



Guía Técnica

Firma Transacción

Noviembre 2019, v0.1
Equipo de Arquitectura

Contenido

CONTENIDO.....	2
1. INTRODUCCIÓN.....	3
1.1. Objetivo del Documento	3
1.2. Recomendaciones	3
1.3. Actualización	3
2. SERVICIO.....	3
2.1. Condiciones	3
2.2. Definición	3
2.3. Request.....	4
2.4. Response	5
2.5. Vista Lógica.....	7

1.Introducción

1.1. Objetivo del Documento

El objetivo del presente documento es explicar la implementación de firma para las transacciones que van a la Plataforma de Salud.

1.2. Recomendaciones

Para la implementación de firma, se debe tener un certificado de persona jurídica de la institución.

1.3. Actualización

Este documento se actualizará cada vez que se analice/diseñe un requerimiento el cual implique cambios en la definición del servicio.

2.Servicio

2.1. Condiciones

Se deberá exponer un servicio en una IP de RedSalud (10.253.Subred.19/26) con certificado SSL (HTTPS) en el puerto 443.

La CN del certificado se debe llamar igual al nombre del host donde se va a exponer el WSDL.

2.2. Definición

El WSDL que se debe exponer, recibirá 4 datos por parámetros del tipo *String*:

1. userName
2. role
3. policyName
4. issuer

Datos de ejemplo para ambiente de TEST:

- userName: PRUEBAS
- role: OU=TEST_TUTORIAL,O=TEST_PE
- policyName: urn:tokensimple
- issuer: [Nombre_Prestador]

2.3. Request

awsgetsamlrequest services

```

<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:tns="ConectorHCEN"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:ns1="http://schemas.xmlsoap.org/soap/http"
name="awsgetsamlrequest_servicesService" targetNamespace="ConectorHCEN">
  <wsdl:types>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:tns="ConectorHCEN"
elementFormDefault="unqualified" targetNamespace="ConectorHCEN" version="1.0">

  <xs:element name="Execute" type="tns:Execute"/>

  <xs:element name="ExecuteResponse" type="tns:ExecuteResponse"/>

  <xs:complexType name="Execute">
    <xs:sequence>
      <xs:element form="qualified" minOccurs="0" name="userName" type="xs:string"/>
      <xs:element form="qualified" minOccurs="0" name="role" type="xs:string"/>
      <xs:element form="qualified" minOccurs="0" name="policyName" type="xs:string"/>
      <xs:element form="qualified" minOccurs="0" name="issuer" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="ExecuteResponse">
    <xs:sequence>
      <xs:element form="qualified" minOccurs="0" name="samlRequest" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>

</xs:schema>
</wsdl:types>
<wsdl:message name="ExecuteResponse">
  <wsdl:part element="tns:ExecuteResponse" name="parameters"/>
</wsdl:part>
</wsdl:message>
<wsdl:message name="Execute">
  <wsdl:part element="tns:Execute" name="parameters"/>
</wsdl:part>
</wsdl:message>
<wsdl:portType name="awsgetsamlrequest">
  <wsdl:operation name="Execute">
    <wsdl:input message="tns:Execute" name="Execute">
</wsdl:input>
    <wsdl:output message="tns:ExecuteResponse" name="ExecuteResponse">
</wsdl:output>
  </wsdl:operation>
</wsdl:portType>
<wsdl:binding name="awsgetsamlrequest_servicesServiceSoapBinding"
type="tns:awsgetsamlrequest">

```

```

<soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
<wsdl:operation name="Execute">
  <soap:operation soapAction="" style="document"/>
  <wsdl:input name="Execute">
    <soap:body use="literal"/>
  </wsdl:input>
  <wsdl:output name="ExecuteResponse">
    <soap:body use="literal"/>
  </wsdl:output>
</wsdl:operation>
</wsdl:binding>
<wsdl:service name="awsgetsamlrequest_servicesService">
  <wsdl:port binding="tns:awsgetsamlrequest_servicesServiceSoapBinding"
name="awsgetsamlrequestPort">
    <soap:address location="http://pr-xds01:8088/ConectorHCEN/awsgetsamlrequest_services"/>
  </wsdl:port>
</wsdl:service>
</wsdl:definitions>

```

WS Request

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:con="ConectorHCEN">
<soapenv:Header/>
<soapenv:Body>
<con:Execute>
<con:userName>PRUEBAS</con:userName>
<con:role>OU=TEST_TUTORIAL,O=TEST_PE</con:role>
<con:policyName>urn:tokensimple</con:policyName>
<con:issuer>NOMBRE_PRESTADOR</con:issuer>
</con:Execute>
</soapenv:Body>
</soapenv:Envelope>

```

2.4. Response

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ExecuteResponse xmlns="ConectorHCEN">
      <samlRequest>
        <?xml version="1.0" encoding="UTF-8"?>
          <saml1:Assertion AssertionID="_ed7fb151d60639012d3ffa298af6c258"
IssueInstant="2018-02-08T13:18:13.869Z" Issuer="ANDA" MajorVersion="1" MinorVersion="0"
xmlns:saml1="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
            <saml1:Conditions NotBefore="2018-02-08T13:03:13.869Z"
NotOnOrAfter="2018-02-08T13:33:13.869Z"/>
            <saml1:AuthenticationStatement AuthenticationInstant="2018-02-
08T13:18:13.869Z" AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
              <saml1:Subject>
                <saml1:NameIdentifier
Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">OU=TEST_TUTORIAL,O=TEST_PE</saml1:NameIdentifier>

```

```

        <saml1:SubjectConfirmation>
    <saml1:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</saml1:ConfirmationMeth
od>
        </saml1:SubjectConfirmation>
    </saml1:Subject>
</saml1:AuthenticationStatement>
<saml1:AttributeStatement>
    <saml1:Subject>
        <saml1:NameIdentifier
Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">OU=TEST_TUTORIAL,O=TEST_PE</saml1:NameIdentifier>
    </saml1:SubjectConfirmation>

    <saml1:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</saml1:ConfirmationMeth
od>
        </saml1:SubjectConfirmation>
    </saml1:Subject>
    <saml1:Attribute AttributeName="User"
AttributeNamespace="urn:tokensimple">
        <saml1:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">PRUEBAS</saml1:AttributeValue>
    </saml1:Attribute>
</saml1:AttributeStatement>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
    </ds:CanonicalizationMethod>
        <ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    </ds:SignatureMethod>
        <ds:Reference
URI="#_ed7fb151d60639012d3ffa298af6c258">
    </ds:Reference>
        <ds:Transforms>
            <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
    </ds:Transform>
            <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
    </ds:Transform>
        </ds:Transforms>
        <ec:InclusiveNamespaces
PrefixList="xs" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#">
    </ec:InclusiveNamespaces>
        </ds:Transform>
    </ds:Transforms>
        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    </ds:DigestMethod>
        <ds:DigestValue>Q9YI2bBH6QtK9vFgTPKUXTchkbA=</ds:DigestValue>
    </ds:DigestValue>
    </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>MuWikMjMn0DAGD63EeyCUgztvm0ArXoTSpwAkuilnLI2wwswQEifW3dw2
3Q3CF3h6xVQS3Kp+RZ8N/U+NvYT3I8nSENZG5UUPEuURqviKZil0hzWQWsiW9T1lvCMGzQwYGeXa
Qi4Q0jDulHubF5gnsH++1Q+knuHk56QPosgX7udy3/t98CerA2vVaOg0rsq8uavZo/i1g0yIV8MRBcEvvSB

```

```
Rw2lt1dgMX5DyVJgnPRx9WcBA0IVfSiXTeKSNf565YjGkvg5yGOaSpErLz/PkudPetYk0EJIY6xnj0BAZ2
AnETH4sMnxoG200qVpzPYc5I2zBMC0Y4iOb18VF7SbkQ==</ds:SignatureValue>
<ds:KeyInfo>
  <ds:X509Data>
    <ds:X509Certificate>MIIGNTCCBB2gAwIBAgIUAUkSa5QuP+fyI0ZdWblxela1544wDQYJKoZIhvc
    NAQELBQAwWjEdMBsG
    A1UEAxMUQ29ycmVvIFVydWd1YXlvc0gQ0ExLDAqBgNVBAoMI0FkbWluaXN0cmFjacOzbiBOYWNP
    b25hbCBkZSBDb3JyZW9zMQswCQYDVQQGEWJVWTAeFw0xNzA0MjQxOTMwMjBaFw0xOTA0MjQx
    OTMw
    MjBaMGExGDAWBgNVBAUTD1JVZzlxMzEwODc0MDAxODELMAkGA1UEBhMCVvKxKTAnBgNVBAo
    TIEFT
    T0NJQUJNT04gTkFDSU9OQUwgREUgQUZJTEIBRE9TMQ0wCwYDVQQDEwRBTKRBMiIBlANBgkqh
    kiG
    9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0ocFDzi4w61gp+lTh80+KHEc9/pp/cIHG22hj9qO5WX+PO6g
    icTx37LA2CpnkR6eREsD8vpb+e3TmCNSScmdx4npuAlla19sYf7oI0ltNXne5N8GaTYB8/WkFSE7
    trhrtjtkkutjrmop54u6093u54oith3i9gy43oti43hti034ut9t0434t390tu3oitho3ihhh
    ZDK1IRZd897MNWx3I1YN8M0avqsZ6DQ+wBcy0MLvjo2Nw4IQN9SjcEuEY/MeHwS5sA8XcTMgEC4S
    7JSrf/MF/YIj13Djc03TWCt8/1IYRhxUb4rWaTXm8VjGjjqyNCVs6oophTPELK+OSQIDAQABo4IB
    6jCCAeYweQYIKwYBBQUHAQEETBrMDYGCCsGAQUFBzAChipodHRwOi8vYW5jY2EuY29ycmVvL
    mNv
    gfdgfdgfdyeyhffsañalnalkhiuy94y3hi43ooi9896903nngerourei09reu09u050u09uu
    LnV5L2FuY2NhL09DU1AwDgYDVR0PAQH/BAQDAgTWMAwGA1UdEwEB/wQCMAAwOwYDVR0fBDQ
    wMjAw
    oC6gLIYqaHR0cDovL2FuY2NhLmNvcnJlby5jb20udXkvYW5jY2EvYW5jY2EuY3JsMIG4BgNVHSAE
    gbAwga0wZAYLYIZahOKuHYSIBQQwVTBTBgggBgEFBQcCARZHaHR0cDovL3VjZS5ndWludXkvaW5
    m
    b3JtYWNPb24tdGVjbmljYS9wb2xpdGJjYXNvY3BfcGVyc29uYV9qdXJpZGljYS5wZGYwRQYLYIZa
    gdfg54645654ghfggdf43534gerrgerer6547jtykuo8ojk665hth4t43t45y45746hrjtjyjj
    Y3BzLnBkZjATBgNVHSUEDDAKBgggBgEFBQcDAjAdBgNVHQ4EFgQUPwLBFJRgqDARiDEkfDW56V
    hb
    /qQwHwYDVR0jBBgwFoAUbOKwJo1b1iYIH5hdaeAOf1XsrnYwDQYJKoZIhvcNAQELBQADggIBAGMv
    d6KWtxbs8W+8+AvqcnukFb8+eJA8vWBJddUNGBJNeW6ONebjHyx/Kxb4LAIvP3B6x+LayM8wT+V
    /1eGomQUGqMNc0d8S3U94yaWOAfS+QKWqCWkYigkt9wRDD4cmtTAUAX4AVayEkfQFLFnAL/yL27V
    cdmHAhQlKpbj/re6gerye7547hthdddyyrkbds+gKHSmFnDKaB4WZoWq8Q8GycEAK3n+58EOGm63
    bukU9pAh5+dhP3sA/HYulNrqJX5e7TapNQiT+lJBOsLzqrj3mnZcjbXdOuw6FQrleON8UXeMClr
    rUISs8jboUdVKHTgell2WigjibC161KcYGSrFmMfPXET0T99e+edonDwdF0fOUMnt1f0MqMAQSA3
    ZZXcOKatbQBY42AYThS29750t7Ytitlms9h0FsdDovnQkwd4UKH0oONpGEILwGkwXx9R/aRY8Fvc
    KejZYH2fl48MUaCLnH2Z2WMAeeWaF4fN6vKwTqxdStIR/afwQheDGyEwKYCpiuveQrcCWUEL0cXP
    TpGz5v2WNNvcB/MZKmd1LQ8HC9BSZ8C5z/qUUUu+kyHWRf3RcQtFdX5cnmusXJxZrqp4Co5NFRdw
    vAINCNU2hK4gdx7WsdAQMA344ewdnV7uFi7Oi/os/HWXIAAx4O3hVF7FYSLSjs9tO/HpV6D/</ds:X509
    Certificate>
  </ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
</saml1:Assertion>
</samlRequest>
</ExecuteResponse>
</soap:Body>
</soap:Envelope>
```

2.5. Vista Lógica

En esta vista muestra las diferentes interacciones entre los componentes del sistema para la implementación de los casos de uso.

Diagrama de secuencia

Servicios Plataforma HCEN

