DISEÑO DE ARQUITECTURA TÉCNICA PARA LA IMPLEMENTACIÓN DE LA PLATAFORMA DE INTEROPERABILIDAD DEL ESTADO

BOGOTÁ, AGOSTO DE 2019

CONTENIDO

INTRODUCCIÓN

El servicio ciudadano digital de interoperabilidad es aquel que brinda las capacidades necesarias para garantizar el adecuado flujo de información y de interacción entre los sistemas de información de las entidades públicas, permitiendo el intercambio, la integración y la compartición de la información, con el propósito de facilitar el ejercicio de sus funciones constitucionales y legales, estando conforme con los lineamientos del marco de interoperabilidad. Por lo anterior, la Agencia Nacional Digital está ejecutando el proyecto de implementación de la plataforma de interoperabilidad del estado colombiano con el fin de contribuir a mejorar las condiciones de intercambio de información entre entidades y éstas operen de manera articulada como un único gran sistema que le brinde a los ciudadanos información oportuna, trámites ágiles y mejores servicios.

El Proyecto consiste en la instalación, configuración, puesta en operación de la plataforma de interoperabilidad del Estado colombiano basado en la plataforma X-Road y en el acompañamiento técnico para la integración de las entidades públicas a este servicio ciudadano digital.

El presente documento corresponde a la construcción del diseño técnico donde se definen los criterios para el diseño y se evidencian las arquitecturas de componentes, despliegue y secuencia de la plataforma de interoperabilidad. El documento también contiene el plan de pruebas funcionales, no funcionales y de seguridad que serán ejecutadas en el marco de la ejecución del proyecto.

ARQUITECTURA TÉCNICA PARA LA IMPLEMENTACIÓN DEL SERVICIO CIUDADANO DIGITAL DE INTEROPERABILIDAD

La Agencia Nacional Digital - AND, 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.

Las características generales que esta plataforma de intercambio ofrece son las siguientes:

- Es un software de código abierto que permite a instituciones y organizaciones intercambiar información a través de Internet.
- Es una plataforma que habilita las capacidades de manera distribuida para poder realizar un intercambio seguro de datos.
- El sistema garantiza la seguridad suficiente para el tratamiento de las consultas realizadas a las bases de datos de las entidades y las respuestas recibidas.
- La infraestructura de la plataforma de interoperabilidad – PDI, se compone de software, hardware y métodos organizativos para el uso estandarizado en el intercambio de información.
- La seguridad de la PDI permite autenticación, autorización multinivel, un sistema de procesamiento de registros de alto nivel y tráfico de datos cifrados con estampa cronológica de tiempo.

1. **Criterios de diseño de arquitectura de la plataforma de interoperabilidad**

    - **La PDI es descentralizada**: el intercambio de datos se produce directamente entre las entidades, sin intermediarios. El intercambio continuo de datos depende únicamente de la disponibilidad de los componentes, sistemas y de la red de las entidades.
    - **Canal de comunicación**: Internet como canal de comunicación de datos entre entidades.
    - **Propiedad de los datos**: No cambia la propiedad de los datos. El propietario de los datos (proveedor de servicios) controla quién puede acceder a consumir los servicios.
    - Todos los mensajes procesados por la PDI son utilizables como evidencia digital. La solución técnica debe cumplir los requisitos de firmas digitales, esto implica la compatibilidad con dispositivos de creación de firma digital segura.
    - Toda la comunicación se implementa como llamadas de servicio mediante el protocolo SOAP o REST.
    - **Encapsulado del protocolo de seguridad**: Las medidas de seguridad y el protocolo de seguridad se encapsulan en componentes estándares. Las entidades están obligadas a implementar la funcionalidad relacionada con la seguridad para el intercambio de datos.
    - **Estandarización:** Tiene como objetivo estandarizar el protocolo de comunicación entre las entidades. Esto permite a las entidades conectarse a cualquier número de proveedores de servicios web sin implementar protocolos adicionales. La PDI no realiza la conversión de protocolos y datos. Si es necesario, estas conversiones se pueden realizar mediante el sistema

de información de la entidad.

- **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.
- **Autenticación de dos niveles:** el componente central de la PDI maneja la autenticación y el control de acceso a nivel de la entidad. La autenticación del usuario final la realiza el sistema de información del cliente de servicio usando el servicio de autenticación digital.

2. Modelo de Componentes de la plataforma de interoperabilidad-PDI

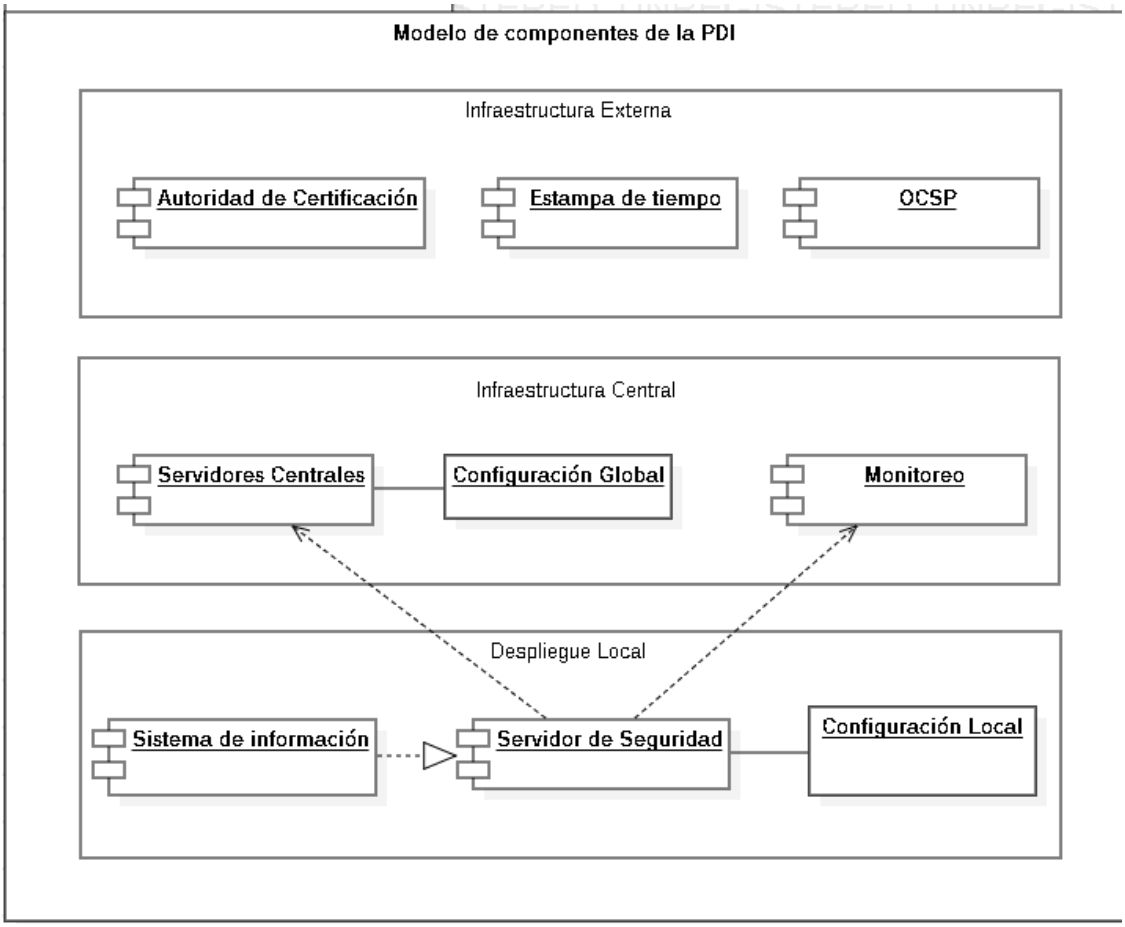

Figura 1: Modelo de Componentes de la PDI

La infraestructura central del sistema consta de un servidor central, un servidor de seguridad, una configuración compartida y un componente de monitoreo. Esa parte central consume servicios de una autoridad de certificación externa. El servidor central tiene dos funciones principales, la primera es servir de vehículo para de gestión y distribución de la configuración compartida hacia otros servidores de seguridad. La segunda, se encarga de recopilar estadísticas de los servidores de seguridad implementados localmente en las entidades. Ninguna comunicación pasa a través del servidor central; este podría no estar presente en la red durante horas sin ningún impacto en la disponibilidad del servicio de la plataforma de interoperabilidad. La configuración compartida es, como su nombre lo indica, la configuración que se comparte entre los servidores de seguridad. Incluye los parámetros de configuración de red de bajo nivel necesarios para la comunicación entre servidores de seguridad y la información relacionada con la autoridad de certificación.

La autoridad de certificación (una autoridad de certificación es parte de lo que se conoce como Infraestructura de clave pública), es un componente clave para la forma en que ocurre la autenticación y la autorización en X-Road. Cada Entidad recibe un certificado digital que se utiliza para cifrar todas las comunicaciones y garantizar que solo las entidades autorizadas tengan acceso a los servicios.

Para el ambiente de despliegue local en las entidades, la parte clave del sistema es el servidor de seguridad. Este actúa como punto principal de contacto para acceder al sistema de información que proporciona el servicio. Allí se establecen las reglas para permitir el acceso al consumo de los servicios de intercambio. Además de bloquear el acceso no autorizado y asegurar el canal de comunicación, el servidor de seguridad también garantiza la irrefutabilidad de las solicitudes y respuestas firmando digitalmente las solicitudes y respuestas y enviando hashes de todas las comunicaciones al servidor central.

3. Arquitectura de Componentes de la plataforma de interoperabilidad-PDI

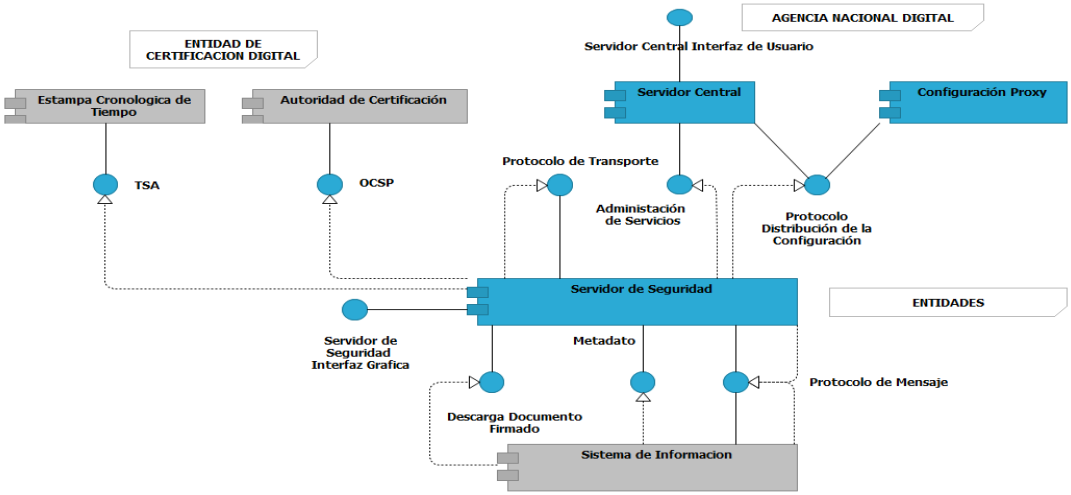

Figura 2: Arquitectura de componentes de la PDI

3.1 Servidor Central

¡Error! No se encuentra el origen de la referencia.

- Lista de autoridades de certificación de confianza.
- Lista de autoridades confiables de estampa cronológica de tiempo.
- Parámetros ajustables, como la duración máxima permitida de una respuesta OCSP.

¡Error! No se encuentra el origen de la referencia.

Adicional a la distribución de configuración, el servidor central proporciona una interfaz para realizar tareas de administración, como agregar y quitar clientes de servidor de seguridad. Estas tareas se invocan desde la interfaz de usuario de los servidores de seguridad.

3.2 Servidores de Seguridad

- El servidor de seguridad interactúa con las llamadas de servicio y las respuestas de servicio web entre sistemas de información. La plataforma administra las claves para la firma digital, autenticación y envío de mensajes a través del canal seguro G-NAP, creación del valor de prueba jurídica para mensajes con firmas digitales, estampado de tiempo) y el registro. Para el cliente de servicio y el sistema de información del proveedor de servicios, el servidor de seguridad ofrece un protocolo basado en SOAP o REST. Este protocolo es el mismo tanto para el cliente como para el proveedor de servicios, lo que hace que el servidor de seguridad sea transparente para las aplicaciones.
- Un único servidor de seguridad puede hospedar varias entidades. La entidad que administra el servidor de seguridad y es el propietario del servidor, las entidades hospedadas son clientes del servidor de seguridad.
- El servidor de seguridad administra dos tipos de claves (certificados digitales). Las claves de autenticación se asignan a un servidor de seguridad y se utilizan para establecer canales de comunicación criptográficamente seguros con los otros servidores de seguridad. Las claves de firma se asignan a los clientes del servidor de seguridad y se usan para firmar los mensajes intercambiados. Las claves se pueden almacenar en el disco duro (token de software) o en un dispositivo criptográfico físico.
- El servidor de seguridad descarga y almacena en caché la configuración global actualizada y la información de validez del certificado. El almacenamiento en caché permite que el servidor de seguridad funcione incluso cuando las fuentes de información no están disponibles.**¡Error! No se encuentra el origen de la referencia.**

3.3 Sistema de información

El sistema de información utiliza y/o proporciona servicios web a través de la plataforma de interoperabilidad-PDI. Para el cliente de servicios web el servidor de seguridad actúa como punto de entrada a todos los servicios web. El cliente es responsable de implementar un mecanismo de autenticación de usuario y control de acceso que cumpla con los requisitos de la instancia de X-Road en particular. La identidad del usuario final se hace disponible para el proveedor de servicios incluida en el

mensaje SOAP o REST. El cliente puede descubrir los miembros de X-Road y los servicios disponibles mediante el protocolo de metadatos de X-Road.

El sistema de información del proveedor de servicios web implementa un servicio SOAP o REST y lo hace disponible a través de X-Road. Para este propósito, el servicio debe ajustarse al Protocolo de mensajes X-Road.

3.4 Servicio Estampa Cronológica de Tiempo-TSA

La autoridad de estampado de tiempo emite estampas cronológicas de tiempo que certifican la existencia de elementos de datos en un determinado momento. La autoridad de estampado de tiempo debe proveer el protocolo de estampa de tiempo.

La PDI utiliza la estampa de tiempo por lotes. Esto reduce la carga del servicio de estampa de tiempo. La carga no depende del número de mensajes intercambiados a través de la PDI, en su lugar depende del número de servidores de seguridad en el sistema.

3.5 Autoridad de Certificación Digital

La entidad de certificación (AC) emite certificados digitales a los servidores de seguridad (certificados de autenticación) y a las entidades miembro de la PDI (certificados de firma). Todos los certificados se almacenan en los servidores de seguridad. La AC debe ser capaz de procesar las solicitudes de firma de certificados conforme a al algoritmo [PKCS10][1].

La AC debe distribuir la información de validez del certificado vía el protocolo OCSP, Los servidores de seguridad guarda en caché las respuestas OCSP[2] para reducir la carga en el servicio OCSP y para aumentar la disponibilidad. La carga en el servicio OCSP depende del número de certificados emitidos.

3.6 Proxy de Configuración

El proxy de configuración implementa la parte del cliente y la parte del servidor del Protocolo de distribución de configuración administrada por la Agencia Nacional Digital. El proxy de configuración descarga la configuración, la almacena y la pone a disposición para su descarga. Por lo tanto, el proxy de configuración se puede utilizar para aumentar la disponibilidad del sistema mediante la creación de un origen de configuración adicional y reducir la carga en el servidor central.

3.7 Protocolos e interfaces

[1] http://doc.nisu.org/docs/berliner/pkcs10.html

[2] https://csrc.nist.gov/glossary/term/Online-Certificate-Status-Protocol

3.7.1 Protocolo de mensajes

Es utilizado por los sistemas de información del cliente y del proveedor de servicios para comunicarse con el servidor de seguridad X-Road.

El protocolo es un protocolo de estilo RPC sincrónico, iniciado por el cliente (Sistema de Información) o por el servidor de seguridad del proveedor de servicios.

El protocolo de mensajes se basa en SOAP o REST a través de HTTP (S) y agrega campos de encabezado adicionales para identificar el cliente de servicio y el servicio invocado.

Este protocolo (junto con el protocolo de transporte de mensajes) constituye el núcleo del intercambio de datos de X-Road. Si los componentes implicados no están disponibles, el intercambio de datos no es posible. La arquitectura PDI permite mejorar la disponibilidad de los componentes implicados mediante la redundancia.

3.7.2 Protocolo distribución de la configuración

Los clientes deben descargar los archivos de configuración global generados desde el servidor central.
El protocolo de descarga de la configuración es un protocolo sincrónico que es ofrecido por el servidor central. Lo utilizan los clientes de configuración, como los servidores de seguridad y los proxys de configuración.

El protocolo se basa en la mensajería multiparte HTTP y MIME. La configuración está firmada digitalmente por el servidor central para protegerla contra modificaciones. Por lo general, la configuración consta de varias partes. El protocolo permite a los clientes de configuración comprobar si la configuración ha cambiado y la descargar de partes modificadas.

Los servidores de seguridad X-Road mantienen una copia local de la configuración global, que actualizan periódicamente desde su respectivo origen de configuración. Esta configuración global almacenada en caché tiene un período de validez, que, en general, es más largo que el período en el que los clientes de configuración están configurados para actualizar su copia local. Los servidores de seguridad siguen estando totalmente operativos mientras la configuración global almacenada en caché sigue siendo válida. Sin embargo, una copia obsoleta de la configuración global restringe severamente las capacidades de administración del servidor de seguridad y prohíbe a los servidores de seguridad procesar las solicitudes entrantes. Un tiempo de inactividad corto de la interfaz es admisible dentro de los límites del período de validez de la configuración. La Agencia Nacional Digital notificará a las entidades el plan detallado para actualizaciones y periodicidad de las copias de seguridad.

3.7.3 Protocolo de transporte de mensajes

El servidor de seguridad utiliza el protocolo de transporte de mensajes para intercambiar solicitudes de servicio y respuestas de servicio. El protocolo es un protocolo de estilo RPC sincrónico Iniciado por el servidor de seguridad del cliente de servicio.

El protocolo se basa en HTTPS y utiliza la autenticación TLS basada en certificados mutuos. Los mensajes SOAP o REST recibidos del cliente y el proveedor de servicios se ajustan en un mensaje MIME de varias partes junto con datos adicionales relacionados con la seguridad, como firmas y respuestas OCSP. Este protocolo (junto con el protocolo de mensajes) forma el núcleo del intercambio de datos. Si los componentes implicados no están disponibles, el intercambio de datos es imposible. La arquitectura X-Road permite mejorar la disponibilidad de los componentes implicados mediante la redundancia.

3.7.4 Protocolo metadatos de servicio

El protocolo de metadatos del servicio puede ser utilizado por los sistemas de información del cliente de servicio para recopilar información sobre la instancia de X-Road. En particular, el protocolo se puede utilizar para encontrar las entidades de X-Road, los servicios ofrecidos por estas entidades y las descripciones de los servicios.

El protocolo es un protocolo de estilo RPC sincrónico iniciado por el cliente de servicio (Sistema de Información). Algunos de los servicios de información se implementan como solicitudes HTTP (S) GET para simplificar la implementación del cliente. Los demás servicios de información se denominan servicios estándar de X-Road. El protocolo de metadatos de servicio se utiliza para la configuración del cliente y, por tanto, la disponibilidad, el rendimiento y la latencia de sus componentes de implementación no son fundamentales para el funcionamiento de X-Road.

3.7.5 Descarga documento firmado

El servicio de descarga de documentos firmados puede ser utilizado por los sistemas de información para descargar los contenedores firmados desde el registro de mensajes del servidor de seguridad. Además, el servicio proporciona un método de verificación para descargar la configuración global que se puede utilizar para validar los contenedores firmados.

El protocolo es un protocolo sincrónico de estilo RPC Iniciado por el sistema de información. El servicio se implementa como solicitudes HTTP (S) GET.

El protocolo Descarga documento firmado es utilizado por el sistema de información para descargar los datos almacenados en el servidor de seguridad y, por lo tanto, la disponibilidad, el rendimiento y la latencia de sus componentes de implementación no son críticos para el funcionamiento de X-Road.

3.7.6 Protocolo de servicios de administración

Los servidores de seguridad llaman a los servicios de administración para realizar tareas de administración, como registrar un cliente de servidor de seguridad o eliminar un certificado de autenticación. El protocolo de servicio de administración es un protocolo sincrónico de estilo RPC que ofrece el servidor central. Los servidores de seguridad llaman al servicio. Los servicios de administración se implementan como servicios estándares de X-Road que ofrece la organización que administra la instancia de X-Road.

La excepción es el servicio de registro de certificados de autenticación que, por razones técnicas, se implementa directamente en el servidor central. Los detalles completos de los servicios de gestión se describen en general, los servicios de gestión no son críticos para el funcionamiento de X-Road y, por lo tanto, su disponibilidad no es primordial. Si los servicios de administración no están disponibles, los servidores de seguridad no pueden administrar sus clientes y certificados de autenticación.

Algunas acciones (como la eliminación de clientes y certificados) se pueden realizar manualmente por el administrador del servidor central, sin utilizar los servicios de administración. Las operaciones del servicio de administración no son de tiempo crítico (el usuario del servidor de seguridad elige explícitamente enviar la solicitud de administración y la interfaz de usuario no implica que esta operación sea instantánea).

3.7.7 Protocolo OCSP

Los servidores de seguridad utilizan el protocolo OCSP (Protocolo de comprobación del Estado de un Certificado En línea) que permite consultar la información de validez sobre los certificados de firma y autenticación.

El protocolo OCSP es un protocolo sincrónico que ofrece el servicio de una entidad emisora de certificados. Cada servidor de seguridad es responsable de descargar y almacenar en caché la información de validez sobre sus certificados. Las respuestas OCSP se envían a los otros servidores de seguridad como parte del Protocolo de transporte de mensajes. Esto garantiza que los servidores de seguridad no necesiten detectar el servicio OCSP utilizado por la otra parte. Además, esta disposición admite la situación en la que el acceso al servicio OCSP está restringido a los propietarios de certificados o está sujeto a cargos. Los servidores de seguridad nunca incluyen el campo “nonce” en la petición OCSP. Esto permite que el servicio OCSP emplee varias estrategias de optimización, como la creación previa de las respuestas OCSP.

Debido a que las respuestas OCSP se utilizan en el proceso de validación de certificados, el error del servicio OCSP deshabilita eficazmente el intercambio de mensajes de X-Road. Cuando las respuestas OCSP almacenadas en caché no se pueden actualizar, los servidores de seguridad no son capaces de comunicarse. Por lo tanto, la duración de las respuestas OCSP determina la cantidad máxima de tiempo que el servicio OCSP puede no estar disponible. La duración es definida por el propietario del servidor central y puede variar entre diferentes instancias de X-Road.

3.7.8 Protocolo de Estampa Cronológica de Tiempo -TSA

Los servidores de seguridad utilizan el protocolo de Estampa de Tiempo (TSA) para garantizar integridad y autenticidad a largo plazo de los mensajes intercambiados. Los servidores de seguridad registran todos los mensajes y sus firmas. Estos registros se marcan periódicamente para crear evidencias a largo plazo. Es un protocolo sincrónico proporcionado por la autoridad certificadora. Sin embargo, los servidores de seguridad utilizan el protocolo de estampa de tiempo de forma asincrónica. Los servidores de seguridad registran todos los mensajes que se intercambian con otros servidores de seguridad. Estos mensajes se marcan de forma asincrónica mediante la estampa de tiempo por lotes. Esto se hace para desacoplar la disponibilidad del intercambio de mensajes con la disponibilidad de la autoridad certificadora, para disminuir la latencia del intercambio de mensajes y para reducir la carga en la autoridad de certificación en el servicio de estampa de tiempo. Debido a que el servicio de estampa cronológica de tiempo se utiliza de forma asincrónica, en caso de indisponibilidad temporal del servicio de estampa de tiempo no afecta directamente al intercambio de mensajes de X-Road. Sin embargo, si los servidores de seguridad no pueden marcar el tiempo los mensajes acumulados para cierto período de tiempo entonces puede ser difícil probar la hora exacta de los mensajes intercambiados. Para minimizar este riesgo los servidores de seguridad dejarán de reenviar mensajes si el tiempo de estampa ha estado fallando durante algún tiempo. El período de tiempo máximo permitido entre el registro de un mensaje y la adquisición de una marca de tiempo para un mensaje se define por el propietario del servidor central.

4. Arquitectura de secuencia para el registro en la PDI

La siguiente es la arquitectura de secuencia corresponde a las interacciones que se realizan en los componentes de la plataforma de interoperabilidad para el proceso de creación de los certificados digitales y servicios de estampa en el servidor central y el registro del servidor central de seguridad y los servidores de seguridad de las entidades.