eID Identity Provider

Guía para desarrolladores de Software

Rolosa HyJ S.A. - MICITT

11 de Agosto de 2014

Resumen

El presente documento es una guía para desarrolladores de software útil como punto de entrada para integrar el eID IDP en una aplicación web.

Tabla de contenido

Introducción

El eID Identity Provider (eID IdP) es un proveedor de identidad que utiliza el eID Applet para autenticar usuarios.

El principal objetivo del eID Identidy Provider es facilitar la integración del eID en aplicaciones Web de un Proveedor de Servicios. Este utiliza el eID trust service para la validación de certificados digitales.

El eID Identity Provider soporta los siguientes protocolos para autenticación:

- SAML v2.0
- OpenID v2.0
- WS-Federation v1.1

Pre-requisitos

Para proseguir con el presente documento, es necesario disponer de:

- Una Tarjeta Inteligente para Firma Digital de Costa Rica
- Un lector de tarjetas apropiado
- Certificados Digitales de la cadena de la confianza de la Firma Digital de Costa Rica
- Drivers necesarios para la Tarjeta Inteligente, dependiendo el sistema operativo en el que se desee realizar los trabajos.

Los drivers y certificados digitales tienen que ser obtenidos desde el sitio de Soporte de Firma Digital de Costa Rica:

https://www.soportefirmadigital.com/sfd/default.aspx

SAML v2.0

POST del Navegador

Solicitud de Autenticación

La aplicación web del Proveedor de Servicio (SP) envía una solicitud de autenticación SAML v2.0 codificada en Base64 utilizando HTTP Post a través del navegador del cliente. El parámetro POST utilizado para eso es SAMLRequest.

El siguiente es un ejemplo de dicha solicitud de autenticación SAML v2.0:

```
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
      AssertionConsumerServiceURL="https://192.168.1.101:443/eid-idp-sp/saml2-
landing"
    Destination="https://192.168.1.101:443/eid-idp/protocol/saml2"
    ForceAuthn="true"
    ID="authn-request-21b80327-7204-44ef-9e42-73633ae2e175"
    IssueInstant="1970-01-01T00:00:00.000Z"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Version="2.0">

    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        https://192.168.1.101:443/eid-idp-sp/saml2-landing
    </saml2:Issuer>

</saml2p:AuthnRequest>
```

Respuesta de Autenticación

El Identity Provider retornará una respuesta de autenticación SAML v2.0 codificada en Base64 utilizando un POST del navegador del cliente. El parámetro POST utilizado para esto es SAMLResponse.

El siguiente es un ejemplo de dicha respuesta de autenticación SAML v2.0:

```
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
    Destination="https://192.168.1.101:443/eid-idp-sp/saml2-landing"
    ID="saml-response-eccaf61a-f8f1-4346-9c25-a83c1e8fa599"
    IssueInstant="2010-08-03T08:56:53.366Z"
    Version="2.0">

    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ...
    </ds:Signature>

    <saml2p:Status>
       <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </saml2p:Status>
    <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        ID="assertion-765aec37-0788-4c3b-a6ca-88eb78a9890c"
        IssueInstant="2010-08-03T08:56:53.366Z"
        Version="2.0">

        <saml2:Issuer>http://www.e-contract.be/</saml2:Issuer>

        <saml2:Subject>
            <saml2:NameID>71715100070</saml2:NameID>

  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml2:SubjectConfirmationData
              InResponseTo="authn-request-21b80327-7204-44ef-9e42-73633ae2e175"
                NotBefore="2010-08-03T08:56:53.366Z"
                NotOnOrAfter="2010-08-03T09:01:53.366Z"
              Recipient="https://192.168.1.101:443/eid-idp-sp/saml2-landing" />
            </saml2:SubjectConfirmation>
        </saml2:Subject>

        <saml2:Conditions
            NotBefore="2010-08-03T08:56:53.366Z"
            NotOnOrAfter="2010-08-03T09:01:53.366Z">
            <saml2:AudienceRestriction>
                <saml2:Audience>
                    https://192.168.1.101:443/eid-idp-sp/saml2-landing
                </saml2:Audience>
            </saml2:AudienceRestriction>
        </saml2:Conditions>

        <saml2:AuthnStatement AuthnInstant="2010-08-03T08:56:53.366Z">
            <saml2:AuthnContext />
        </saml2:AuthnStatement>

        <saml2:AttributeStatement>
            <saml2:Attribute Name="urn:be:fedict:eid:idp:name">
                <saml2:AttributeValue>
                    SPECIMEN
                </saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="urn:be:fedict:eid:idp:firstName">
                <saml2:AttributeValue>
                    Alice Geldigekaart2266
                </saml2:AttributeValue>
            </saml2:Attribute>
        </saml2:AttributeStatement>

    </saml2:Assertion>
</saml2p:Response>
```

Artifact Binding

Se tiene disponible soporte para enlaces de artefactos pero sólo aplicable a las respuestas de autenticación. Enviar solicitudes de autenticación SAML v2.0 es posible de manera similar al protocolo HTTP-POST o HTTP-Redirect pero al punto de entrada del protocolo de enlace de artefactos.

Respuesta de Autenticación

En el enlace de artefactos HTTP, la respuesta de la autenticación SAML es transmitida por referencia utilizando un artefacto. Un enlace síncrono separado es utilizado para intercambiar la respuesta de la autenticación actual utilizando un web service de resolución de artefactos.

El siguiente es un ejemplo de las respuestas de artefactos SAML v2.0.

```
HTTP/1.1 302 Object Moved
Date: 21 Jan 2004 07:00:49 GMT
Location: https://www.rp.com/SAML?SAMLart=AAQAADWNEw5VT47wcO4z
X%2FiEzMmFQvGknDfws2ZtqSGdkNSbsW1cmVR0bzU%
3D&RelayState=0043bfc1bc45110dae17004005b13a2b
Content-Type: text/html; charset=iso-8859-1
```

El Proveedor de Servicios responderá con una Solicitud de Resolución de Artefactos a ser enviada al Web Service de resolución de artefactos SAML v2.0 mediante SOAP. El siguiente es un ejemplo de tal solicitud:

```
POST /SAML/Artifact/Resolve HTTP/1.1
Host: eid-idp.be
Content-Type: text/xml
Content-Length: nnn
SOAPAction: http://www.oasis-open.org/committees/security
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Body>
        <samlp:ArtifactResolve
            xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
            xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
            ID="_6c3a4f8b9c2d" Version="2.0"
            IssueInstant="2004-01-21T19:00:49Z">
            <Issuer>https://www.rp.com/SAML</Issuer>
            <Artifact>
                AAQAADWNEw5VT47wcO4zX/iEzMmFQvGknDfws2ZtqSGdkNSbsW1cmVR0bzU=
            </Artifact>
        </samlp:ArtifactResolve>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

El siguiente es un ejemplo de la respuesta del servicio de resolución:

```
HTTP/1.1 200 OK
Date: 21 Jan 2004 07:00:49 GMT
Content-Type: text/xml
Content-Length: nnnn
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Body>
        <samlp:ArtifactResponse
            xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
            xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
            ID="_FQvGknDfws2Z" Version="2.0"
            InResponseTo="_6c3a4f8b9c2d"
            IssueInstant="2004-01-21T19:00:49Z">
            <Issuer>https://eid-idp.be/SAML</Issuer>
            <samlp:Status>
                <samlp:StatusCode
                    Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
            </samlp:Status>
            <saml2p:Response ...>
                ...
            </samlp:Response>
        </samlp:ArtifactResponse>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Browser Redirect

Se dispone de soporte para el enlace de re direccionamiento HTTP de solicitudes de autenticación entrantes esto se ha agregado para el soporte de librerías cómo SimpleSAMLphp o mod_mellon.

La respuesta de autenticación SAML v2.0 será enviada utilizando el protocolo POST o el de enlace de Artefactos ,de acuerdo a lo que se está utilizando en el punto de entrada del protocolo del IdP.

Metadata

Para cada punto de entrada del protocolo SAML v2.0 del IdP , se provee un documento de metadatos para publicar servicios SAML v2.0.Esto ha sido agregado para librerías SimpleSAMLphp o mod_mellon.

El siguiente es un ejemplo el documento de metadatos SAML v2.0:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    entityID="https://eid-idp.be/eid-idp/protocol/saml2/post/auth">

    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ...
    </ds:Signature>

    <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

        <md:KeyDescriptor>
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>
                        ...
                    </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>

        <md:NameIDFormat>
            urn:oasis:names:tc:SAML:2.0:nameid-format:transient
        </md:NameIDFormat>

        <md:SingleSignOnService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://eid-idp.be/eid-idp/protocol/saml2/post/auth"/>

    </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

OpenID v2.0

Se ha agregado soporte para OpenID para integración transparente en plataformas como Drupal. Un documento dinámico de identidad YADIS, se utiliza para iniciar una autenticación OpenID. El proveedor de identidad IdP utiliza selección OP.

El proveedor de identidad soporta intercambio de atributos OpenID (OpenID AX) como parte de la solicitud de autenticación . Por defecto se retornan el nombre completo y el primer nombre son retornados. El proveedor de servicios puede solicitar otros atributos explícitamente.

El proveedor de identidad soporta la extensión 1.0 de la política de autenticación OpenID (OpenID PAPE) para comunicarse entre el proveedor de identidad y el proveedor de servicios intercambiar la política de autenticación.

OpenID Protocol

EL URL OpenID retorna el siguiente archivo:

```
<HTML>
    <HEAD>
        <META http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
          <META content="https://localhost:48745/identity/xrds" http-equiv="X-
XRDS-Location"/>
    </HEAD>

    <BODY>
        <P>OpenID Identity URL</P>
    </BODY>
</HTML>
```

A continuación, el consumidor OpenID descargará el documento YADIS, que contiene:

```
<xrds:XRDS xmlns:xrds="xri://$xrds" xmlns="xri://$xrd*($v*2.0)">
    <XRD>
        <Service>
            <Type>http://specs.openid.net/auth/2.0/server</Type>
            <URI>https://localhost:48745/producer</URI>
        </Service>
        <Service>
            <Type>http://specs.openid.net/auth/2.0/signon</Type>
            <URI>https://localhost:48745/producer</URI>
        </Service>
    </XRD>
</xrds:XRDS>
```

El primer elemento Service específica donde contactar al proveedor de identidad para establecer una clave de asociación toda la comunicación se realiza sobre SSL de manera unilateral.

La solicitud de asociación se envía utilizando HTTP POST por el consumidor OpenID hacia el IdP:

```
openid.ns:http://specs.openid.net/auth/2.0
openid.mode:associate
openid.session_type:DH-SHA256
openid.assoc_type:HMAC-SHA256
openid.dh_consumer_public:...
```

El eID IdP reacciona a esta solicitud de asociación con el siguiente mensaje:

```
openid.ns:http://specs.openid.net/auth/2.0
openid.session_type:DH-SHA256
openid.assoc_type:HMAC-SHA256
openid.assoc_handle:1273064471124-0
openid.expires_in:1799
openid.dh_server_public:...
openid.enc_mac_key:...
```

Luego de que la asociación es establecida entre el consumidor OpenID y el proveedor de identidad, el consumidor está listo para enviar la solicitud de autenticación utilizando una redirección del navegador con los siguientes argumentos:

```
openid.ns.ext1:http://openid.net/srv/ax/1.0
openid.ext1.type.name:http://schema.openid.net/namePerson/first
openid.ns:http://specs.openid.net/auth/2.0
openid.identity:http://specs.openid.net/auth/2.0/identifier_select
openid.claimed_id:http://specs.openid.net/auth/2.0/identifier_select
openid.mode:checkid_setup
openid.ext1.mode:fetch_request
openid.ext1.required:name
openid.realm:https://localhost:48745/consumer
openid.assoc_handle:1273064471124-0
openid.return_to:https://localhost:48745/consumer
```

El consumidor hace que el proveedor de identidad seleccione los identificadores los cuales se especifican utilizando los parámetros openid.identity y openid.claimed_id . El ejemplo también muestra cómo se solicita un atributo como parte de la solicitud de autenticación.

Después de manejar la solicitud de autenticación el proveedor de identidad direccionar a al usuario a través del navegador hacia el Applet para que el usuario pueda autenticarse después de esto una redirección de respuesta será enviada de vuelta al consumidor conteniendo los siguientes argumentos:

```
openid.op_endpoint:https://localhost:48745/producer
openid.signed:op_endpoint,claimed_id,identity,return_to,response_nonce,
    assoc_handle,ns.ext1,ns.ext2,ext1.mode,ext1.type.name,ext1.value.name,
    ext2.auth_policies
openid.ns.ext1:http://openid.net/srv/ax/1.0
openid.ext1.type.name:http://schema.openid.net/namePerson/first
openid.sig:eCG4ER1zAzuGOdDd+MuxOI1bjQImsfaPO+e/S5gACOk=
openid.ns.ext2:http://specs.openid.net/extensions/pape/1.0
openid.response_nonce:2010-05-05T13:01:11Z0
openid.claimed_id:https://localhost:48745/identity/idp/123456789
openid.assoc_handle:1273064471124-0
openid.ns:http://specs.openid.net/auth/2.0
openid.ext1.value.name:sample-first-name
openid.ext2.auth_policies:http://schemas.openid.net/pape/policies/2007/06/
multi-factor-physical
openid.identity:https://localhost:48745/identity/idp/123456789
openid.ext1.mode:fetch_response
openid.mode:id_res
openid.return_to:https://localhost:48745/consumer
```

Obsérvese que el atributo y la extensión están firmados por el proveedor de identidad con la clave que ha sido intercambiada durante la etapa de asociación.

Finalmente el consumidor OpenID contactara al proveedor de identidad una vez más para validar si el identificador seleccionado es permitido por el proveedor de identidad esto es realizado a través del segundo elemento Service en el documento YADIS.

WS-Federation v1.1

Se dispone de soporte para el modelo de solicitantes pasivos Web de WS-Federation. Este soporte provee integración transparente con aplicaciones ASP.net utilizando Windows Identity Foundation.

Metadata

EL IdP discovery para WS-Federation utiliza un documento de metadatos, como se describe en OASIS SAML v2.0 Metadata. El siguiente es un ejemplo de dicho documento:

Son muy importantes las ubicaciones del endpoint del solicitante pasivo WS-Federation y el listado de todos los tipos disponibles por el proveedor de identidad. También contiene la identidad digital del IdP y una indicación de la clave utilizada para firmar tokens de autenticación de respuesta.

```
<md:EntityDescriptor
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"
    xmlns:wsa="http://www.w3.org/2005/08/addressing"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"

    ID="saml-metadata-d1ea2940-3032-4e7a-8093-c131ca7bab00"
    entityID="https://127.0.0.1:54705/eid-idp/protocol/ws-federation">

    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ...
    </ds:Signature>
```

```
    <md:RoleDescriptor
                protocolSupportEnumeration="http://docs.oasis-open.org/wsfed/
federation/200706"
        xsi:type="fed:SecurityTokenServiceType">

        <md:KeyDescriptor use="signing">
            <ds:KeyInfo>
                <ds:X509Data>
                    ...
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>

        <fed:ClaimTypesOffered>
            <auth:ClaimType
                Optional="true"
              Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">

                <auth:DisplayName>Name</auth:DisplayName>
                <auth:Description>The name of the Subject.</auth:Description>
            </auth:ClaimType>

            <auth:ClaimType
                Optional="true"
                    Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
givenname">

                <auth:DisplayName>FirstName</auth:DisplayName>
                 <auth:Description>Preferred name or first name of a Subject.</
auth:Description>
            </auth:ClaimType>

            <auth:ClaimType
                Optional="true"
                    Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
surname">

                <auth:DisplayName>LastName</auth:DisplayName>
                     <auth:Description>Surname or family name of a Subject.</
auth:Description>
            </auth:ClaimType>

            <auth:ClaimType
                Optional="true"
                    Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
streetaddress">

                <auth:DisplayName>StreetAddress</auth:DisplayName>
```

```
                <auth:Description>...</auth:Description>
            </auth:ClaimType>

            <auth:ClaimType
                Optional="true"
                    Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
locality">

                <auth:DisplayName>Locality</auth:DisplayName>
                <auth:Description>...</auth:Description>
            </auth:ClaimType>

            <auth:ClaimType
                Optional="true"
                    Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
postalcode">

                <auth:DisplayName>PostalCode</auth:DisplayName>
                <auth:Description>...</auth:Description>
            </auth:ClaimType>

            <auth:ClaimType
                Optional="true"
                    Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
country">

                <auth:DisplayName>Country</auth:DisplayName>
                <auth:Description>...</auth:Description>
            </auth:ClaimType>

            <auth:ClaimType
                Optional="true"
                    Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
dateofbirth">

                <auth:DisplayName>DateOfBirth</auth:DisplayName>
                <auth:Description>...</auth:Description>
            </auth:ClaimType>

            <auth:ClaimType
                Optional="true"
           Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/gender">

                <auth:DisplayName>Gender</auth:DisplayName>
                <auth:Description>...</auth:Description>
            </auth:ClaimType>

            <auth:ClaimType
```

```
                Optional="true"
                    Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
privatepersonalidentifier">

                <auth:DisplayName>PPID</auth:DisplayName>
                <auth:Description>...</auth:Description>
            </auth:ClaimType>

        </fed:ClaimTypesOffered>

        <fed:PassiveRequestorEndpoint>
            <wsa:EndpointReference>
                <wsa:Address>
                    https://127.0.0.1:54705/eid-idp/protocol/ws-federation
                </wsa:Address>
            </wsa:EndpointReference>
        </fed:PassiveRequestorEndpoint>

    </md:RoleDescriptor>
</md:EntityDescriptor>
```

Solicitud de Autenticación

Abajo se muestra un ejemplo de los parámetros de la solicitud de autenticación en la cadena de solicitud enviado al IdP.

```
wa=wsignin1.0
wtrealm=http://localhost:49267/BidIdpTest/
wctx=rm=0
id=passive
ru=/BidIdpTest/Default.aspx
wct=2011-01-05T08:14:31
```

Respuesta de Autenticación

Abajo se tiene un ejemplo del mensaje de respuesta WS-Trust después de una autenticación exitosa. Una aserción SAML v2.0 es entregada como un token por el IdP.

```
<trust:RequestSecurityTokenResponseCollection
    xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:wsa="http://www.w3.org/2005/08/addressing"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

    <trust:RequestSecurityTokenResponse Context="some-context-identifier">

       <trust:TokenType>urn:oasis:names:tc:SAML:2.0:assertion</trust:TokenType>

        <trust:RequestType>
            http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
        </trust:RequestType>

        <trust:KeyType>
            http://docs.oasis-open.org/ws-sx/ws-trust/200512/Bearer
        </trust:KeyType>

        <trust:RequestedSecurityToken>
            <saml:Assertion
                ID="saml-8eb46c40-c2d9-4c42-abc0-dcc9cbf425c1"
                IssueInstant="2010-05-05T14:51:03.324+02:00"
                Version="2.0">

                <saml:Issuer>CN=Test</saml:Issuer>

                <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                    ...
                </ds:Signature>

                <saml:Subject>
                    <saml:NameID>test-auth-identifier</saml:NameID>
                    <saml:SubjectConfirmation
                        Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
                </saml:Subject>

                <saml:Conditions
                    NotBefore="2010-05-05T14:51:03.324+02:00"
                    NotOnOrAfter="2010-05-05T15:51:03.324+02:00">
                    <saml:AudienceRestriction>
                        <saml:Audience>http://return.to.here</saml:Audience>
                    </saml:AudienceRestriction>
                </saml:Conditions>

                <saml:AttributeStatement>

                    <saml:Attribute
                         Name="http://schemas.xmlsoap.org/ws/2005/05/identity/
claims/givenname">
```

```
                        <saml:AttributeValue xsi:type="xs:string">
                            test-first-name
                        </saml:AttributeValue>
                    </saml:Attribute>

                    ...
                </saml:AttributeStatement>
            </saml:Assertion>
        </trust:RequestedSecurityToken>
    </trust:RequestSecurityTokenResponse>
</trust:RequestSecurityTokenResponseCollection>
```

Sign out

Algunas implementaciones WS-Federation realizan un cierre de sesión automático. Debido a este se tiene implementada la acción: wsignout1.0.

```
wa=wsignout1.0
wreply=http://localhost:49267/EidIdpTest/
```

Abajo se tiene un ejemplo de los parámetros de solicitud de cierre de sesión WS-Federation sign-out en la cadena que se envía al IdP.