INFORME TÉCNICO
VINCULACIÓN A SERVICIOS CIUDADANOS BASE /X-ROAD DE EMPRESAS PRIVADAS

Contexto

Conforme al principio de "masificación del gobierno en línea", hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2o de la Ley 1341 de 2009, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones.

De acuerdo con el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones (DUR- TIC), la Política de Gobierno Digital se desarrolla a través de un esquema que articula los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo

Según el mismo artículo 2.2.9.1.2.1 del DUR-TIC, los sujetos obligados desarrollarán las capacidades que les permitan ejecutar las Líneas de Acción de la Política de Gobierno Digital, mediante la implementación, entre otros, del habilitador de los Servicios Ciudadanos Digitales, que busca desarrollar, mediante soluciones tecnológicas, las capacidades de los sujetos obligados a la Política de Gobierno Digital para mejorar la interacción con la ciudadanía y garantizar su derecho a la utilización de medios digitales ante la administración pública.

El artículo 9o del Decreto 2106 de 2019, "*por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública*", señala que las autoridades deberán integrarse y hacer uso del modelo de Servicios Ciudadanos Digitales y se implementarán por parte de las autoridades de conformidad con los estándares que establezca el MinTIC.

El numeral 13 del artículo 2.2.17.1.4. del DUR-TIC define los Servicios Ciudadanos Digitales como el conjunto de soluciones y procesos transversales que brindan al Estado capacidades y eficiencias para su transformación digital y para lograr una adecuada interacción con el ciudadano, garantizando el derecho a la utilización de medios electrónicos ante la administración pública. Estos servicios se clasifican en servicios base y servicios especiales.

Los numerales 6 y 7 del mismo artículo 2.2.17.1.4. definen la Guía de lineamientos de los servicios ciudadanos digitales como "*el documento expedido y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones, el cual incluye las condiciones necesarias que el Articulador debe cumplir con el fin de garantizar*

la correcta prestación de los servicios ciudadanos digitales"; y, la Guía para vinculación y uso de los servicios ciudadanos digitales como "*el documento expedido y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones destinado a las autoridades y que indica las condiciones necesarias y los pasos que éstas deben realizar para la preparación, adecuación, integración, uso y apropiación de los servicios ciudadanos digitales, a través de los cuales podrán integrar a sus sistemas de información los mecanismos de autenticación digital, interoperabilidad, carpeta ciudadana digital y vincularlos al Portal Único del Estado colombiano*".

El artículo 2.2.17.4.1. del DUR-TIC señala como obligaciones del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en concordancia con el numeral 2, literal a. del artículo 18 de la Ley 1341 de 2009, entre otras, expedir y publicar la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de los servicios ciudadanos digitales, estas fueron publicadas para participación ciudadana entre los días 5 de junio y el 6 de julio de 2020.

Mediante la Resolución 2160 de 2020, el Ministerio de las Tecnologías de la Información y las Comunicaciones expidió la "*Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos*".

En Colombia existen entidades privadas que están habilitadas para ejercer funciones públicas de acuerdo con los casos taxativamente señalados en la Constitución Política (artículos 48, 49, 68, 123, 210 y 365) y la ley. Estas entidades pueden investirse de la autoridad del Estado. Dentro de las actividades que pueden ser desarrolladas por privados, se encuentran:

1. La seguridad social
2. La atención en salud
3. El saneamiento ambiental
4. La educación
5. La que desarrollan los notarios y los registradores

En este contexto, los servicios públicos son inherentes a la finalidad social del Estado y es deber de éste asegurar su prestación eficiente a todos los habitantes del territorio nacional.

Teniendo en cuenta lo anterior y en el proceso de vinculación a los Servicios Ciudadanos Digitales (SCD) Base (Decreto 620[1] y Resolución 2160[2], ambos de 2020) por parte de las Entidades Públicas de orden nacional y territorial, y en

[1] "*Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales*".

[2] "*Por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos*".

especial en el desarrollo de algunos proyectos propios de algunas de las entidades privadas que prestan o realizan actividades públicas, se ha evidenciado la necesidad de contar con información cuya fuente primaria son entidades privadas o se evidencia la necesidad de la participación de estas últimas respetando el Hábeas Data y la reserva de la misma.

Por ejemplo, en el proyecto de Interoperabilidad de la Historia Clínica Electrónica (Ley 2015[3] de 2020) se requiere el intercambio de información de la historia clínica de Instituciones Prestadoras de Servicios de Salud (IPS) Públicas y Privadas; en el proyecto de diseño de automatización del trámite de cargue y validación de contratos en el Sistema Electrónico para la Contratación Pública (SECOP), Colombia Compra Eficiente y la Superintendencia Financiera de Colombia, manifestaron la necesidad de que sean las empresas aseguradoras quienes proporcionen la información sobre las pólizas de seguro de los contratos.

Por necesidades como las enunciadas anteriormente es necesario vincular al SCD Base de Interoperabilidad a estas entidades privadas, por lo que se hace necesario precisar las condiciones legales, administrativas, funcionales y técnicas que correspondan.

Justificación

En particular, en el avance del proceso de vinculación a los Servicios Ciudadanos Digitales, se está trabajando, desde MinTIC en coordinación con Ministerio de Salud y Protección Social (MinSalud), en el proyecto de Interoperabilidad de datos de la Historia Clínica Electrónica, proceso que requiere obligatoriamente la participación de las IPS públicas y privadas con el Ministerio de Salud y Protección Social, por las razones expuestas a continuación:

Uno de los derechos fundamentales de las personas, es el derecho a la salud (artículos 44 y 49 de la Constitución) mediante condiciones de accesibilidad, oportunidad y continuidad adecuadas respecto de los servicios prestados. Actualmente los prestadores de servicios de salud requieren datos de la Historia Clínica de las personas para apoyar el proceso de atención de salud, pero esta se encuentra de forma fragmentada y no estandarizada por cada uno de los prestadores de servicios de salud con los cuales un individuo se relaciona, lo que genera inconvenientes en la calidad, oportunidad y continuidad de la atención del mismo. Para tal efecto, actualmente se desarrollan procesos de transformación digital[4] en el sector de la salud, en donde se han establecido los principios, las definiciones normativas y técnicas, los elementos de datos a interoperar, estándares

[3] "*Por medio del cual se crea la Historia Clínica Electrónica interoperable y se dictan otras disposiciones*".
[4] De acuerdo con el Decreto 1263 de 2022 la Transformación Digital "*Corresponde al proceso de explotación de tecnologías digitales que tiene la capacidad de crear nuevas formas de hacer las cosas en todos los sectores de la administración pública, generando nuevos modelos de desarrollo, procesos y la creación de productos y servicios, que a su vez producen valor, principalmente a través de la digitalización que representa la conversión de datos y procesos análogos hacia formatos que pueden ser entendidos y procesados por máquinas*".

internacionales a utilizar, protocolos de seguridad y en general los lineamientos que permitan avanzar en esta vía, pero garantizando la reserva y confidencialidad de la información que se comparte. Estos lineamientos y reglamentaciones se deben establecer por parte del Ministerio de Salud y Protección Social y el Ministerio de Tecnologías de la Información y las Comunicaciones.

Las tecnologías de la información y las comunicaciones (artículo 6° Ley 1341 de 2009, modificado por el artículo 5 Ley 1978 de 2019) aplicadas en el campo de la salud tienen el potencial de optimizar el gasto, mejorar la calidad asistencial, contribuir a la seguridad y la equidad en la atención de los pacientes. Por otro lado, el sector salud en Colombia demanda un alto grado de intercambio de información entre las IPS, tanto públicas como privadas, para mejorar la continuidad en la asistencia médica, contar a tiempo con la información de las personas, fortalecer la toma de decisiones por parte de los profesionales de la salud, agilizar el acceso y ejercicio de los derechos a la salud, combatir la corrupción y fomentar la competitividad del sector y del país.

En Colombia, la información clínica de los pacientes se encuentra actualmente fragmentada y dispersa en múltiples bases de datos, múltiples sistemas de información y tecnologías no integradas.

Dado lo anterior, en coordinación entre el Ministerio de Tecnologías de la Información y las Comunicaciones y el Ministerio de Salud y Protección Social, en Colombia se ha desarrollado el Modelo tecnológico de Interoperabilidad de datos de la Historia Clínica Electrónica – IHCE. Modelo que permite que los prestadores de servicios de salud realicen el intercambio de un conjunto de datos clínicos y administrativos de un paciente, utilizando además estándares semánticos y técnicos internacionales, con lo cual se buscan obtener los beneficios ya mencionados.

Este mecanismo beneficia a toda persona en Colombia que requiera de la prestación de un servicio de salud, indistintamente de su posición geográfica, si pertenece o no a uno de los regímenes del sistema de seguridad social en Colombia o si es nacional o extranjero. Al menos 50 millones de colombianos se verán beneficiados.

La IHCE se desarrolló en el marco de la Política de Gobierno Digital a través de la utilización de los Servicios Ciudadanos Digitales, los cuales tienen tres componentes: 1) Autenticación Digital, 2) Interoperabilidad herramienta X-Road, y 3) Carpeta Ciudadana Digital. Además, se aplican las políticas de seguridad y privacidad de la información, datos abiertos, inteligencia artificial, "*machine learning*" y "*block chain*" para la generación de política pública en el país y de esta manera poder encaminar al Estado colombiano hacia la incorporación a la Cuarta Revolución Industrial.

En Colombia, se avanza en la implementación del modelo en las regiones a través de los prestadores de servicios de salud públicos, sin embargo, el servicio de salud en el país es prestado también por entidades privadas lo que permite la

universalidad y el cubrimiento del servicio de salud pública en más del 95% de la población del país. Al implementar el modelo de interoperabilidad de datos de la historia clínica en Colombia, utilizando la plataforma de interoperabilidad del Estado Colombiano, es decir la herramienta X-Road, resulta necesario incluir al sector privado de salud en el uso de dicha herramienta, asegurando como ya se mencionó condiciones de confidencialidad, integridad, accesibilidad, oportunidad y continuidad adecuadas.

La Ley 100 de 1993 en su artículo 4 establece: "*La Seguridad Social es un servicio público obligatorio, cuya dirección, coordinación y control están a cargo del Estado y que será prestado por las entidades públicas o privadas en los términos y condiciones establecidos en la presente Ley*".

Adicional a lo anterior, la Ley 2015 de 2020, por medio de la cual se crea la historia clínica interoperable, establece en el artículo 3, correspondiente al ámbito de aplicación, lo siguiente:

> "*Los prestadores de servicios de salud están obligados a diligenciar y disponer los datos, documentos y expedientes de la historia clínica en la plataforma de interoperabilidad que disponga el Gobierno Nacional*".

Además, el artículo 4° (Reglamentación y administración) de la citada Ley establece:

> "*Los Ministerios de Salud y Protección Social y el de Tecnologías de la Información y las Comunicaciones, o aquellos que hagan sus veces, reglamentarán el modelo de Interoperabilidad de la Historia Clínica Electrónica. El Ministerio de Salud y Protección Social administrará el modelo de Interoperabilidad de la Historia Clínica Electrónica (IHCE) y el Ministerio de Tecnologías de la Información y las Comunicaciones será el responsable de la administración de la herramienta tecnológica de la plataforma de interoperabilidad.*
>
> *Parágrafo. El modelo de Interoperabilidad de la Historia Clínica Electrónica deberá ser reglamentado en un término máximo de doce (12) meses, contados a partir de la entrada en vigencia de la presente ley*". (Subrayado fuera de texto)

En el artículo 12 de la ley antes citada se establece la prohibición de divulgar datos de cualquier persona consignados en la Historia Clínica Electrónica y en el artículo 13 se establecen disposiciones generales en cuanto a la Seguridad de la información y seguridad digital.

Y finalmente, la Resolución 866 de 2021 del Ministerio de Salud y Protección Social que reglamenta inicialmente la Ley 2015 de 2020 establece:

> "*Artículo 2. Ámbito de aplicación. Las disposiciones contenidas en el presente acto administrativo serán aplicables a los actores que a continuación se*

relacionan, quienes deberán cumplir los lineamientos y estándares establecidos en el marco de interoperabilidad para Gobierno Digital y el modelo de seguridad y privacidad de la política de gobierno digital:

2.1 La persona titular de la historia clínica.
2.2 Los prestadores de servicios de salud públicos y privados.
2.3 Las Entidades Promotoras de Salud -EPS.
2.4 Las Entidades Adaptadas al Sistema General de Seguridad Social en Salud - SGSSS.
2.5 Las Entidades que administren planes voluntarios de salud.
2.6 Las Administradoras de Riesgos Laborales y los fondos de pensiones en sus actividades de salud.
2.7 Las entidades pertenecientes a los Regímenes de Excepción o Especial de salud, Las secretarias, institutos y unidades administrativas departamentales, distritales y municipales de salud, siempre que accedan a la información de forma innominada.
2.9 Las compañías de seguros que emiten pólizas de seguros de accidentes de tránsito, siempre que tengan la autorización del titular de la información o de quien este legitimado para autorizar el conocimiento de los datos.

(…)

Artículo 23. Servicios ciudadanos digitales. Los sujetos referidos en el artículo 2° de la presente resolución deberán cumplir las condiciones y estándares establecidos en la guía para vinculación y uso de los servicios ciudadanos digitales que se encuentran señaladas en el Anexo Técnico 2 de la Resolución 2160 de 2020, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, para la preparación, adecuación, integración, uso y apropiación de los servicios ciudadanos digitales, a través de los cuales podrán integrar a sus sistemas de información los mecanismos de interoperabilidad".

Desarrollo técnico

Para realizar la conexión de los servidores de seguridad de entidades privadas que están habilitadas para ejercer funciones públicas y sus servicios al ecosistema de producción de X-Road o la consulta de información desde entidades públicas, cuya fuente primaria son entidades particulares, la Entidad Privada deberá adquirir un certificado de autenticación digital y un certificado de firma a una de las Entidades de Certificación Digital con acreditación vigente en el Organismo Nacional de Acreditación Nacional – ONAC, en los términos de la Ley 527 de 1999, para que estos sean importados en el servidor de seguridad al momento de la configuración.

La Entidad de Certificación Digital dispondrá de un mecanismo para que la entidad privada pueda realizar la solicitud de los certificados y la solicitud de firma de los Certificados.

Si bien las entidades públicas reciben los certificados de manera gratuita por parte de la Agencia Nacional Digital a través de la Entidad de Certificación Digital, en el caso de las entidades privadas no sucede lo mismo y deberán entregar a la Agencia Nacional Digital la siguiente configuración: Certificados de autenticación digital y firma, URL, Autoridad de Estampa de Tiempo y el Protocolo de comprobación del estado del certificado en línea (OCSP por sus siglas en inglés: *Online Certificate Status Protocol*), con el propósito de realizar las respectivas configuraciones nivel central. Los certificados de la Entidad de Certificación (CA por sus siglas en inglés *Certification Authority*), deberán cumplir con las siguientes especificaciones técnicas:

1. Los certificados emitidos deben permitir la compatibilidad e integración con el sistema X-Road para el intercambio de información con la versión 6.25 Colombia.
2. Estructura del certificado de la CA-Subordinada:
    a. La estructura del certificado subordinado se genera a partir de certificado Raíz de la Entidad de Certificación Digital.
    b. Algoritmo de firma: SHA256.
    c. Uso de Claves: contener el uso de firma de certificados y firma de lista de revocación de certificados.
    d. Usos Mejorados: contener el uso de firma de OCSP.
3. Estructura de los certificados de firma y autenticación digital.

Los certificados de firma y autenticación digital emitidos son firmados por la Subordinada de la Entidad de Certificación Digital, las solicitudes de estos certificados se generan desde los servidores de seguridad de X-Road bajo la extensión (.PEM) y bajo el formato X.509 para dos (2) usos: Firma y Autenticación de Servidores de seguridad.

Al recibir la petición, la Entidad de Certificación Digital, construye un certificado X.509 con base en el nombre y la llave pública que está en la petición del certificado y datos propios del mismo con extensión (.CRT).

Los certificados de firma digital de persona jurídica deben tener las siguientes características:

Emitido por: Certificado subordinado de la Entidad de Certificación Digital.

1. Algoritmo de firma: SHA256.
2. Uso de Claves: Sin repudio.
3. Acceso a información de autoridad:
    a. Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)
    b. Nombre alternativo: URL=https:// Url del servicio para OCSP
    c. Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2)
    d. Nombre alternativo: URL=https:// Url nombre alternativo

La Entidad de Certificación Digital debe estar acreditada por el Organismo Nacional de Acreditación de Colombia – ONAC, dando cumplimiento al artículo 161 del Decreto-Ley 019 de 2012, en las siguientes actividades:

a. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.
b. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.
c. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.

El servicio de Estampa Cronológica de Tiempo debe cumplir las siguientes características:

1. El servicio de Estampa cronológica de tiempo debe permitir la compatibilidad e integración con el sistema X-Road versión 6.25 Colombia para el intercambio de información.

2. Prestar el Servicio de Estampado Cronológico (Timestamping) como mecanismo on-line que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. La implementación debe cumplir con el protocolo definido en la norma RFC 3161 "*Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*" o posteriores.

3. El servicio no deberá leer el contenido de los mensajes de datos para estampar la Transacción.

4. La Entidad de Certificación mantendrá un registro de las estampas emitidas para su futura verificación.

5. El servicio de estampa cronológica deberá soportar un rendimiento de mínimo 1000 transacciones criptográficas por segundo de las operaciones de firma.

6. Una solicitud Autoridad de Estampa de Tiempo que utiliza el método POST se construye de la siguiente manera: El encabezado Content-Type tiene el valor "application/timestamp-query", mientras que el cuerpo del mensaje es el valor binario Time-Stamp Request Message.

7. Una respuesta Autoridad de Estampa de Tiempo basada en HTTP se compone del valor binario de la codificación del Time-Stamp Response Message. El encabezado

   Content-Type tiene el valor "application/timestamp-reply".
   URL: url del servicio de Autoridad de Estampa de Tiempo

Método: Post
Parámetro: Header = Content – Type (application/timestamp-query)
Body = TimeStampRequest
Returns: Header = Content – Type (application/timestamp-reply)
Body = TimeStampResponse.

8. El servicio de Autoridad de Estampa de Tiempo debe ser provisto haciendo uso de las librerías criptográficas Bouncy Castle (OpenSource), bajo el RFC 3161. La solicitud (request) al servicio de Autoridad de Estampa de Tiempo se realiza haciendo uso del algoritmo de cifrado 2.16.840.1.101.3.4.2.3 de la librería BouncyCastle correspondiente al algoritmo SHA512. El response del servicio se realiza haciendo uso del algoritmo de cifrado 1.3.14.3.2.26, el cual corresponde al algoritmo SHA1.

9. La entidad privada deberá en conjunto con la entidad certificadora que presta el servicio de Autoridad de Estampa de Tiempo, llevar el control / filtro de consumo de las estampas, utilizando los mecanismos que considere adecuados.

El protocolo de comprobación del estado de un certificado en línea (OCSP) debe cumplir las siguientes características:

1. El protocolo de comprobación del estado de un certificado en línea debe permitir la compatibilidad e integración con el sistema X-Road para el intercambio de información.
2. Integrar a la plataforma de X-Road el servicio de OCSP que permita por medio de una URL verificar el estado de los certificados vigentes o revocados dando pleno cumplimiento al RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
3. Una solicitud OCSP que utiliza el método POST y se debe construir de la siguiente manera: El encabezado Content-Type tiene el valor “application/ocsp-request”, mientras que el cuerpo del mensaje es el valor binario de la OCSPRequest.
4. Una respuesta OCSP basada en HTTP se debe componer del valor binario de la codificación del OCSPResponse. El encabezado Content-Type tiene el valor “aplicación/ocsp-response” este encabezado especifica la longitud de la respuesta.
   URL: Url del servicio de OCSP
   Método: Post
   Parametro: Header = Content-Type (application/ocsp-request)
   Body = {
   TBSRequest
   }
   Respuesta: Header = Content-Type (application/ocsp-response)
   Body = {
   OCSPResponseStatus,
   OCSPCertificado

}

La validez del certificado debe poder verificarse cada 50 minutos contra el servicio de OCSP expuesto por la Entidad de Certificación Digital. En la respuesta de este servicio se debe establecer el parámetro NextUpdate en 50 minutos.

El servicio de OCSP debe ser provisto haciendo uso de las librerías criptográficas Bouncy Castle, bajo el RFC 6960. La solicitud (request) al servicio de OCSP se realiza haciendo uso del algoritmo 1.3.14.3.2.26 de BouncyCastle, el cual equivale al algoritmo SHA1. El response del servicio OCSP se realiza haciendo uso del algoritmo 1.2.840.113549.1.1.5 corresponde al algoritmo SHA1 con RSA de la librería BouncyCastle para la verificación de la firma del servicio OCSP.

Conclusiones y recomendaciones

Teniendo en cuenta todas las consideraciones anteriores y dado que en Colombia el servicio de salud en el país es prestado tanto por empresas públicas como privadas, lo que permite el cubrimiento del servicio de salud pública en más del 95% de la población del país, al obedecer el mandato de la Ley 2015 de 2020 y la Resolución 866 del 2021[5] de implementar el modelo de interoperabilidad de datos de la historia clínica en Colombia utilizando la plataforma de interoperabilidad del estado Colombiano, es decir la herramienta X-Road, estamos hablando de que se debe incluir al sector privado de salud en Colombia asegurando, como ya se mencionó, condiciones de accesibilidad, oportunidad y continuidad adecuadas del servicio de salud en el país.

Así mismo, es necesario contar con la especificación de condiciones técnicas, jurídicas y administrativas necesarias para la eventual vinculación de entidades privadas al intercambio de información a través de X-Road, cuyos datos sean indispensables para la transformación digital de trámites y servicios de las entidades del Estado.

Ante lo anterior, se propone realizar el siguiente ajuste al anexo 2 de la Resolución 2160 de 2020.

Detalle de los ajustes:

Se incluyen las secciones 6.6.7 y 6.6.8 de la siguiente forma:

> **6.6.7.** Proceso de solicitud de certificados digitales para Entidades Privadas

Para realizar la conexión de los servidores de seguridad de entidades privadas y sus servicios al ecosistema de producción de X-Road, la Entidad Privada deberá adquirir un certificado de autenticación digital y un certificado de firma a una de las

[5] Expedida por el Ministerio de Salud y Protección Social.

Entidades de Certificación Digital con acreditación vigente en el Organismo Nacional de Acreditación Nacional - ONAC, para que estos sean importados en el servidor de seguridad al momento de la configuración. La Entidad de Certificación Digital dispondrá de un mecanismo para que la entidad privada pueda realizar la solicitud de los certificados y la solicitud de firma de los certificados.

El proceso general de la solicitud de certificados que se describe a continuación es un ejemplo del proceso, este puede diferir dependiendo de las Entidades de Certificación Digital:

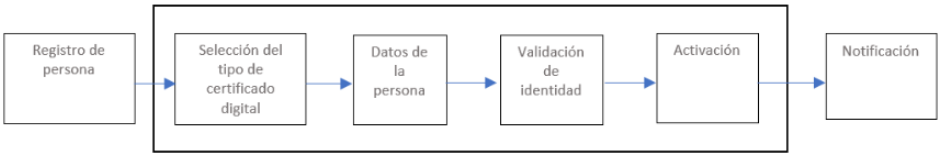

Figura 91 Proceso de solicitud de certificados
(Fuente: Suministrada por la Agencia Nacional Digital)

Registro de persona: El representante legal de la entidad privada o quien haga sus veces deberá hacer el registro y la solicitud de los certificados digitales en el portal de la Entidad de Certificación Digital.

Selección de tipo de certificado digital: El producto que se debe seleccionar es el tipo de certificado perteneciente a persona jurídica.

Datos de la persona: El representante legal de la entidad privada o quien haga sus veces deberá diligenciar un formulario con datos del Prestador Privado y personales.

Validación de identidad: El representante legal de la entidad privada o quien haga sus veces deberá cargar los documentos que acrediten la relación laboral con el Prestador Privado.

Activación: La Entidad de Certificación Digital revisará y aprobará la solicitud.

Notificación: El CIO, director o jefe del área de tecnologías de la información recibirá una notificación al correo electrónico registrado con el estado de la solicitud. El proceso general para la solicitud de la firma de los certificados digitales que se generan desde el servidor de seguridad es el siguiente.

Figura 20 Proceso de firma de certificados
(Fuente: Suministrada por la Agencia Nacional Digital)

Inicio de sesión: El representante legal de la entidad privada o quien haga sus veces deberá ingresar las credenciales creadas en el proceso anterior.

Buscar solicitud: Ingresar y buscar el ID de la solicitud enviado al correo electrónico registrado.

Generar certificados: Generar desde el Servidor de Seguridad en formato (.PEM) las solicitudes de firma de los certificados y proceder a firmarlos a través de la entidad certificadora correspondiente. En la siguiente sección se detallará el proceso de generación de los certificados.

Solicitudes finalizadas: Buscar en la opción de solicitudes finalizadas y descargar los certificados firmados por la Entidad de Certificación Digital. La entidad deberá almacenar estos certificados de manera segura de acuerdo con su política de seguridad y privacidad de la información.

Cerrar Sesión: Salir del portal de firma de certificados de la Entidad de Certificación Digital.

6.6.8. Condiciones técnicas de los certificados que deben proporcionar las Entidades Privadas

Si bien las entidades públicas reciben los certificados de manera gratuita por parte de la Agencia Nacional Digital a través de la Entidad de Certificación Digital, en el caso de las entidades privadas no sucede lo mismo y deberán entregar a la Agencia Nacional Digital la siguiente configuración: Certificados de autenticación digital y firma, URL, Autoridad de Estampa de Tiempo y OCSP, con el propósito de realizar las respectivas configuraciones a nivel central.

Los certificados CA, deberán cumplir con las siguientes especificaciones técnicas:

1. Los certificados emitidos deben permitir la compatibilidad e integración con el sistema X-Road para el intercambio de información con la versión 6.25 Colombia.
2. Estructura del certificado de la CA-Subordinada:

a. La estructura del certificado subordinado se genera a partir de certificado Raíz la Entidad de Certificación Digital.

b. Algoritmo de firma: SHA256.
c. Uso de Claves: contener el uso de firma de certificados y firma de lista de revocación de certificados.
d. Usos Mejorados: contener el uso de firma de OCSP.

3. Estructura de los certificados de firma y autenticación digital.

Los certificados de firma y autenticación digital emitidos son firmados por la Subordinada de la Entidad de Certificación Digital, las solicitudes de estos certificados se generan desde los servidores de seguridad de X-Road bajo la extensión (.PEM) y bajo el formato X509 para dos (2) usos: Firma y Autenticación de Servidores de seguridad.

Al recibir la petición, la Entidad de Certificación Digital, construye un certificado X.509 con base en el nombre y la llave pública que está en la petición del certificado y datos propios del mismo con extensión (.CRT).

Los certificados de firma digital de persona jurídica deben tener las siguientes características:

Emitido por: Certificado subordinado de la Entidad de Certificación Digital.

1. Algoritmo de firma: SHA256.
2. Uso de Claves: Sin repudio
3. Acceso a información de autoridad:
    a. Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)
    b. Nombre alternativo: URL=https:// Url del servicio para OCSP
    c. Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2)
    d. Nombre alternativo: URL=https:// Url nombre alternativo

La Entidad de Certificación Digital debe estar acreditada por el Organismo Nacional de Acreditación de Colombia – ONAC, dando cumplimiento al artículo 161 del Decreto Ley 019 de 2012, en las siguientes actividades:

a. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.
b. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.
c. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.

El servicio de Estampa Cronológica de Tiempo debe cumplir las siguientes características:

1. El servicio de Estampa cronológica de tiempo debe permitir la compatibilidad e integración con el sistema X-Road versión 6.25 Colombia para el intercambio de información.

2. Prestar el Servicio de Estampado Cronológico (Timestamping) como mecanismo on-line que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. La implementación debe cumplir con el protocolo definido en la norma RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)” o posteriores.

3. El servicio no deberá leer el contenido de los mensajes de datos para estampar la transacción.

4. La Entidad de Certificación mantendrá un registro de las estampas emitidas para su futura verificación.

5. El servicio de estampa cronológica deberá soportar un rendimiento de mínimo 1000 transacciones criptográficas por segundo de las operaciones de firma.

6. Una solicitud Autoridad de Estampa de Tiempo que utiliza el método POST se construye de la siguiente manera: El encabezado Content-Type tiene el valor “application/timestamp-query”, mientras que el cuerpo del mensaje es el valor binario Time-Stamp Request Message.

7. Una respuesta Autoridad de Estampa de Tiempo basada en HTTP se compone del valor binario de la codificación del Time-Stamp Response Message. El encabezado Content-Type tiene el valor “application/timestamp-reply”.
   URL: url del servicio de Autoridad de Estampa de Tiempo
   Método: Post
   Parámetro: Header = Content – Type (application/timestamp-query)
   Body = TimeStampRequest
   Returns: Header = Content – Type (application/timestamp-reply)
   Body = TimeStampResponse.

8. El servicio de Autoridad de Estampa de Tiempo debe ser provisto haciendo uso de las librerías criptográficas Bouncy Castle (OpenSource), bajo el RFC 3161. La solicitud (request) al servicio de Autoridad de Estampa de Tiempo se realiza haciendo uso del algoritmo de cifrado 2.16.840.1.101.3.4.2.3 de la librería BouncyCastle correspondiente al algoritmo SHA512. El response del servicio se realiza haciendo uso del algoritmo de cifrado 1.3.14.3.2.26, el cual corresponde al algoritmo SHA1.

9. La entidad privada deberá en conjunto con la entidad certificadora que presta el servicio de Autoridad de Estampa de Tiempo, llevar el control / filtro de consumo de las estampas, utilizando los mecanismos que considere adecuados.

El protocolo de comprobación del estado de un certificado en línea debe cumplir las siguientes características:

1. El protocolo de comprobación del estado de un certificado en línea debe permitir la compatibilidad e integración con el sistema X-Road para el intercambio de información.

2. Integrar a la plataforma de X-Road el servicio de OCSP que permita por medio de una URL verificar el estado de los certificados vigentes o revocados dando pleno cumplimiento al RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

3. Una solicitud OCSP que utiliza el método POST y se debe construir de la siguiente manera: El encabezado Content-Type tiene el valor "application/ocsp-request", mientras que el cuerpo del mensaje es el valor binario de la OCSPRequest.

4. Una respuesta OCSP basada en HTTP se debe componer del valor binario de la codificación del OCSPResponse. El encabezado Content-Type tiene el valor "aplicación/ocsp-response" este encabezado especifica la longitud de la respuesta.
   URL: Url del servicio de OCSP
   Método: Post
   Parametro: Header = Content-Type (application/ocsp-request)
   Body = {
   TBSRequest
   }
   Respuesta: Header = Content-Type (application/ocsp-response)
   Body = {
   OCSPResponseStatus,
   OCSPCertificado
   }

La validez del certificado debe poder verificarse cada 50 minutos contra el servicio de OCSP expuesto por la Entidad de Certificación Digital. En la respuesta de este servicio se debe establecer el parámetro NextUpdate en 50 minutos.

El servicio de OCSP debe ser provisto haciendo uso de las librerías criptográficas Bouncy Castle, bajo el RFC 6960. La solicitud (request) al servicio de OCSP se realiza haciendo uso del algoritmo 1.3.14.3.2.26 de BouncyCastle, el cual equivale al algoritmo SHA1. El response del servicio OCSP se realiza haciendo uso del algoritmo 1.2.840.113549.1.1.5 corresponde al algoritmo SHA1 con RSA de la librería BouncyCastle para la verificación de la firma del servicio OCSP.

Adicionalmente se ajusta la sección 8.4.1 en concordancia a lo anterior incluyendo el siguiente texto:

(…) Aunque dentro del carpeta ciudadana la entidad puede publicar servicios independientes, se recomienda, como una buena práctica, tener un servicio de consulta de información bajo el cual se publicarán los otros servicios de historiales y alertas.

BIBLIOGRAFÍA

- Ley 2015 de 2020, por medio del cual se crea la historia clínica electrónica interoperable y se dictan otras disposiciones.
- Resolución 866 de 2021 del Ministerio de Salud y Protección Social, por la cual se reglamenta el conjunto de elementos de datos clínicos relevantes para la interoperabilidad de la historia clínica.
- Resolución 2160 de 2020 del Ministerio de Tecnologías de la Información y las Comunicaciones, por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos.
- Decreto número 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones (DUR- TIC), título IX Y XVII.