Apéndice III

Ejemplos

Ejemplo de Token de Organismo

La Figura 1 presenta un ejemplo simplificado de un *token* SAML generado y firmado por un organismo, mostrando cómo ubicar los datos necesarios mediante el uso de *AuthenticationStatements* y *AtributeStatements*.

```
<saml1:Assertion xmlns:saml1="..." AssertionID="..."
        IssueInstant="2010-04-22T21:21:10.156Z"
        Issuer="Agesic" MajorVersion="1" MinorVersion="1">
        <saml1:AuthenticationStatement
               AuthenticationInstant="2010-04-22T21:21:10.062Z"
               AuthenticationMethod="...">
              <saml1:Subject>
                    <saml1:NameIdentifier Format="…">
                                 o=agesic, ou=certUy, ou=admin
                    </saml1:NameIdentifier>
                     ...
        </saml1:AuthenticationStatement>

        <saml1:AttributeStatement>
               <saml1:Subject>
                    <saml1:NameIdentifier Format="...">
                           o=agesic, ou=certUy, ou=admin
                     </saml1:NameIdentifier>
                    ...
               </saml1:Subject>
               <saml1:Attribute AttributeName="User"
                    AttributeNamespace="urn:simpletoken">
                    <saml1:AttributeValue ...
                                 xsi:type="xs:string">
                                Juan
                    </saml1:AttributeValue>
              </saml1:Attribute>
        </saml1: AttributeStatement>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            ...
        </ds:Signature>
```

Rol del Usuario

Rol del Usuario

Policy Name

Nombre de Usuario

Figura 1 – Ejemplo de un *token* SAML generado y firmado por un organismo

Ejemplo de RST

La Figura 2 presenta un ejemplo simplificado de un mensaje RST, mostrando cómo ubicar los elementos requeridos para la solicitud, utilizando WS-Trust.

```
<s:Envelope xmlns:a="..." xmlns:s="...">
  <s:Header>
      ...
  </s:Header>
  <s:Body>
     <RequestSecurityToken
        xmlns="http://schemas.xmlsoap.org/ws/2005/02/trust">
        <TokenType>                                              Tipo de token
         http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1
        </TokenType>
        <AppliesTo xmlns="http://schemas.xmlsoap.org/ws/2004/09/policy">
                  <a:EndpointReference>                          Servicio
                     <a:Address>http://192.168.40.190:9000/Servicio</a:Address>
                  </a:EndpointReference>
        </AppliesTo>
        <RequestType>
                http://schemas.xmlsoap.org/ws/2005/02/trust/Issue
        </RequestType>
        <Issuer>                                                 Policy Name
               <a:Address>urn:nac</a:Address>
        </Issuer>
        <Base>
            <saml1:Assertion xmlns:saml1="..." AssertionID="..."
                  IssueInstant="2010-04-22T21:21:10.156Z" Issuer="Agesic" ... >
                   ...                                           Token SAML emitido por
            </saml1:Assertion>                                   organismo
        </Base>
        <SecondaryParameters>                                    Rol del Usuario
                 <Rol>Doctor</Rol>
        </SecondaryParameters>
     </RequestSecurityToken>
  </s:Body>
</s:Envelope>
```

Figura 2 – Ejemplo de un RST

Ejemplo Token emitido por PGE

En la Figura 3 se presenta una versión simplificada de un *token* de seguridad emitido por la PGE.

```
<saml:Assertion AssertionID="..." IssueInstant="..." Issuer="..."
      MajorVersion="1" MinorVersion="1" xmlns:saml="...">
      <saml:Conditions NotBefore="..." NotOnOrAfter="...">
            <saml:AudienceRestrictionCondition>
                  <saml:Audience>                                    Servicio
                        http://192.168.40.190:9000/Servicio
                  </saml:Audience>
            </saml:AudienceRestrictionCondition>
      </saml:Conditions>
      <saml:AuthenticationStatement
            AuthenticationInstant="..." AuthenticationMethod="...">
            <saml:Subject>
                  <saml:NameIdentifier>                              Rol del usuario en
                        uid=rolPruebaDoctor,cn=agesic                la PGE
                  </saml:NameIdentifier>
            </saml:Subject>
      </saml:AuthenticationStatement>
      <saml:AttributeStatement>
            <saml:Subject>
                  <saml:NameIdentifier>                              Rol del usuario en
                        uid=rolPruebaDoctor,cn=agesic                la PGE
                  </saml:NameIdentifier>
            </saml:Subject>                                          Policy Name
            <saml:Attribute AttributeName="User" AttributeNamespace="urn:nac">
                  <saml:AttributeValue>Juan</saml:AttributeValue>    Nombre de
                                                                     Usuario
            </saml:Attribute>
      </saml:AttributeStatement>
      <ds:Signature Id="uuid2765608c-0128-1428-9ce4-8913af9af38d"
            xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...
      </ds:Signature>
```

Figura 3 – Ejemplo de un *token* SAML emitido por el STS de la PGE

Ejemplo de Invocación

La Figura 4 presenta un ejemplo simplificado de un mensaje SOAP para consumir el servicio "Certificado de Nacidos Vivos" utilizando los estándares WS-Addressing y WS-Security con la información mencionada anteriormente.

```
<env:Envelope xmlns:env='…'>
    <env:Header xmlns:wsa='…'>
        <wsse:Security env:mustUnderstand='1'
              xmlns:ds='...'    xmlns:wsse='...' xmlns:wsu='...'>
              <saml:Assertion AssertionID='...' IssueInstant='...'
                    Issuer='...' MajorVersion='1' MinorVersion='1'
                    xmlns:saml='urn:oasis:names:tc:SAML:1.0:assertion'>
                   ...
              </saml:Assertion>
        </wsse:Security>          Cabezales WS-Security: token SAML emitido por la PGE

        <wsa:To>http://192.168.40.190:9000/Servicio</wsa:To>
        <wsa:Action>

http://xml.cnve.msp.gub.uy/.../certificadoCNVEWSDLPortType/registrarCNVE
        </wsa:Action>          Cabezales WS-Addressing: To (Servicio) y Action (Método)

    </env:Header>
    <env:Body>
       <ns1:solicitudCNVE usuario='Juan'
            xmlns='http://xml.msp.gub.uy/schema/cnveSchema'
            xmlns:ns1='http://xml.msp.gub.uy/schema/cnveSchema'>
            <numeroCertificado />
            <datosMadre>
                      <primerNombre>Marta</primerNombre>
            </datosMadre>
       </ns1:solicitudCNVE>                    Información de Negocio
    </env:Body>
```

Figura 4 – Ejemplo de Mensaje SOAP para Consumir un Servicio de la PGE