SISTEMA NACIONAL DE INFORMACIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO (SISESAT)

ANEXO
FIRMA ELECTRÓNICA DOCUMENTOS
XML IDT

Santiago de Chile, agosto de 2016

FIRMAR ELECTRÓNICAMENTE UN XML

Los documentos XML IDT recepcionados por SISESAT deben venir firmados electrónicamente, para el ambiente productivo la firma es obligatoria y para el ambiente de pruebas la firma es opcional.

En términos simples, en el proceso de firma de un documento XML, primero se aplica una función de hash (típicamente SHA1) sobre las secciones a firmar, y a partir de los hash (message digest) se obtiene la firma utilizando la llave privada. Para el caso de los documentos la firma es por el documento completo. En estos ejemplos se usan llaves RSA generadas con OpenSSL.

Para realizar la firma electrónica de los documentos XML IDT, se debe agregar al documento XML un template de la zona de firma (ZONA_O). A continuación, se presenta la estructura del template para la ZONA_O:

```
  <ZONA_O>
    <seguridad id="">
      <descripcion>Aqui va la descripcion</descripcion>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
                    <CanonicalizationMethod  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
          <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <Reference URI="#z_padre">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue></DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue />
        <KeyInfo>
          <X509Data >
            <X509SubjectName/>
            <X509IssuerSerial/>
            <X509Certificate/>
          </X509Data>
          <KeyValue />
        </KeyInfo>
      </Signature>
    </seguridad>
  </ZONA_O>
```

A continuación se presenta el documento idt1 con la ZONA_O agregada:

```
<?xml version="1.0" encoding="UTF-8"?>
<idt1                                          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#"      xmlns:ns1="http://www.w3.org/2001/04/xmlenc#"
xsi:schemaLocation="http://www.w3.org/2000/09/xmldsig#                    xmldsig-core-schema.xsd
```

```
http://www.w3.org/2001/04/xmlenc#                                    xenc-schema.xsd"
xsi:noNamespaceSchemaLocation="SISESAT_RALF_1.1.0.xsd" id="z_padre">
   <ZONA_A_IDT>...
   </ZONA_A_IDT>
   <ZONA_U>...
   </ZONA_U>
   <ZONA_O>
      <seguridad id="">
         <descripcion>Aqui va la descripcion</descripcion>
         <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
                        <CanonicalizationMethod  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
               <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
               <Reference URI="#z_padre">
                  <Transforms>
                     <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                  </Transforms>
                  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <DigestValue></DigestValue>
               </Reference>
            </SignedInfo>
            <SignatureValue />
            <KeyInfo>
               <X509Data >
                  <X509SubjectName/>
                  <X509IssuerSerial/>
                  <X509Certificate/>
               </X509Data>
               <KeyValue />
            </KeyInfo>
         </Signature>
      </seguridad>
   </ZONA_O>
</idt1>
```

Dado que se quiere firmar completamente el documento desde tu tag principal “idt1”, se debe agregar un atributo id a este tag

```
<idt1 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#"
xmlns:ns1="http://www.w3.org/2001/04/xmlenc#"
xsi:schemaLocation="http://www.w3.org/2000/09/xmldsig#  xmldsig-core-
schema.xsd  http://www.w3.org/2001/04/xmlenc#  xenc-schema.xsd"
xsi:noNamespaceSchemaLocation="SISESAT_RALF_1.1.0.xsd" id="z_padre">
```

Para firmar utilizaremos xmlsec1. Es necesario tener los certificados para realizar la firma electrónica. Al firmar, hay que agregar el parámetro --id-attr indicando el nodo que tiene el atributo id, en nuestro caso el nodo es idt1

```
xmlsec1 --sign --pkcs12 doc_firma.p12 --pwd pass --trusted-pem
algun_pem.pem --id-attr:id idt1 --output idt1_firmado.xml idt1.xml
```