Programa Salud.uy
Historia Clínica Electrónica Nacional

Guía de implementación Firma electrónica de documentos Clínicos

Elaborado por el Programa Salud.uy en el marco del Convenio firmado por Presidencia de la República, Ministerio de Economía y Finanzas, Ministerio de Salud Pública y la Agencia de Gobierno Electrónico y Sociedad de la Información.

Liniers 1324
Torre Ejecutiva Sur - piso 3
Tel./Fax: (+598) 2901.2929*
Email: salud.uy@agesic.gub.uy
Montevideo - Uruguay

Edición	2013-01
Responsable	Componente Historia Clínica Electrónica Nacional
Revisión	Salud.uy
Aprobación	Comité de Dirección Programa Salud.uy
Nombre Archivo	SaludUy_FirmaElectronica_0.5
Fecha	17/10/2013

Índice de contenido

1 Introducción

1.1 Antecedentes

Los procesos de intercambio de información en salud, requieren la definición de estrategias para velar por la autenticidad, integridad y validez de los datos que son llevados de un lugar a otro; dado el nivel de confidencialidad y de criticidad que puede resultar la información propia con relación al estado de las condiciones de salud de la persona.

A nivel de firma electrónica avanzada, la seguridad informática ha evolucionado en sus diferentes técnicas (criptografía, firma digital, procesos de infraestructura, entre otros), para brindar la confianza e integridad a los documentos que son intercambiados electrónicamente, permitiendo que estos sean válidos y verificables por mecanismos fiables.

Uruguay a partir de la ley 18600 de 2009 cuenta con normativa de firma electrónica, y ha desarrollado la infraestructura necesaria para que las organizaciones inicien su adopción y uso en los diferentes tipos de documentos que son generados por sus procesos.

El proyecto salud.uy por su parte, con el propósito de la puesta en marcha de la Historia Clínica Electrónica Nacional HCEN, avanza en su fase de definiciones; la HCEN estará conformada por documentos que son generados e intercambiados por las organizaciones asistenciales en donde los pacientes son atendidos, cuando estos documentos son accedidos para ser consultados, deben ser confiables, íntegros y veraces. Es necesario, entonces generar una aproximación inicial hacia el proceso de adopción de firma electrónica avanzada (cuando ella sea requerida), dentro de los documentos a intercambiar en salud, la cual haga uso de disposiciones y estándares de seguridad que Uruguay ya ha definido.

1.2 Propósito

El propósito de esta guía de implementación es brindar los fundamentos para el uso de firma electrónica avanzada en documentos clínicos electrónicos. La guía está dirigida a los ámbitos técnicos, asistenciales, jurídicos y administrativos de las organizaciones de salud, que requieren orientación en las definiciones de adopción y uso de firma electrónica en sus sistemas de información.

2 Alcance

Este documento es una guía de implementación de firma electrónica avanzada utilizando XML DSIG a través de las definiciones y la applet desarrollada por el área de Identificación Electrónica de Seguridad de la Información de AGESIC en documentos clínicos electrónicos, estos documentos pueden ser documentos HL7 V3 CDA r2 o documentos digitalizados.

3 Objetivo

Elaborar una guía de implementación de firma electrónica avanzada para documentos clínicos utilizando las definiciones de Identificación Electrónica de Seguridad de la Información de AGESIC.

4 Sobre esta guía

La guía se basa en las definiciones XML DSIG de W3C de firma digital, de igual manera, se tomaron en cuenta las definiciones de Identificación Electrónica de Seguridad de la Información de AGESIC; se revisó el documento que se encuentra a nivel en discusiones por los comités de trabajo de HL7 internacional "HL7 Implementation Guide for CDA® Release 2: Digital Signatures and Delegation of Rights Release 1, julio 2013", y el perfil de IHE "IHE Document Digital Signature (DSG) Profile".

La guía presenta los casos de uso y realiza una descripción de los procesos de implementación práctica.

4.1 Recomendaciones normativas

Uso de la notación XML y conocimiento de los componentes del RIM HL7 CDA, también sería de utilidad acceder a la *"Guía de implementación - estructura mínima nacional del documento clínico HL7 V3 CDA-R2"*.

4.2 Notaciones seguidas en la guía

La notación utilizada a continuación es la sugerida dentro de los documentos "Clinical Document Architecture (CDA) Release 2.0" y "Quick Start Guide for Simple CDA Release 2.0 Documents", por consiguiente los códigos de ejemplo se desplegarán con formato "Courier", y el color denotará la obligatoriedad del elemento o valor según la siguiente clasificación:

```
<ElementoRequerido requerido="Valorfijo" opcional="Valorvariable">
<ElementoOpcional requerido=" Valorvariable" opcional="Valorvariable">
```

El texto narrativo aparecerá en formato "Times New Roman"

elemento cuando un element XML se discute en un texto narrativo

atributo cuando un atributo XML se discute en un texto narrativo

En el presente documento existen referencias a la normativa de HL7 CDA- R2, a otras partes de la especificación y a otros documentos externos al estándar internacional. Siguen el formato: [x], y la referencia se puede consultar en el apartado de Referencias y Bibliografía del mismo.

Esta guía utiliza notación **XPATH**. El propósito de usar esta notación es proporcionar un mecanismo para identificar las partes de un documento XML sobre los cuales se pueda aplicar las restricciones enumeradas.

Ocasionalmente y de acuerdo al contexto, puede que no se exprese la raíz en el **XPATH** con el fin de abreviar las expresiones

4.3 Acciones previas con Firma Electrónica Avanzada

La guía retoma algunos de los principios de seguridad informática que se mencionan a continuación:

Criptografía

La criptografía se ocupa de las técnicas para cifrar y descifrar información, por medio de algoritmos, protocolos y sistemas con el propósito de que el intercambio de mensajes o de información solo pueda ser leída por quienes son sus destinatarios y que posean el medio para descifrarlos.

Dentro del intercambio de información, la criptografía busca los siguientes propósitos:

- Confidencialidad, que solo pueda acceder a la información el legítimo destinatario
- Integridad, que la información no pueda ser alterada sin esto ser detectado
- Autenticación, que tanto el emisor como el receptor puedan confirmar la identidad de la otra parte
- Vinculación o no repudio, vincula un documento o transacción a una persona o un sistema de gestión criptográfico automatizado,

Los principios de la criptografía son realmente sencillos, pero los procesos involucrados pueden resultar un poco complejos.

Criptografía de Clave Pública

O criptografía asimétrica, es el método que utiliza un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es *pública* y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la *confidencialidad* del envío

del mensaje, nadie salvo el destinatario puede descifrarlo.

Las Claves Públicas se generan por una autoridad de certificación (CA), quien necesita ser un tercero de confianza , genera claves privadas al azar y sus correspondientes claves públicas unidos a un usuario en particular. Las Autoridades Certificadoras emiten certificado con Datos del suscriptor y la Clave Pública

Certificados digitales

Los certificados de clave pública, conocidos como certificados digitales X.509, son utilizados para una gran variedad de propósitos como el de compartir una llave privada utilizada para encriptar información, para firmar electrónicamente documentos y para autenticar la identidad de la persona o entidad usando un mecanismo de desafío - respuesta.

Un certificado es un documento electrónico, contiene en general:

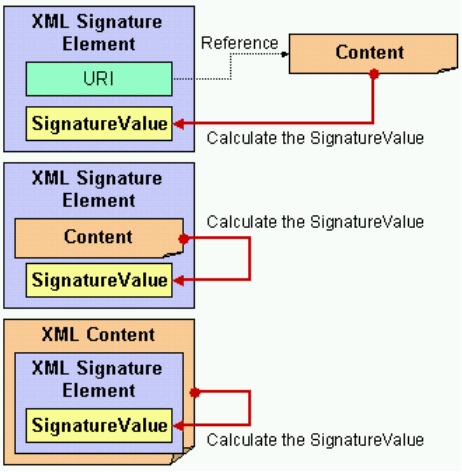
- Número de serie del certificado
- Clave pública del sujeto
- Nombre del Objeto
- Rango de fechas de validez
- Nombre de la autoridad de certificación (CA) que emitió el certificado digital
- Firma de la CA que emitió el certificado
- Huella digital - hash del certificado para asegurarse de que no ha sido manipulado
- Detalles de los algoritmos utilizados
- Las extensiones opcionales, tales como los fines para los cuales el certificado se puede utilizar por ejemplo, SMTP y S / MIME

El estándar actual recomendado es el X.509 V3, perfil del certificado definido en RFC 5280 (mayo de 2008) .

Certificado digitales en documentos XML

La recomendación de W3C para implementar firma electrónica en documentos XML es XML Digital Signature (tambié llamado XMLDsig, DSig XML, XML-Sig). Las firmas XML se pueden utilizar para firmar datos o recursos electrónicos de cualquier tipo, normalmente documentos XML, pero cualquier recurso digital accesible a través de una URL puede firmarse. En general existen diferentes alternativas para la implementación de una firma XML.

- Cuando se utiliza para firmar un recurso fuera del documento XML que la contiene se llama una firma separada (detached).
- Si se utiliza para firmar una parte del documento que la contiene, se llama una firma envuelta (enveloped).
- Si contiene los datos firmados dentro de sí mismo se llama una firma envolvente (enveloping).



5 Casos de uso

Dentro del documento se especifica el uso de firma electrónica avanzada y sencilla dentro de organizaciones que intercambian la información.

Los documentos electrónicos cada vez se utilizan más dentro de las organizaciones de la salud. En el ámbito sanitario, una firma valida la autoría del acto médico y la conformidad con lo que ello expresa. De esa manera, las firmas son parte de los procesos del registro del cuidado de la salud. Para permitir el intercambio de información confiable entre diferentes sistemas es necesario estándares que implementen la confidencialidad, integridad, y la vinculación o no repudio de los datos.

Los casos de uso, corresponden a escenarios en los cuales se viabilice el uso de la firma electrónica.

5.1 Consentimiento Clínico Informado

Si bien se han logrado importantes avances en la implementación de sistemas de información en la generación de documentos electrónicos dentro de las organizaciones de salud, es bastante común que continúen existiendo los documentos físicos, estos pueden corresponder a diferentes eventos obtenidos por procesos que aún no se soportan por los sistemas de información de la organización. Un caso son los reportes remitidos desde otros hospitales en donde se consigna información clínica del paciente o documentos que pueden ser firmados; otro caso son documentos físicamente firmados por los pacientes, como por ejemplo el documento del consentimiento clínico informado. Esta información pasa a ser parte de la Historia Clínica del paciente, y en algunos casos, acorde con el establecimiento de las políticas se puede firmar electrónicamente.

Cuando un documento ha sido digitalizado y firmado electrónicamente, es posible verificar que este es copia fiel de una fuente valida. Al verificar la firma, el documento es una copia fiel. De lo contrario, el documento puede tener una modificación y por lo tanto no ser confiable.

Un ejemplo de ello es el documento del consentimiento informado de cirugía, el paciente que será intervenido, debe leer y firmar físicamente el documento que ha diligenciado en presencia del profesional de salud, el documento que ha sido firmado con la rúbrica personal del paciente, es digitalizado por un tercero y llevado a un formato PDF. Una vez el documento se encuentra en formato PDF, es firmado con la firma electrónica avanzada por quien haya realizado la digitalización del documento. El uso de la firma electrónica avanzada, permite verificar que el documento sea el mismo que el original y que no ha sido modificado por error o intención, funcionalidad que valida la integridad del documento. Adicionalmente permite determinar la identidad del firmante y la razón de la firma.

5.2 Reporte Clínico en HL7 V3 CDA r2

Las aplicaciones informáticas hospitalarias generan documentos clínicos electrónicos, que corresponden a resultados de una observación asistencial o de un acto clínico, como es el caso de los resultados de laboratorio, reportes de imagen médica o informes de evolución de internación, el profesional de salud puede firmar electrónicamente este tipo de documentos.

Si un reporte ha sido generado utilizando firma electrónica, cuando es validado posteriormente, es posible verificar que este fue realizado por un profesional de salud, otorgándole validez, al contenido de información clínica.

Cuando el profesional de salud genera un reporte clínico dentro del sistema de información allí utiliza su firma electrónica y el sistema genera el reporte CDA con la firma envolvente; ha validado que el informe es completo y correcto, su validez se efectúa mediante el uso de una firma. Si hay una necesidad de verificar este reporte o documento clínico, la firma electrónica proporciona el mecanismo para llevar a cabo esta validación.

5.3 Prescripción electrónica de medicamentos

Este caso de uso hace mención al proceso de prescripción electrónica de medicamentos; las organizaciones implementan la automatización de la orden de medicamentos o prescripción electrónica, la cual es diligenciada directamente por el médico desde el HIS; para realizar la orden el médico debió ingresar con un sistema de usuario y contraseña al HIS, lo que para el caso es una forma de Firma Electrónica sencilla.

Cuando el profesional de la salud realiza la orden de medicamentos, esta acción es asociada a la identificación del médico; cuando la orden es enviada electrónicamente a la farmacia o a la dependencia encargada de verificar las solicitudes de medicamentos realizadas, es posible identificar tanto al médico que solicitó

la orden como los contenidos de la solicitud, proceso que optimiza la gestión de medicamentos y apoya el concepto de seguridad del paciente.

La firma electrónica sencilla (login y password) no es recomendable, en su lugar se recomienda la firma electrónica avanzada ya que se considera significativamente más segura.

Cuando los sistemas no son de la misma organización o no están conectados en línea, se puede también definir un procedimiento de interoperabilidad con o sin firma electrónica avanzada, para que el paciente reciba de la farmacia los medicamentos solicitados por el profesional de salud.

6 Implementación en HL7 V3 CDA r2

Dado que HL7 CDA es un documento XML, sobre el cual se estandarizan documentos clínicos interoperables, la recomendación de W3C para implementar firma electrónica en documentos XML es XML DigitalSignature (también llamado XMLDsig, DSig XML, XML-Sig). Como se mencionó anteriormente XML DigitalSignature puede estar incluída al interior del documento XML, puede envolver el documento o puede ser un archivo independiente que hace referencia al documento firmado. Acerca de cuál es la mejor opción de estas, hay diferentes opiniones y no existe unicidad. Por ejemplo, HL7 internacional aún no especifica dentro del estándar el lugar para la inclusión de XML DigitalSignature.

Para realizar la implementación se podría definir la firma al interior del documento CDA, lo cual implica generar una extensión propia dentro del mismo, afectando la conformidad internacional de un documento CDA; los comités técnicos de HL7 internacional, vienen liberando documentos en versión borrador en los que se plantea que la firma se incluya al interior del documento dentro del elemento LegalAutencticator del CDA correspondiente al autor del reporte, sin embargo, esta versión aún no está validada y tiene muchas observaciones y reparos por parte de otro grupo de expertos.

Otra alternativa de implementar la firma electrónica en documentos en salud, es utilizando una referencia al documento firmado, la cual es la planteada por IHE dentro del perfil *Document Digital Signature (DSG) Profile*; allí se recomienda utilizar la firma referenciando al documento objeto de la firma; este tipo de firma ha demostrado ser bastante útil y versátil dado que puede aplicar a archivos de gran volumen y tamaño como es el caso de archivos DICOM. Sin embargo, hay quienes también mencionan la vulnerabilidad de este tipo de firma dado que el certificado emitido es independiente del archivo firmado.

Para la definición de la guía actual, se optó por la utilización de la firma como envolvente del documento original. El documento CDA original debe estar definido acorde con las especificaciones del documento *"Guía de implementación - estructura mínima nacional del documento clínico HL7 V3 CDA-R2"*. Para no modificar el esquema original de CDA, se define un nuevo esquema bajo la raíz <SignedClinicalDocument>, el cual contiene a nivel interior 2 componentes, uno que corresponde al documento CDA y otro correspondiente a la firma electrónica avanzada.

```
<SignedClinicalDocument … >
    <ClinicalDocument ,….>
    </ClinicalDocument … >
    <DigitalSignature ,….>
    </DigitalSignature … >
</SignedClinicalDocument … >
```

7 Recomendaciones

- Uruguay cuenta con avances importantes en las definiciones y uso de Firma Electrónica
- Los documentos externos que son digitalizados y vinculados a un sistema de Historia Clínica pueden ser firmados electrónicamente, se pueden observar las prácticas que para el caso utilizan en el sistema de Expediente Electrónico
- Sin bien HL7 V3 CDA no ha definido en sus guías de implementación, la firma del documento, es posible firmar el documento CDA sin afectar su esquema con una firma avanzada envolvente
- Es necesario avanzar en la promoción y habilitación de las órdenes médicas electrónicas, la firma electrónica sencilla y avanzada pueden reemplazar la rúbrica realizada por el profesional de salud solicitante.
- Hay casos de uso, a nivel de órdenes médicas o de reportes clínicos que no se precisaría de una firma electrónica avanzada
- Continuar con el acompañamiento del área de Identificación Electrónica de Seguridad de la Información de AGESIC, para las definiciones de adopción de firma electrónica

8 Referencias

AGESIC. (Enero de 2013). *Agencia de Gobierno Electrónico y Sociedad de la Información*. Obtenido de http://www.agesic.gub.uy

Bensom, T. (2012). Principles of Health Interoperability HL7 and SNOMED, 2nd Edition. En T. Bensom.

CDA - HL7. (Enero de 2013). *Clinical Document Architecture*. Obtenido de Health Level Seven International: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7

CERT.uy. (2013). *www.cert.uy*.

El Senado y la Cámara de Representantes de la República Oriental del Uruguay, r. e. (15 de Setiembre de 2009). Ley Nº 18.600. *DOCUMENTO ELECTRÓNICO Y FIRMA ELECTRONICA*. Montevideo, Uruguay.

Group, S. D. (2013). *HL7 Implementation Guide for CDA® Release 2: Digital Signatures and Delegation of Rights,.*

Guía para el desarrollo de documentos CDA. (Agosto de 2013). *HL7 Spain.* Obtenido de Subcomité Técnico - V3-CDA HL7 Spain: http://www.hl7spain.org/

HL7. (Enero de 2013). *Health Level Seven International*. Obtenido de http://www.hl7.org/

IHE IT Infrastructure (ITI). (2010). *Document Digital Signature.*

Metadato Definiciones Comunes. (Enero de 2013). *AGESIC - Área de Tecnología - División Arquitectura y Normas.*

Metadato Modelo de Referencia Persona. (Enero de 2013). *Diccionario de Datos.* Obtenido de AGESIC - Área de Tecnología - División Arquitectura y Normas.

Moehrke, J. (2013). *http://healthcaresecprivacy.blogspot.com/*.

MSP. (Enero de 2013). *Ministerio de Salud Pública*. Obtenido de http://www.msp.gub.uy/

Object Identifier. (Enero de 2013). *Object Identifier (OID) Repository*. Obtenido de http://www.oid-info.com/

Uruguay. (Enero de 2013). *República Oriental del Uruguay*. Obtenido de http://www.uruguay.gub.uy/

9 Anexo I : Ejemplo CDA firmado electrónicamente

Estos ejemplos están basados en el documento *"Guía de implementación - estructura mínima nacional del documento clínico HL7 V3 CDA-R2"*

```
<?xml version="1.0"?>
<!-- To use the impl_cdar2.xls stylesheet, remove the comment delimiters from the
style sheet call below. -->
<?xml-stylesheet type="text/xsl" href="cda_qsg.xsl"?>

<!– Envoltorio externo del documento , requerido para que se haga la firma por
fuera del CDA.-->
<SignedClinicalDocument xmlns="urn:hl7-org:v3" xmlns:voc="urn:hl7-org:v3/voc"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:hl7-
org:v3 CDA.xsd">

<ClinicalDocument>
<!--
************************************************************
  CDA Header
************************************************************
-->
   <typeId root="2.16.840.1.113883.1.3" extension="POCD_HD000040">

   <id root="2.16.858.2.[idOrganización].[Familia de items].x" extension="x"/>
   <code codeSystem="2.16.840.1.113883.6.1" code="34133-9" codeSystem
       Name="LOINC" displayName="Epicrisis – Informe al Alta"/>

   <effectiveTime value="20130830110830-0300"/>

   <confidentialityCode code="N" codeSystem="2.16.840.1.113883.5.25"/>

   <recordTarget>

       <patientRole>

             <id root="2.16.858.1.858.68909.12345678"/>
             <!-- Identificador del paciente
             El root 2.16.858.1.858.68909.12345678 asocia el identificador de persona definido por la UNAOID, no es necesario
             incorporar la extensión.
             -->
          <patient>
             <name>
                <given></given>
                <given></given>
                <family></family>
                <family></family>
             </name>
            <administrativeGenderCode code="1" displayName="Masculino"
                    codeSystem="2.16.858.2.10000675.69600" />
            <birthTime value="19541125"/>
          </patient>
       </patientRole>
   </recordTarget>
   <author>

      <time value="20130830113000-300"/>
      <assignedAuthor>
         <id root="2.16.858.2.10000675.69585" extension="3456"/>
             <!-- Identificador del profesional de la salud.
             El root 2.16.858.2.10000675.69585 identifica al registro de Profesionales como catálogo provisto por el SNIS, y en la
```

```
                extensión se encuentra el número de habilitación del profesional en dicho catálogo (3456).
                En caso de no contar con el número de profesional o no corresponder su registro, deberá utilizarse el identificador de
                persona definido por la UNAOID, sin extensión.
                <id root="2.16.858.1.1.858.68909.12345678"/>
                -->
            </assignedAuthor>
        </author>
        <custodian>
            <assignedCustodian>
                <representedCustodianOrganization>
                    <id root="2.16.858.0.2.16.86.1.0.0.21270104001"/>
                        <!-- Identificador de la Organización definido por la UNAOID-->
                    <name>Prestador de Salud X</name>
                </representedCustodianOrganization>
            </assignedCustodian>
        </custodian>
<!--
************************************************************
  CDA Body
************************************************************
-->
        <component>
            <structuredBody>
                <component>
                    <section>
                        <text>
                            <content></content>
                        </text>
                    </section>
                </component>
            </structuredBody>
        </component>
</ClinicalDocument>
<!— Inicio de la Firma Electrónica Avanzada.-->
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:etsi="http://uri.etsi.org/01903/v1.3.2#" Id="Signature1014329">
<ds:SignedInfo Id="Signature-SignedInfo935259">
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference Id="SignedPropertiesID290493" Ty-
pe="http://uri.etsi.org/01903#SignedProperties" URI="#Signature1014329-
SignedProperties499894">
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>BuC+u6TgB76f7fr9wR1i7iCEgoE=</ds:DigestValue>
</ds:Reference>
<ds:Reference URI="#Certificate1902404">
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>jmUyKbG2WiZtzUIeqrKDww4BsBI=</ds:DigestValue>
</ds:Reference>
<ds:Reference Id="Reference-ID-238767" URI="">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>hGSc7nH1JFZAi96J7O6mTqvbE+s=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue Id="SignatureValue661919">
OK/Xp+RsHhoUO00/KzhokLvW5iPJYa+CWnAv02GhUeu7Abk3Y2fbNfZ2SFRFZVYLFhWJG38ykknQ
3zgcLQ20KpSWn68dKgS+Pumk2auYwlMs7yOFqHbmRpscb4sXHJAkOU/5cqVTlCZC7sJ2OzEp7kkr
UyXJFmubpezRRnsDxyw=
</ds:SignatureValue>
<ds:KeyInfo Id="Certificate1902404">
<ds:X509Data>
<ds:X509Certificate>
```

MIIFUzCCAzugAwIBAgIQUUMiNpkFBTpQac6Qvu8MjDANBgkqhkiG9w0BAQUFADB6MQswCQYDVQQG
EwJVWTErMCkGA1UECgwiQURNSU5JU1RSQUNJT04gTkFDSU9OQUwgREUgQ09SUkVPUzEfMB0GA1UE
CwwWU0VSVklDSU9TIEVMRUNUUk9OSUNPUzEdMBsGA1UEAwwUQ29ycmVvIFVydWd1YXlvIC0gQ0Ew
HhcNMTIxMDAxMTcxMDQwWhcNMTMxMDAxMTcxMDQwWjBuMSMwIQYJKoZIhvcNAQkBFhRwcnVlYmFA
Y29ycmVvLmNvbS51eTELMAkGA1UEBhMCVVkxFDASBgNVBAUTC0lERTExMTExMTExMSQwIgYDVQQD
DBtQUlVFQkEgUFJVRUJBIFBSVUVCQSBQUlVFQkEwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
+gLYYraHR0cDov

</ds:X509Certificate>
</ds:X509Data>
<ds:KeyValue>
<ds:RSAKeyValue>
<ds:Modulus>
ll4DdFU754IVO1Y4n5pYo/KhRTMM05CX45BAlc46Bv3O2c5yZAhxnFdRyPNcY1QuSac0VirxTPM/
pp8UvtsuY8mfH0rVKxjXN5taDftFhINCtlUKvkAYxoA1E5nFMX8XWzqjYAsu95oOkFMcuiRdMfNJ
</ds:Modulus>
<ds:Exponent>AQAB</ds:Exponent>
</ds:RSAKeyValue>
</ds:KeyValue>
</ds:KeyInfo>
<ds:Object Id="Signature1014329-Object627225"><etsi:QualifyingProperties Tar-
get="#Signature1014329"><etsi:SignedProperties Id="Signature1014329-
SignedProperties499894"><etsi:SignedSignatureProperties><etsi:SigningTime>2013-10-
23T16:49:22-
02:00</etsi:SigningTime><etsi:SigningCertificate><etsi:Cert><etsi:CertDigest><ds:Di
gestMethod Algo-
rithm="http://www.w3.org/2000/09/xmldsig#sha1"/><ds:DigestValue>N8txY/RKYWMvWUtDcZd
u6NmddUU=</ds:DigestValue></etsi:CertDigest><etsi:IssuerSerial><ds:X509IssuerName>C
N=Correo Uruguayo - CA,OU=SERVICIOS ELECTRONICOS,O=ADMINISTRACION NACIONAL DE CO-
RREOS,C=UY</ds:X509IssuerName><ds:X509SerialNumber>108016045475704594902690388195490598028</ds:X509SerialNumber></etsi:IssuerSerial></etsi:Cert></etsi:SigningCertificate></etsi:SignedSignatureProperties><etsi:SignedDataObjectProperties><etsi:DataObjectFormat ObjectReference="#Reference-ID-
238767"><etsi:Description/><etsi:MimeType>text/xml</etsi:MimeType></etsi:DataObject
For-
mat></etsi:SignedDataObjectProperties></etsi:SignedProperties></etsi:QualifyingProperties></ds:Object></ds:Signature>
<!— Fin de la Firma.-->
</SignedClinicalDocument>

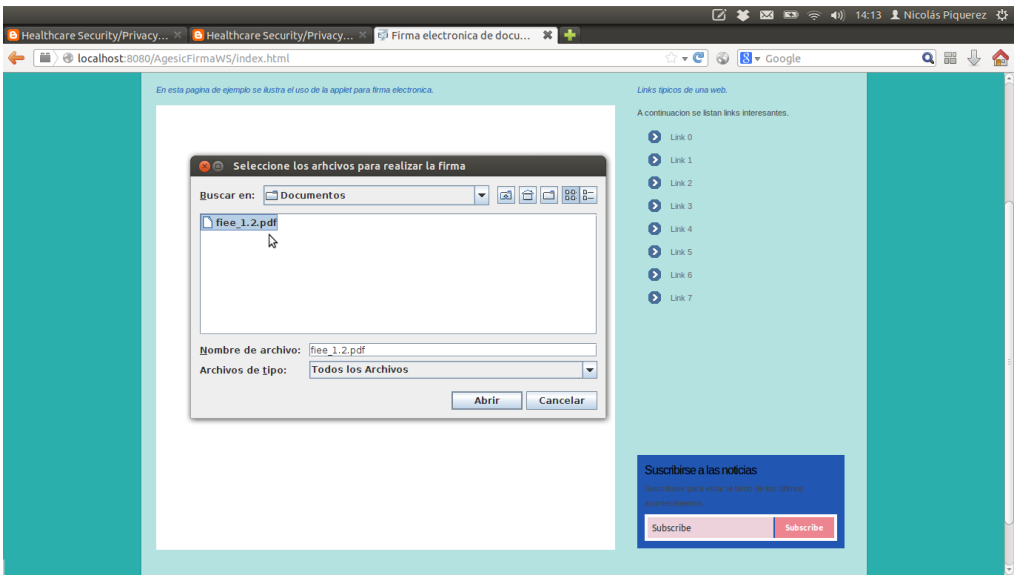
10 Anexo II: Formato XSD de firma

El documento CDA firmado generado debe ser válido contra un esquema que valide como documento XML bien formado; el siguiente esquema, incluye los dos elementos : Un elemento CDA "ClinicalDocument" y un elemento de firma "Signature", los cuales están definidos dentro de la raíz "SignedClinicalDocument" como envolvente y permiten la validación del CDA firmado.

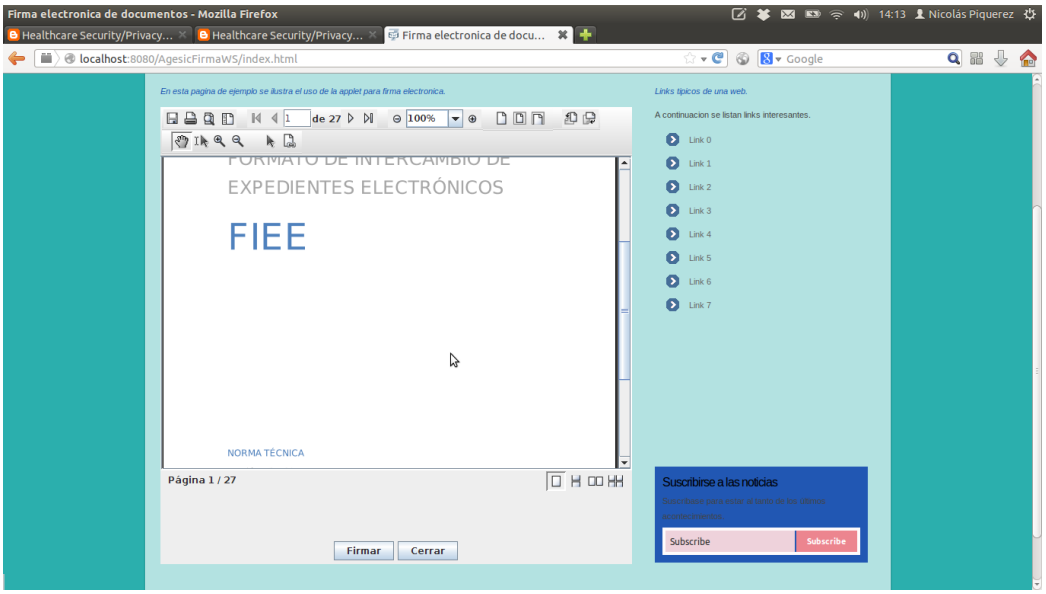
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!-- edited with XMLSPY v2004 rel. 3 U (http://www.xmlspy.com) by Bob Dolin (HL7
CDA TC) -->
<xs:schema targetNamespace="urn:hl7-org:v3"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns="urn:hl7-org:v3"
      xmlns:mif="urn:hl7-org:v3/mif" elementFormDefault="qualified">
      <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-
schema.xsd"/>
      <xs:include schemaLocation="POCD_MT000040.xsd"/>
      <xs:include schemaLocation="XAdES.xsd"/>
      <xs:element name="SignedClinicalDocument">
            <xs:complexType>
                  <xs:sequence>
                        <xs:element name="ClinicalDocument"
type="POCD_MT000040.ClinicalDocument"/>
                        <xs:element ref="ds:Signature"/>
                  </xs:sequence>
            </xs:complexType>
      </xs:element>
</xs:schema>
```

11 Anexo III: Applet Firma Electrónica

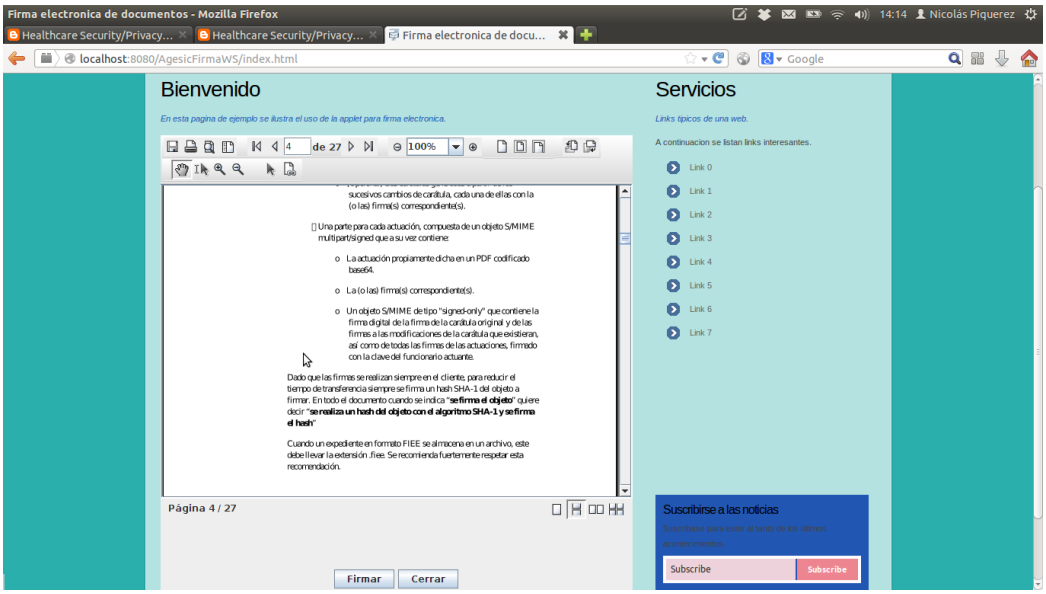
Inicio del Applet de Firma Electrónica

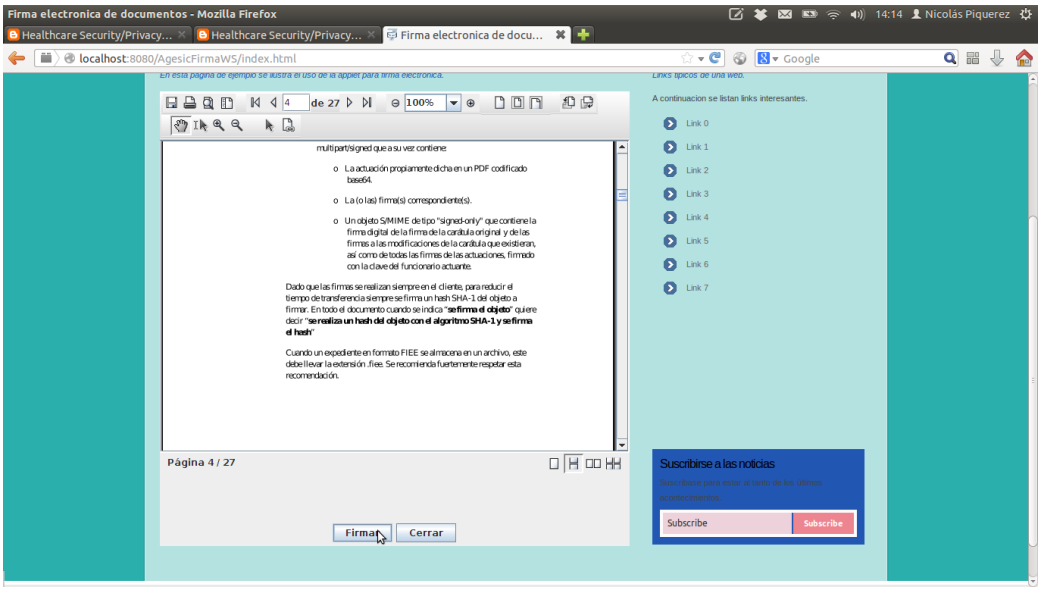


Selección del documento a firmar

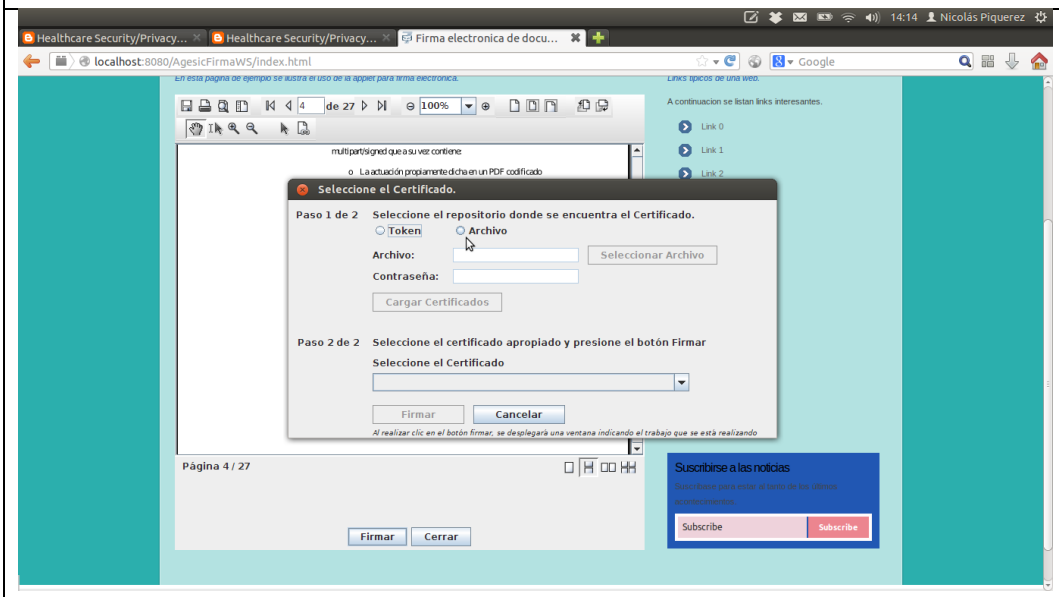


Visualización del documento que se firma

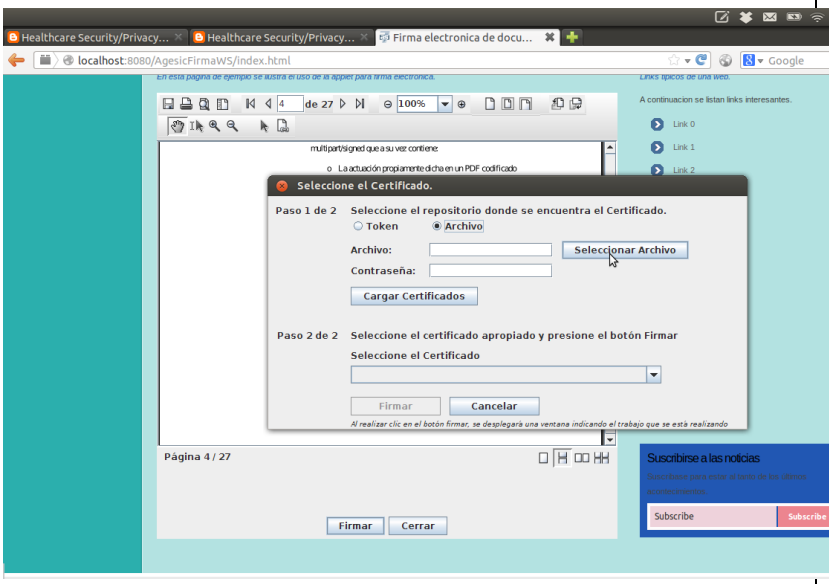




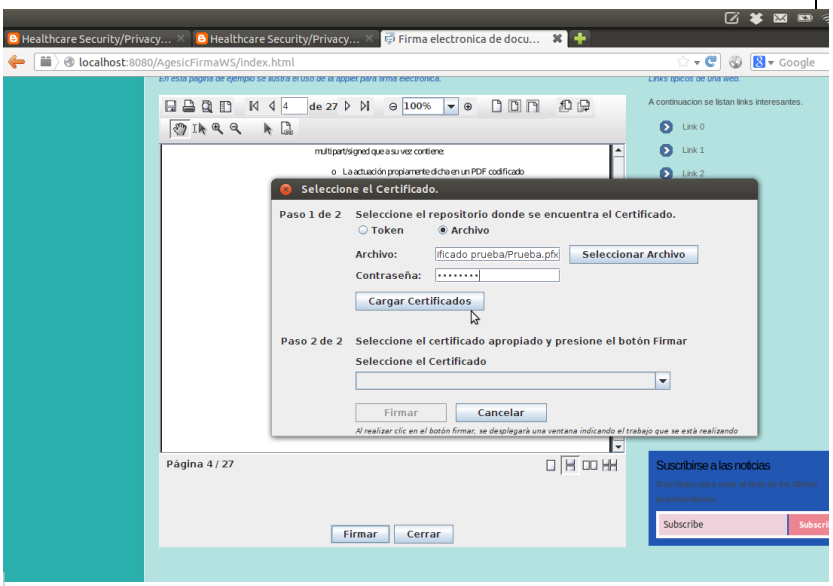
Selección de la opción de Firmar el documento



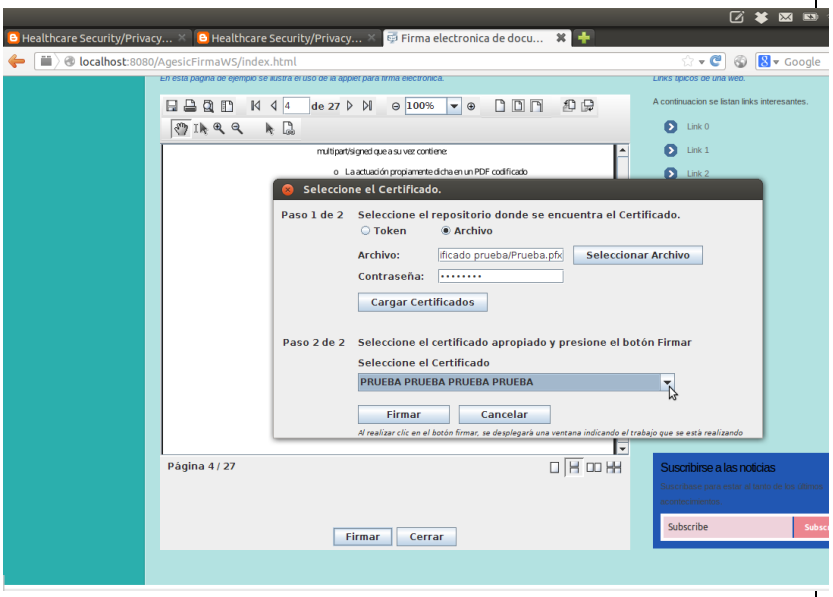
Se selecciona la opción de carga del certificado



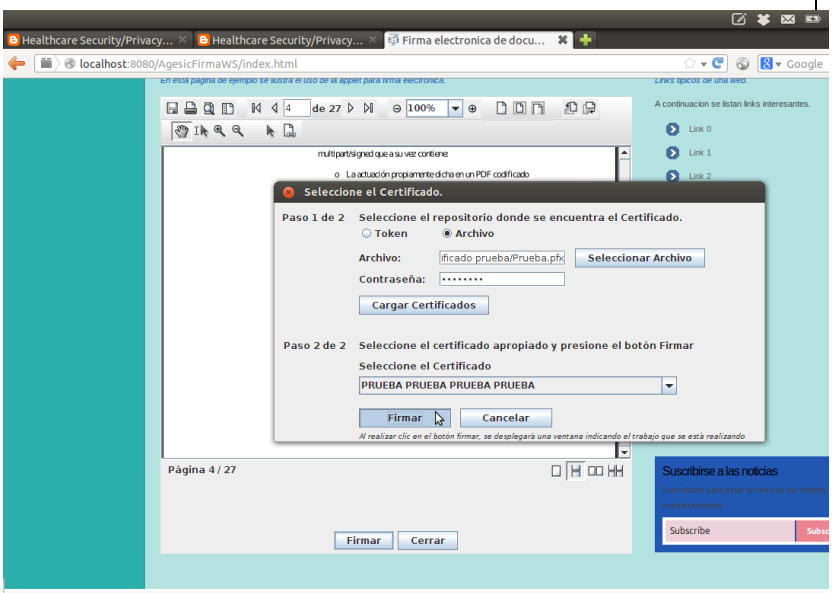
Selección del certificado dentro de la unidad



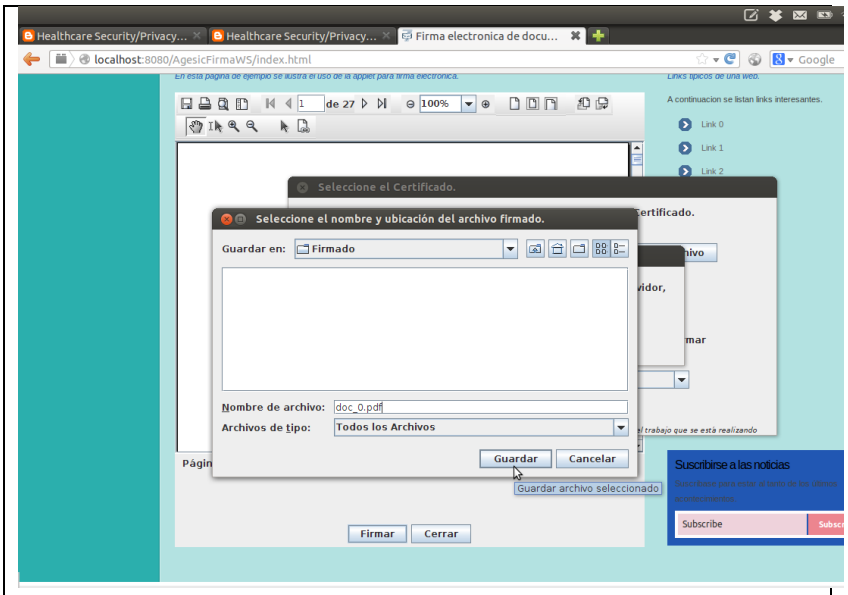
Ingreso de la clave personal



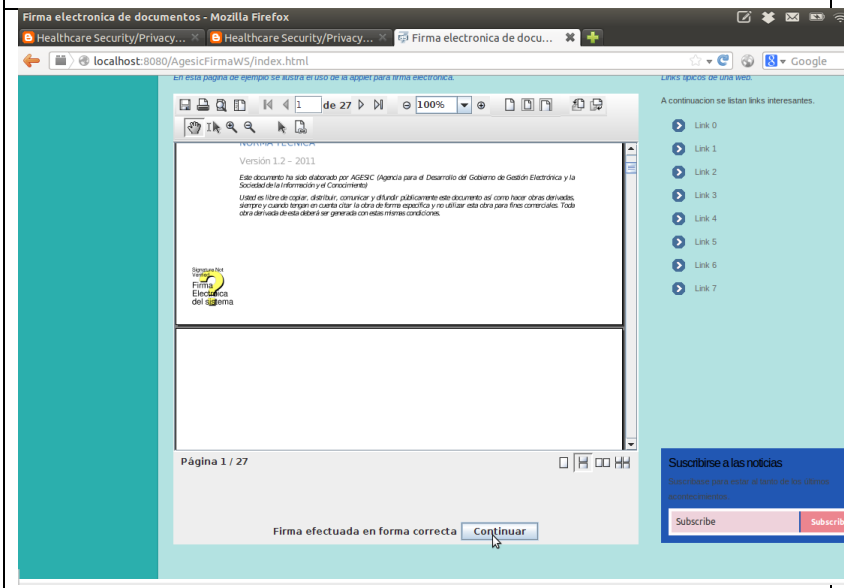
Elección del certificado como archivo



Se firma el documento



Generación del nuevo documento firmado



Visualización del nuevo documento firmado