de Interoperabilidad

Atendiendo a la definición de interoperabilidad el Marco de Interoperabilidad es el enfoque común para la prestación de servicios de intercambio de información de manera interoperable. Este marco define el conjunto de principios, recomendaciones y lineamientos que orientan los esfuerzos políticos y legales, organizacionales, semánticos y técnicos de las entidades con el fin de facilitar el intercambio seguro y eficiente de información.

Figura 1. Marco de Interoperabilidad

Y ofrece un modelo de madurez, una serie de actividades que pueden ser usadas como referente por las entidades para compartir datos a través de servicios de intercambio de información vinculados a los Servicios Ciudadanos Digitales, con el propósito de facilitar la prestación de sus trámites y servicios a los ciudadanos, empresas y otras entidades públicas en el país.

2.2 Principios de interoperabilidad

- Enfoque en el ciudadano
- Cobertura y proporcionalidad
- Seguridad, protección y preservación de la Información
- Colaboración y participación
- Simplicidad
- Neutralidad, tecnológica y adaptabilidad
- Reutilización
- Confianza
- Costo-efectividad

2.3 Dominios del Marco de Interoperabilidad

El Marco de Interoperabilidad para Gobierno Digital contempla múltiples interacciones, denominadas dominios de interoperabilidad. Estos dominios, mediante un conjunto de lineamientos permiten mejorar la gobernanza de las actividades relacionadas a la interoperabilidad, permitiendo establecer relaciones entre proveedores y consumidores de información y racionalizar los procesos que dan soporte a los trámites y servicios de las entidades para los ciudadanos.

2.3.1 Dominio Político - legal

Este dominio corresponde a la disposición de un conjunto de políticas y normas que permiten el intercambio de información. La interoperabilidad político - legal consiste en garantizar que las entidades públicas realizan el intercambio de información ajustado al marco jurídico vigente, las políticas y estrategias pueden trabajar juntas y no se obstaculiza o impide la interoperabilidad.

2.3.2 Dominio Organizacional

Este dominio de la interoperabilidad se refiere al modo en que las misiones, políticas, procesos y expectativas interactúan con aquellos de otras entidades para alcanzar las metas adoptadas de común acuerdo y mutuamente beneficiosas, a través del intercambio de información. Para lograrlo es necesario la integración, adaptación o incluso la eliminación o definición de nuevos

procesos, trámites, servicios y otros procedimientos administrativos, así como realizar la identificar de los conjuntos de datos que son pertinentes y susceptibles de ser intercambiados.

2.3.3 Dominio Semántico

El dominio semántico permite garantizar que, en el momento de intercambiar datos, el significado de la información sea exacto y el mismo para todas las partes interesadas. De igual manera, permite que las entidades del Estado colombiano puedan estandarizar, gestionar y administrar su información.

2.3.4 Dominio Técnico

El dominio técnico de la interoperabilidad hace referencia a las aplicaciones e infraestructuras que conectan sistemas de información, las aplicaciones con los servicios de intercambio de información. Incluye aspectos como especificaciones de interfaz, protocolos de interconexión, servicios de integración de datos, presentación e intercambio de datos y protocolos de comunicación seguros.

2.4 Vinculación al servicio de interoperabilidad de los Servicios Ciudadanos Digitales

A continuación, se describe la información más relevante de cómo hacer para que la entidad se integre al servicio de Interoperabilidad.

1. **Planificar**

1.1.Alineación y modelo conceptual de la Interoperabilidad

La interoperabilidad tiene como propósito hacer que el Estado funcione como una sola Entidad eficiente que les brinde a sus ciudadanos información oportuna, trámites y servicios en línea ágiles. Las entidades deben ser conscientes del impacto de la interoperabilidad en la sociedad, asumir con compromiso y dar el primer paso para estar digitalmente conectados y articulados. ¡Ser un solo Sistema!

El Marco de Interoperabilidad es genérico y aplicable a todas las entidades públicas y privadas en Colombia, el marco establece las condiciones básicas que se deben considerar para alcanzar la interoperabilidad tanto a nivel local, interinstitucional, sectorial, nacional o internacional y orientado a todos los involucrados en definir, diseñar, desarrollar y entregar servicios de intercambio de información, como son:

- Entidades públicas responsables de planear servicios que requieran colaboración interinstitucional.
- Entidades públicas que para mejorar su funcionamiento y relacionamiento con otras entidades a través del uso de las TIC.
- Organizaciones privadas involucradas en la ejecución y/o evolución de la estrategia de Gobierno Digital.
- Miembros de gobiernos extranjeros interesados en la interoperabilidad con entidades del Estado colombiano.
- Miembros de la comunidad académica interesados en la interoperabilidad del Gobierno Digital.

El Marco de Interoperabilidad proporciona la orientación necesaria a las entidades públicas y en general todos aquellos que quieran intercambiar información, mediante un conjunto de lineamientos sobre cómo mejorar la gobernanza de las actividades relacionadas a la interoperabilidad, permitiendo establecer relaciones entre proveedores y consumidores de información y racionalizar los procesos que dan soporte a los trámites y servicios o cualquier servicio digital prestado por las entidades, de conformidad con el marco normativo vigente y con garantía de hacerlo en un entorno de confianza digital.

1.2.Marco de Implementación de la Interoperabilidad

Como parte de la estrategia de implementación del Servicio Ciudadano Digital de Interoperabilidad, utilizará como plataforma tecnológica de intercambio de datos entre entidades públicas la plataforma X-ROAD, favoreciendo así la transformación del Estado colombiano para que funcione como una sola institución que le brinde a los ciudadanos información oportuna, trámites ágiles y mejores servicios.

La plataforma de interoperabilidad tiene las siguientes características:

- Es una plataforma que habilita las capacidades para poder realizar un intercambio seguro de datos.
- Es una plataforma descentralizada, el intercambio de datos se produce directamente entre las entidades sin intermediarios.
- La propiedad de los datos no cambia. El propietario de los datos (proveedor de servicios) controla quién puede acceder a servicios concretos.

- Todos los mensajes procesados por la PDI son utilizables como evidencia digital. La seguridad de la PDI permite autenticación, autorización en el nivel central y en los servidores de seguridad, tráfico de datos cifrados con estampa cronológica de tiempo.
- Toda la comunicación se implementa como llamadas de servicio mediante el protocolo SOAP y tecnología REST.
- No hay roles predeterminados, una vez que una entidad se ha unido a la infraestructura, puede actuar como cliente y proveedor de servicios web sin tener que realizar ningún registro adicional.

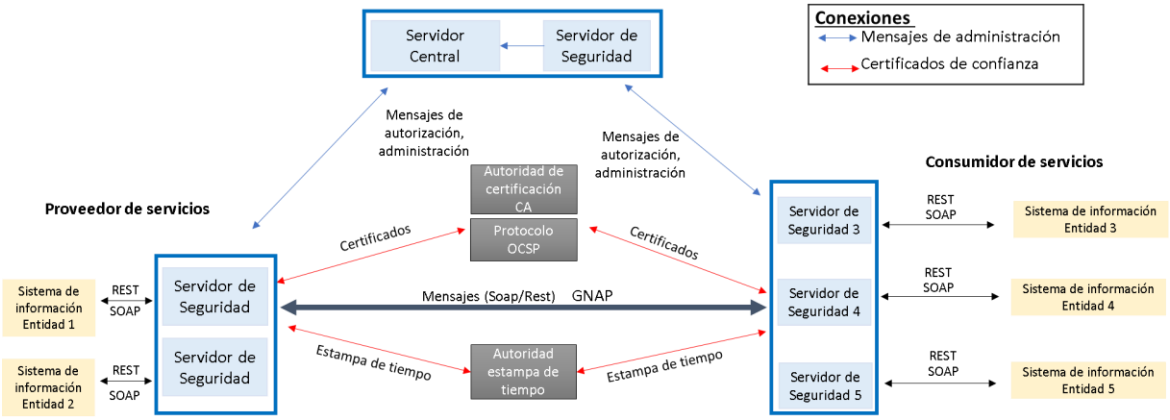


Figura 2. Modelo Conceptual de la plataforma de interoperabilidad

La Agencia Nacional Digital - AND como articulador de los Servicios Ciudadanos Digitales administra los componentes centrales de la plataforma, que estarán conectados a los servicios de confianza (Firma Digital y Estampa Cronológica de tiempo) prestados por una Autoridad de Certificación Digital, cada entidad pública deberá desplegar un servidor de seguridad para que sea integrado con los servicios web de sus sistemas de información, estos servidores de seguridad deberán estar registrados ante el componente central de la AND para habilitar el intercambio seguro de datos con mecanismos de firma digital y estampado cronológico, garantizando así la integridad y autenticidad en los datos.

Con la entrada del servicio de la plataforma de interoperabilidad, se estima que las entidades públicas sean más sostenibles (social, económica y medioambientalmente), más eficientes y efectivos en la contribución de la mejora de la calidad de los servicios que se prestan a los ciudadanos, mediante el uso de la tecnología. Los objetivos que persigue el servicio de interoperabilidad son los siguientes:

a) Mejorar la calidad de los servicios de intercambio de información prestados, el control de los contratos de servicios generados y la evolución de la gestión de los servicios en las entidades públicas.
b) Mejorar el modelo de gobierno del marco de interoperabilidad, la gestión de relaciones entre las entidades públicas y la participación de entidades, empresas y ciudadanos.
c) Aumentar la información disponible y los servicios adicionales que de ella se deriven para los ciudadanos y empresas, mediante difusión a través de la plataforma de interoperabilidad.
d) Aportar a un gobierno abierto, ofreciendo transparencia mediante la apertura de datos de forma estandarizada, consistente, unificada e integral.
e) Reducir el gasto público y mejorar la coordinación entre diferentes servicios y administraciones públicas.
f) Apoyar y mejorar la toma de decisiones por parte del gestor público a través de información en tiempo real.
g) Mejorar la transparencia de la función pública y la participación ciudadana por medios digitales a través de los trámites de las entidades.
h) Medir los resultados de la gestión de la interoperabilidad y su impacto en la administración pública, el relacionamiento con las empresas y la calidad de vida del ciudadano.
i) Evolucionar hacia un modelo auto gestionado y sostenible tanto en consumo de recursos como en eficiencia en servicios de intercambio de información.

1.3.Requerimientos Mínimos para la integración a la Interoperabilidad

Las entidades deberán contar como mínimo con una infraestructura tecnológica que permita desplegar un servidor virtual. Si requieren alta disponibilidad contar con dos o más nodos que permitan estar en Clúster. La entidad deberá tener la capacidad para poder desplegar la infraestructura de acuerdo con las siguientes especificaciones:

Ítem	Requisito	Explicación
1.0	Sistema Operativo Ubuntu 18.04 Long-Term Support (LTS), 64 bits o Red Hat RHEL7 (v7.3 o más reciente) Nota: Los servidores de seguridad puede ser físicos o virtuales.	X-Road soporta únicamente estas versiones en sistemas operativos

Ítem	Requisito	Explicación
1.1	2 CPU Intel o AMD o compatible de doble núcleo de 64 bits; El soporte del conjunto de instrucciones AES es altamente recomendado.	El hardware del servidor (placa base, CPU, tarjetas de interfaz de red, sistema de almacenamiento) debe ser compatible con RHEL7 o Ubuntu en general.
1.2	6 GB de RAM	Memoria RAM mínima requerida. de acuerdo con la transaccionalidad de la entidad pude aumentar la memoria RAM
1.3	20 GB de espacio libre en disco (partición del sistema operativo) 20-40 GB de espacio libre en disco (/var/partición);	Almacenamiento mínimo requerido.
1.4	Para la instalación del servidor de seguridad, se requiere que el servidor instalado tenga conectividad a internet para acceder a los repositorios de instalación que se detallan en el anexo técnico.	Acceso a repositorios de instalación
1.5	Una tarjeta de interfaz de red de 1000 Mbps. El canal depende de la transaccionalidad de los servicios web.	Red mínima requerida
1.6	El servidor de seguridad puede estar separado de otras redes por un firewall y / o NAT y se deben permitir las conexiones necesarias hacia y desde el servidor de seguridad. La habilitación de los servicios auxiliares que son necesarios para el funcionamiento y la administración del sistema operativo (como DNS, NTP y SSH) se encuentran fuera del alcance de esta guía. Nota: Si el servidor de seguridad tiene una dirección IP privada, se debe crear un registro NAT correspondiente en el firewall.	Segmentación de Red y Seguridad.

Para instalación, configuración y desarrollo plataforma de interoperabilidad las entidades deberán seguir lo establecido en los siguientes capítulos, los cuales detalla la manera de realizar la instalación y configuración de los servidores de seguridad, como también la forma de intervenir los servicios web que se encuentran desarrollados o a desarrollar en estándares REST y SOAP.

3 INSTALAR Y CONFIGURAR

3.1 Instalar

Para la instalación del servidor de seguridad la entidad deberá configurar los siguientes requerimientos:

Ítem	Requisito	Explicación
1.0	https://artifactory.niis.org/xroad-release-deb	Repositorio de paquetes X-Road
1.1	https://artifactory.niis.org/api/gpg/key/public	La clave del repositorio
1.2	**Conexiones entrantes**	Puerto para conexiones entrantes (desde la red externa al servidor de seguridad)
	TCP 5500	Intercambio de mensajes entre servidores de seguridad. Se recomienda utilizar el filtrado de IP (en la **lista blanca solo de AND IP y Nodos**).
	TCP 5577	Consulta de respuestas OCSP entre servidores de seguridad. Se recomienda utilizar el filtrado de IP (**en la lista blanca solo de AND IP y Nodos**)
	TCP 9011	Puerto de escucha JMX del demonio de monitoreo de datos operativos
	TCP 9999	Puerto de escucha JMX del demonio de monitoreo ambiental
1.5	**Conexiones salientes**	Puertos para conexiones salientes (desde el servidor de seguridad a la red externa)

Ítem	Requisito	Explicación
	TCP 5500	Intercambio de mensajes entre servidores de seguridad.
	TCP 5577	Consulta de respuestas OCSP entre servidores de seguridad.
	TCP 4001	Comunicación con el servidor central.
	TCP 2080	Puertos para conexiones salientes (desde el servidor de seguridad a la red interna) Intercambio de mensajes entre el servidor de seguridad y el demonio de monitoreo de datos operativos (de forma predeterminada en localhost)
	TCP 80	Descarga de la configuración global desde el servidor central.
	TCP 80,443	Los servicios de OCSP y de sellado de tiempo más comunes.
1.6	TCP 4000	Interfaz de usuario (red local). **¡No debe ser accesible desde internet!**
1.7	TCP 80, 443	Puntos de acceso al sistema de información (en la red local). **¡No debe ser accesible desde internet!**
	TCP 2080	Intercambio de mensajes entre el servidor de seguridad y el Proceso de monitoreo de datos operativos (de forma predeterminada en localhost)
	TCP 9011	Puerto de escucha JMX del demonio de monitoreo de datos operacionales
1.8	Direcciones IP	Direcciones IP internas de servidor de seguridad y nombre (s) de host

Ítem	Requisito	Explicación
1.9	Dirección Ip Servidor de Seguridad	Servidor de seguridad, dirección IP pública, dirección NAT.
1.10	<de forma predeterminada, las direcciones IP y los nombres del servidor se agregan al campo del Nombre Distinguido (DN) del Certificado Digital>	Información sobre el certificado TLS de la interfaz de usuario.
1.11	<de forma predeterminada, las direcciones IP y los nombres del servidor se agregan al campo del Nombre Distinguido (DN) del Certificado Digital>	Información sobre los servicios del certificado TLS.
1.12	TCP 2552	Puerto para comunicaciones entre los xroad-proxy y xroad-monitoring.
1.13	IP Pública	Monitoreo de seguridad del servidor IP en instancia de Gobierno.

Una vez se tiene el sistema operativo base, se ingresan las configuraciones de usuario, se establece la configuración regional del sistema para que posteriormente se instale paquete de plataforma X-ROAD.

Si durante la instalación se generan errores algunos de los más comunes se encuentran documentados en la guía técnica con el manejo que se le puede dar para su solución.

3.1.1 Instalación en Ubuntu

Para la instalación del software de seguridad X-ROAD en UBUNTU se tiene que seguir los siguientes pasos:

- Agregue la clave de firma del repositorio de X-Road a la lista de claves confiables.
- Agregue el repositorio de paquetes de X-Road.
- Instale los paquetes del servidor de seguridad.

Tras la primera instalación de los paquetes el sistema solicita información como nombre de cuenta del usuario, el nombre distinguido del propietario del certificado TLS autofirmado de la interfaz del usuario y sus nombres alternativos.

Una vez finalizada la instalación si esta se realiza correctamente se inician los servicios del sistema y la interfaz de usuario deberá estar respondiendo.

De forma opcional se puede instalar el soporte para tokens de seguridad por hardware.

3.1.2 Instalación en REDHAT

Para la instalación del software de seguridad X-ROAD en REDHAT se tiene que seguir los siguientes pasos:

- Agregue el repositorio de paquetes X-Road y los repositorios de paquetes adicionales para Enterprise Linux (EPEL).
- Agregue la clave de firma del repositorio de X-Road a la lista de claves confiables.
- Instale los paquetes del servidor de seguridad.
- Agregar usuario del sistema a los que se otorgan todos los roles en la interfaz de usuario.

Una vez finalizada la instalación si esta se realiza correctamente se inician los servicios del sistema y la interfaz de usuario deberá estar respondiendo.

La instalación de soportes para tokens por hardware no se ha probado en este sistema por lo cual no se proporciona soporte.

3.2 Configuración del servidor

Para realizar la configuración inicial haga uso de un navegador web para iniciar sesión por primera vez, use el nombre de cuenta suministrado durante la instalación, una vez iniciada sesión se solicita el archivo de anclaje de configuración global el cual es suministrado por la Agencia Nacional Digital AND. Si la información se descarga correctamente el sistema solicitara nueva información del miembro de propietario del servidor de seguridad.

Durante la configuración inicial del servidor de seguridad se ingresa la información de miembro del nodo X-Road del servidor y el PIN del token de software.

El anclaje de configuración es un conjunto de información que se puede utilizar para descargar y verificar información. Se proporciona un enlace a una configuración descargada. Los anclajes de configuración se distribuyen como archivos XML.

Cada entorno de X-Road tiene una configuración diferente. Utilice la configuración del entorno X-Road que va a utilizar.

Los anclajes de configuración de los tres entornos son los siguientes:

- Entorno de desarrollo: Solicitar a la Agencia Nacional Digital.
- Entorno de prueba: Solicitar a la Agencia Nacional Digital.
- Entorno de producción: Solicitarla a la Agencia Nacional Digital.

Cuando inicie sesión en su servidor web, https: // <SECURITYSERVER IP ADDRESS>: 4000 / por primera vez el sistema solicita la siguiente información:

- El archivo de anclaje de configuración global (solicitarlo a la Agencia Nacional Digital).

Si la configuración se descarga correctamente, el sistema solicita la siguiente información:

- La clase miembro del propietario del servidor de seguridad.
- El código de miembro del propietario del servidor de seguridad, si la clase de miembro y el código de miembro se ingresan correctamente, el sistema muestra el nombre del propietario del servidor de seguridad registrado en el centro de X-Road.

El Código de Miembro debe estar formado de la siguiente manera:

- "sigla de la Entidad-código SIGEP" - sin espacios en blanco

Ejemplo:

- Ministerio de tecnologías de la información y las Comunicaciones (Entidad Estatal).
- Nombre de miembro: MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
- Clase de miembro: CO
- Código de miembro: MinTIC-0012

Dichos requisitos del Código de miembro de CO son necesarios para garantizar la singularidad del Código de miembro de organizaciones en X-Road. Además, los miembros del Código de miembro de X-Road deben corresponder con el campo Identificador de organización (2.5.4.97) en el perfil de certificado de sello electrónico.

Adicionalmente en esta configuración inicial del servidor de seguridad tendrá que realizar lo siguiente:

- Agregar gestión de servicios de estampa cronológica de tiempo.
- Generar una clave de firma haciendo uso del certificado digital.
- Generar clave de autenticación.
- Generación de solicitud de certificado para clave de autenticación.

- Importar un certificado de firma desde un sistema de archivos local.
- Importar un certificado de firma desde un dispositivo criptográfico.
- Importar un certificado de autenticación de un sistema de archivos local.
- Registro del servidor de seguridad en la administración de X-Road.
- Agregar un certificado de prueba a la lista de prueba de OCSP.
- Estados de disponibilidad de dispositivos clave, claves y certificados.
- Condiciones de registro de certificados.
- Propietario y cliente del servidor de seguridad.
- Adicionar un cliente al servidor de seguridad.
- Registro del cliente del servidor de seguridad en la administración de PDI.
- Administración de servicios de datos.
- Activar y desactivar Servicios Web.
- Adición de un certificado TLS de red interna.
- Gestionando el Certificado Intranet TLS.
- Cambiar la clave TLS y el certificado para la intranet.
- Sujetos de derechos de acceso.
- Gestión de derechos de acceso.
- Cambiar los derechos de acceso al servicio.
- Añadir un cliente de servicio.
- Cambio de los derechos de acceso del cliente de servicio.
- Grupos con derechos de acceso locales y globales.
- Añadiendo un grupo local.
- Ver y editar miembros del grupo local.
- Cambiar la descripción del grupo local.
- Copia de seguridad de la configuración del servidor de seguridad.
- Cargar y eliminar un archivo de copia de seguridad de configuración.
- Restaurar la configuración de la interfaz de usuario.

- Transferencia de archivos de un servidor de seguridad.

4 INTEGRAR SERVICIOS WEB

4.1 Intervención de los servicios

Para la intervención de los servicios se debe tener en cuenta si la entidad va a exponer y/o consumir servicios. Nativamente la plataforma de interoperabilidad soporta tecnología REST y protocolo SOAP. Los servicios web en tecnología REST no requieren la intervención cuando estos son de exposición.

El Marco de Interoperabilidad describe una arquitectura de referencia orientada a la integración de servicios de exposición o consumo en la plataforma de interoperabilidad.

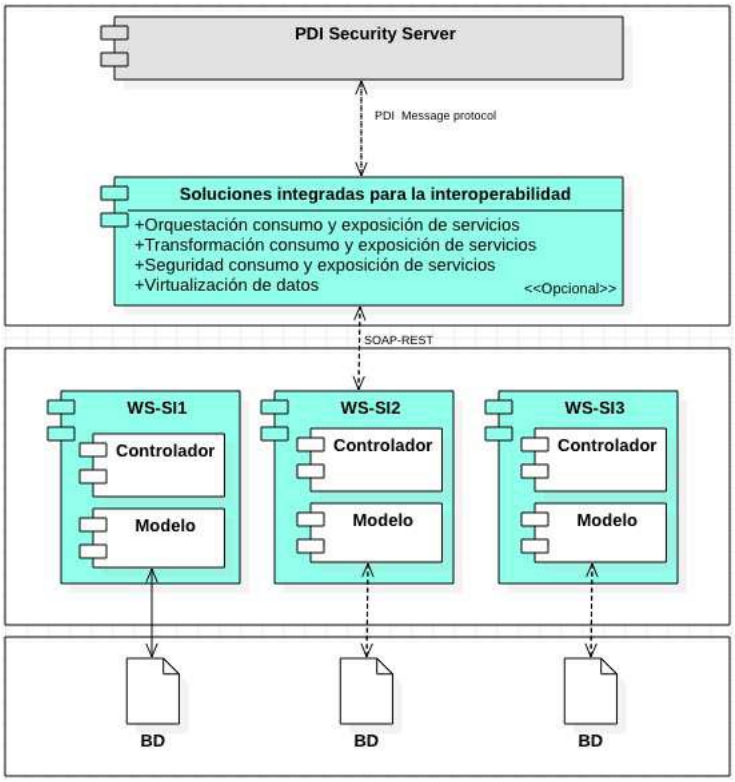


Figura 3. Modelo Conceptual de la plataforma de interoperabilidad

La arquitectura ilustrada muestra el componente de soluciones integradas para interoperabilidad como un componente que tendrá la capacidad de:

- Orquestar los servicios de consumo y exposición.
- Transformar servicios de consumo y exposición.
- Brindar seguridad en el consumo y exposición de servicios.
- Virtualizar datos.

Este componente servirá para agregar los encabezados que se requieren en los servicios web sin necesidad de intervenir estos directamente en su estructura. Este puede ser implementado por diferentes medios como, por ejemplo: un Bus de servicios (ESB Enterprise Service Bus), o un API y es opcional para las entidades dependiendo de la arquitectura interna.

Los encabezados deben tener una estructura y un espacio de nombres correctos, es por esto por lo que los servicios SOAP y REST (consumo) tienen que ser intervenidos para que los siguientes campos obligatorios de X-Road sean agregados

- Client: campo que identifica al cliente que inició la solicitud, que se describe con los siguientes elementos

  - xRoadInstance

  - memberClass

  - memberCode

  - subsystemCode

- Service: es el campo que especifica el servicio de datos que se utilizará. Además de agregar los elementos descriptivos del campo < client > se adicionan los siguientes elementos

  - (xRoadInstance, memberClass, memberCode y subsystemCode)

  - serviceCode

  -serviceVersion (Opcional)

4.2 Creación de subsistemas

En la plataforma de interoperabilidad, los servicios de intercambio de datos son consumidos a través de subsistemas sobre los cuales se conceden los permisos de acceso a cada uno de los clientes.

Las entidades pueden configurar quienes pueden consumir sus servicios a través de la gestión de derechos de acceso

Hay dos formas de administrar los derechos de acceso en un servidor de seguridad.

- La gestión de derechos de acceso basada en servicios: permite abrir o cerrar un servicio para múltiples clientes de servicios.
- Administración de derechos de acceso basada en el cliente: si necesita abrir o cerrar varios servicios para un cliente de servicio.

4.3 Adicionar servicios WEB

4.3.1 SOAP

Cuando se agrega un nuevo archivo WSDL, el servidor de seguridad lee la información del servicio y muestra la información en la tabla de servicios. El código de servicio, el título y la dirección se leen del WSDL.

Para agregar un WSDL, siga estos pasos:

- En el menú “Configuration”, seleccione “Security Server Clients”, seleccione un cliente de la tabla y haga clic en el icono “Services”.
- Haga clic en “ADD WSDL”, ingrese la dirección WSDL en la ventana que se abre y haga clic en Aceptar. Una vez que se cierra la ventana, el WSDL y la información sobre los servicios que contiene se agregan a la tabla. Por defecto, el WSDL se agrega en estado deshabilitado.

Para ver una lista de servicios contenidos en el WSDL haga clic en el símbolo " + " delante de la fila WSDL para expandir la lista.

4.3.2 REST

Cuando se agrega un nuevo servicio REST, el servidor de seguridad muestra la url y el código de servicio proporcionado.

Para agregar un servicio REST, siga estos pasos:

- En el menú “Configuration”, seleccione “Security Server Clients”, seleccione un cliente de la tabla y haga clic en el icono “Services”.
- Haga clic en “ADD REST”, ingrese la url y el código de servicio en la ventana que se abre y haga clic en Aceptar. Una vez que se cierra la ventana, la url y el código de servicio se agregan a la tabla. Por defecto, la API REST se agrega en estado deshabilitado.

Para ver el servicio el servicio REST haga clic en el símbolo " + " delante de la fila REST para expandir la descripción del servicio.

4.4 Pruebas de Intercambio

4.4.1 Monitoreo

La calidad del servicio está determinada, entre otras cosas, por su disponibilidad. Para garantizar que los servicios estén siempre disponibles, los servidores de seguridad que proporcionan el servicio deben tener suficientes recursos.

Por ejemplo, se pueden seguir los siguientes, que determina, entre otras cosas, los requisitos de disponibilidad. Los cuatro niveles de disponibilidad son:

K0: disponibilidad inferior al 80% anual, tiempo de interrupción máximo permisible durante las horas de servicio superior a 24 horas.

K1: disponibilidad 80% -99% anual, tiempo de interrupción único permitido máximo durante las horas de servicio 4-24 horas.

K2: disponibilidad 99% -99.9% anual, tiempo de interrupción único permitido máximo durante las horas de servicio 1-4 horas.

K3: disponibilidad de al menos el 99,9% anual, tiempo máximo de interrupción permitido durante las horas de servicio hasta 1 hora.

Los requisitos de disponibilidad y los tiempos de respuesta generalmente se definen en el Acuerdo de Nivel de Servicio (SLA). Estos requisitos generalmente los define la entidad a la que se le debe solicitar dicha información.

La plataforma de interoperabilidad cuenta con diferentes comandos con los cuales se obtiene información sobre el estado de su funcionamiento, estos son:

- " Top": proporciona una vista dinámica en tiempo real del sistema en ejecución.
- " El tiempo de actividad ": muestra cuánto tiempo se ha estado ejecutando el servidor.
- " ps": muestra información sobre la selección de procesos activos.
- " free": muestra la cantidad total de memoria física y de intercambio libre y usada en el sistema.
- " Df": proporciona información sobre el uso del espacio en disco del sistema de archivos.
- " Iostat": proporciona información sobre las estadísticas de la CPU y la entrada / salida del dispositivo y la sección.

- " Mpstat": proporciona información sobre estadísticas relacionadas con el proceso.
- " Netstat": imprime conexiones de red, tablas de enrutamiento, estadísticas de interfaz, conexiones de enmascaramiento y membresía de multidifusión.
- " Iptraf": es un monitor de LAN IP que genera varias estadísticas de red.
- " Iftop.": muestra el ancho de banda en la interfaz en tiempo real por el host.

4.5 Reporte

Las herramientas enumeradas lo ayudarán a supervisar el servidor de seguridad cuando inicie sesión. A largo plazo, es aconsejable utilizar aplicaciones que recopilen información a lo largo del tiempo y la presenten, por ejemplo, gráficamente. Esto proporciona una mejor comprensión de cómo funciona el sistema con carga alta.

Para obtener resultados confiables, las aplicaciones de monitoreo deben instalarse en un servidor separado. Por ejemplo, los mensajes de error de la red no se pueden enviar por correo electrónico si la propia red no funciona.

A continuación, las siguientes herramientas de monitoreo y reporte se presentarán:

- Cactus
- Nagios
- Zabbix

4.6 Producción

Una vez finalizado la integración de la entidad a la plataforma de interoperabilidad PDI, la decisión de que este pase a etapa de producción está en manos de la entidad, para ello se recomienda tener en cuenta lo siguiente:

- La entidad debe estar certificada en nivel 3 de lenguaje común de intercambio.
- La entidad comprende el marco de interoperabilidad para gobierno digital, el cual se fundamenta en un modelo de madurez basado en aspectos legales, técnicos y organizacionales que permite el desarrollo progresivo de los servicios de intercambio de información al interior de las entidades, estos dominios son:
  - **Dominio Político – legal:** Consiste en garantizar que las entidades públicas realizan el intercambio de información ajustado al marco jurídico vigente, las políticas y estrategias pueden trabajar juntas y no se obstaculiza o impide la interoperabilidad.

- **Dominio Organizacional:** se refiere al modo en que las misiones, políticas, procesos y expectativas interactúan con aquellos de otras entidades para alcanzar las metas adoptadas de común acuerdo y mutuamente beneficiosas, a través del intercambio de información.

- **Dominio Semántico**: permite garantizar que, en el momento de intercambiar datos, el significado de la información sea exacto y el mismo para todas las partes interesadas. De igual manera, permite que las entidades del Estado colombiano puedan estandarizar, gestionar y administrar su información.

- **Dominio Técnico**: hace referencia a las aplicaciones e infraestructuras que conectan sistemas de información, a través de los servicios de intercambio de información. Incluye aspectos como especificaciones de interfaz, protocolos de interconexión, servicios de integración de datos, presentación e intercambio de datos y protocolos de comunicación seguros.

5 INSTALACIÓN Y CONFIGURACIÓN EN DOCKER DEL SERVIDOR DE SEGURIDAD PARA AMBIENTE DE DESARROLLO.

Instalar una máquina virtual para el servicio de PDI-Security con las siguientes características:

Características	Descripción
Máquina Virtual	Permite que se exportada a Hipervisor VMWARE
Sistema Operativo	Ubuntu 18.04.2 LTS
Plataforma	X64
Procesador 1 Cores	1 virtual CPU
Memoria RAM	2 GB
Disco Duro	20 GB
FileSystem	LVM

Al tener instalada la máquina virtual con el sistema operativo y una dirección IP asignada de la red interna de la entidad se procede a instalar el Docker de la siguiente manera:

1. Actualizar la lista de paquetes existente:

   `sudo apt update`

2. Instalación de paquetes de requisitos previos que le permiten a apt usar paquetes mediante HTTPS:

   `sudo apt install apt-transport-https ca-certificates curl software-properties-common`

3. Agregar la clave GPG para el repositorio oficial de Docker a su sistema:

   `curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -`

4. Agregar el repositorio de Docker a las fuentes de APT:

   `sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu bionic stable"`

5. Actualizar la base de datos de paquetes usando los paquetes de Docker del repositorio que acaba de agregar:

   sudo apt update

6. Asegúrese de que va a instalar desde el repositorio de Docker en vez del repositorio de Ubuntu predeterminado:

   apt-cache policy docker-ce

7. Se obtiene el siguiente resultado aunque el número de versión de Docker puede variar:

   Output of apt-cache policy docker-ce

   docker-ce:

   Installed: (none)

   Candidate: 18.03.1~ce~3-0~ubuntu

   Version table:

   18.03.1~ce~3-0~ubuntu 500

   500 https://download.docker.com/linux/ubuntu bionic/stable amd64 Packages

Se evidencia docker-ce no está instalado, pero el candidato para la instalación es del repositorio de Docker para Ubuntu 18.04 (bionic).

8. Instalar el Docker:

   sudo apt install docker-ce

   Docker instalado, el daemon iniciado, y el proceso habilitado para iniciar durante el arranque. Verifique que se esté ejecutando:

   sudo systemctl status docker

   El resultado debería ser parecido al siguiente, indicando que el servicio está activo y se está ejecutando:

   Output

   ● docker.service - Docker Application Container Engine

```
     Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset:
enabled)
     Active: active (running) since Thu 2018-07-05 15:08:39 UTC; 2min 55s ago
     Docs: https://docs.docker.com
   Main PID: 10096 (dockerd)
     Tasks: 16
     CGroup: /system.slice/docker.service
     ├─10096 /usr/bin/dockerd -H fd://
     └─10113 docker-containerd --config /var/run/docker/containerd/containerd.toml
```

Instalar Docker ahora no solamente le ofrece el servicio Docker (daemon), sino también la utilidad de línea de comandos docker o el cliente Docker.

9. **Ejecutar el comando Docker sin sudo (Opcional)**

De forma predeterminada, el comando docker solamente puede ejecutarse por el usuario de root o por un usuario en el grupo docker, el cual se crea automáticamente durante la instalación de Docker. Si intenta ejecutar el comando docker sin prefijo con sudo o sin estar en el grupo docker, el resultado será como el siguiente:

```
Output

docker: Cannot connect to the Docker daemon. Is the docker daemon running on this
host?.

See 'docker run --help'.
```

10. Agregar el nombre de usuario al grupo docker si quiere evitar escribir sudo siempre que deba ejecutar el comando docker:

```
sudo usermod -aG docker ${USER}
```

Para aplicar la nueva membresía de grupo, debe cerrar sesión en el servidor y volver a iniciarla, o puede escribir lo siguiente:

```
su - ${USER}
```

11. Se le pedirá que ingrese la contraseña de su usuario para poder continuar.
12. Confirme que se haya agregado su usuario al grupo de docker escribiendo:

```
id -nG
```

```
Output
```

```
sammy sudo docker
```

13. Si necesita agregar un usuario al grupo de docker y no ha iniciado sesión como ese usuario, declare tal nombre de usuario explícitamente usando:

```
sudo usermod -aG docker username
```

14. Usar docker consiste en pasarle una cadena de opciones y comandos seguidos de argumentos. La sintaxis sería la siguiente:

```
docker [option] [command] [arguments]
```

Para ver todos los subcomandos disponibles, ingrese:

```
docker
```

Desde que se usa Docker 18, la lista completa de los subcomandos disponibles incluye:

```
Output
attach     Attach local standard input, output, and error streams to a running container
 build     Build an image from a Dockerfile
 commit    Create a new image from a container's changes
 cp        Copy files/folders between a container and the local filesystem
create     Create a new container
 diff      Inspect changes to files or directories on a container's filesystem
 events    Get real time events from the server
 exec      Run a command in a running container
 export    Export a container's filesystem as a tar archive
```

history Show the history of an image

images List images

import Import the contents from a tarball to create a filesystem image

info Display system-wide information

inspect Return low-level information on Docker objects

kill Kill one or more running containers

load Load an image from a tar archive or STDIN

login Log in to a Docker registry

logout Log out from a Docker registry

logs Fetch the logs of a container

pause Pause all processes within one or more containers

port List port mappings or a specific mapping for the container

ps List containers

pull 27ersión image or a repository from a registry

push 27ersión image or a repository to a registry

rename Rename a container

restart Restart one or more containers

rm Remove one or more containers

rmi Remove one or more images

run Run a command in a new container

27ers Save one or more images to a tar archive (streamed to STDOUT by default)

search Search the Docker Hub for images

start Start one or more stopped containers

stats Display a live stream of container(s) resource usage statistics

stop Stop one or more running containers

tag Create a tag TARGET_IMAGE that refers to SOURCE_IMAGE

top Display the running processes of a container

unpause Unpause all processes within one or more containers

update Update configuration of one or more containers

28ersión Show the Docker 28ersión information

wait Block until one or more containers stop, then print their exit codes

15. Si desea ver las opciones disponibles para un comando específico, ingrese:

```
docker docker-subcommand --help
```

16. Desplegar la imagen docker del servidor de seguridad para ambiente de desarrollo:

Nota: Las imágenes independientes del servidor de seguridad están estrictamente diseñadas para fines de prueba y desarrollo. ¡No lo uses en el entorno de producción!

La imagen de la ventana acoplable independiente del servidor de seguridad contiene un conjunto personalizado de módulos en lugar de xroad-securityserver:

- xroad-proxy
- xroad-addon-metaservices
- xroad-addon-wsdlvalidator
- XROAD-autologin

La imagen está construida a partir de fuentes de la versión bionic-6.21.0 o posterior. El servidor de seguridad instalado tiene una organización miembro registrada 'TestOrganization' y dos subsistemas 'TestClient' y 'TestService'.

El servidor de seguridad independiente permanece operativo durante un año.

Credenciales de acceso

Admin UI credenciales: xrd / secr

Desplegar el Docker con el siguiente comando

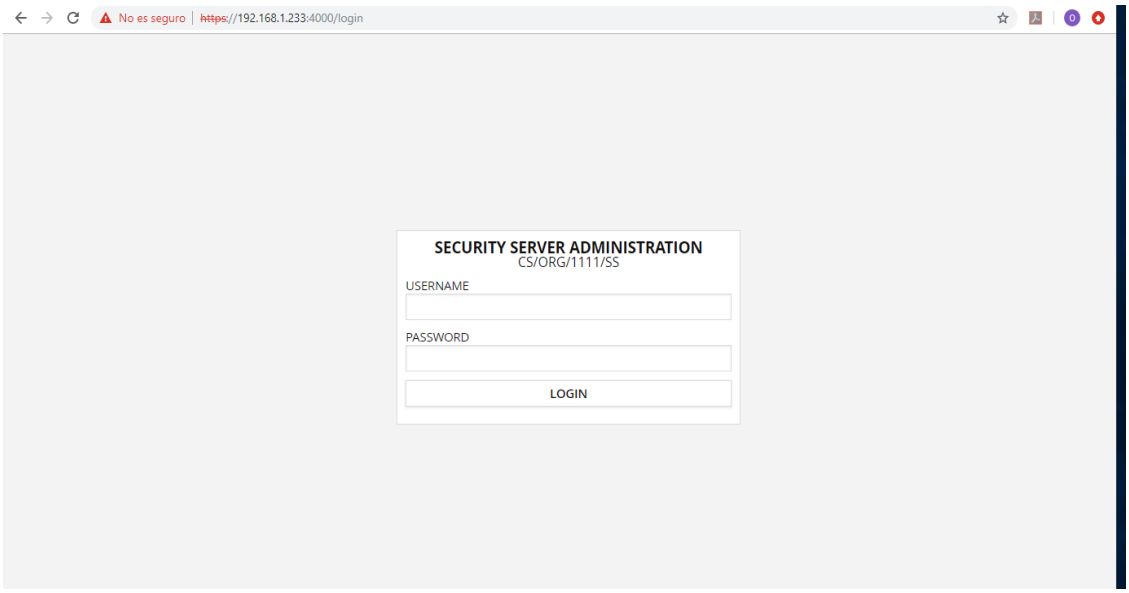
```
docker pull niis/xroad-security-server-standalone
```

Ejecutar el Docker para inicio de los servicios y depligue para fines de desarrollo

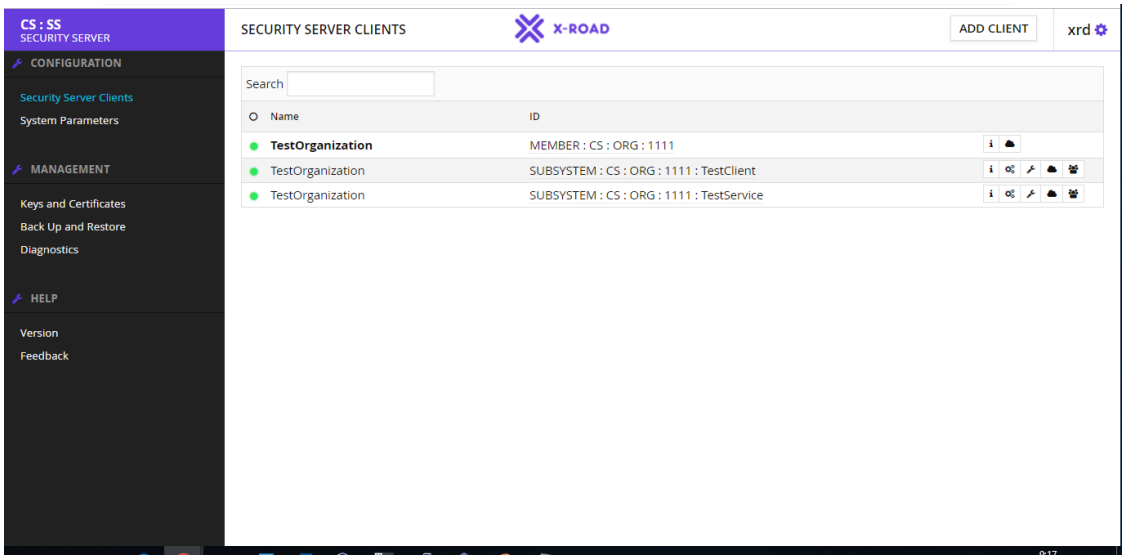
```
docker run -p 4000:4000 -p 80:80 --name ss niis/xroad-security-server-standalone:bionic-6.21.0
```

Ingresar al servidor de seguridad

https://DireccionIpAsigandaporlaEntidad:4000/login



Ingresar credenciales anteriormente mencionadas



Ya se pueden adicionar los servicios en REST o SOAP de acuerdo para intercambiar servicios.