ARCA | AGENCIA DE RECAUDACIÓN Y CONTROL ADUANERO

Especificación Técnica del WebService de Autenticación y Autorización

Índice de contenido

Introducción

Propósito

El siguiente documento describe los aspectos técnicos del servicio de Autenticación y Autorización de WebServices (WSAA) perteneciente a ARCA. Dicho servicio es necesario para que Entes Externos a ARC (EE) accedan a los WebServices de Negocio (WSN) ofrecidos por ARCA.

Descripción General del Servicio

El WS de Autenticación y Autorización es un servicio B2B (“Business to Business”) que permite que los computadores pertenecientes a ARCA y Entes Externos a ARCA intercambien información en forma directa sin intervención de operadores. En dicha tarea intervienen los siguientes componentes:

- Un cliente de WS desarrollado por un EE siguiendo las especificaciones de este documento.
- El WSAA, WS publicado por ARCA que implementa la autenticación de los computadores del EE (CEE) mediante certificados digitales X.509 y la autorización del mismo como consumidor de un determinado WebService de Negocio (WSN).

Al usar especificaciones y protocolos estándares (PKI, XML, CMS, WSDL y SOAP) el cliente puede ser desarrollado con cualquier lenguaje de programación moderno.

Para que un Ente Externo a ARCA (EE) esté autorizado a usar un WSN de ARCA, deberá realizar un tramite administrativo previo, cuya descripción esta fuera del alcance de este documento. Una vez finalizado exitosamente dicho trámite, el que incluye el alta de los CEE, el EE quedará registrado en el servicio de autorización de ARCA como entidad autorizada para usar el WSN.

Para que un CEE pueda utilizar efectivamente un WSN, deberá solicitar un “Ticket de Acceso” (TA) por medio del WS de Autenticación y Autorización (WSAA). Dicho requerimiento se realiza mediante el envío de un "Ticket de Requerimiento de Acceso" (TRA) del CEE al WSAA, mediante mensajería SOAP.

El WSAA realiza la verificación del TRA y si el requerimiento es correcto, devuelve un mensaje que contiene el TA que habilita al CEE a utilizar el WSN solicitado. El TA deberá ser utilizado por el CEE para acceder al WSN.

En la actualidad, los Web Services de la ARCA, no están incluidos en un UDDI (Universal Description Discovery Integration) de acceso externo, por lo tanto para acceder a los servicios que ofrece ARCA, es necesario utilizar WSDL (Web Services Definition Language) según la URL definida por ARCA. A partir del WSDL el EE puede construir un Cliente, para poder consumir el WSN correspondiente.

En términos generales, el presente documento detalla las operaciones a realizar para:

- Generar un "Ticket de Requerimiento de Acceso" (TRA)
- Invocar el "Web Service de Autenticación y Autorización" (WSAA)
- Interpretar el mensaje de respuesta del WSAA y obtener el "Ticket de Acceso" (TA)

Referencias

Para mejor entendimiento de la presente especificación, se recomienda estar familiarizado con los siguientes estándares:

- PKI, http://www.pki.org
- XML, http://www.w3.org/TR/XML/
- SOAP, http://www.w3.org/TR/soap/
- WSDL, http://www.w3.org/TR/wsdl/
- CMS, http://www.ietf.org/rfc/rfc3852.txt
- NTP, http://www.ntp.org

Invocación del WSAA

Fecha y hora de los CEE.

Los CEE que generan el TRA y reciben el TA deberán contar con la fecha y hora actualizada con precisión. Para ello se recomienda la sincronización de la misma mediante el el protocolo NTP (Network Time Protocol) con servidores que presten dicho servicio. Como ser “time.afip.gov.ar” u otros de libre disponibilidad.

WSDL del WSAA

A continuación, se expone el WSDL perteneciente al WSAA. El mismo estará disponible en una URL perteneciente a ARCA. El que se expone pertenece a un equipo de homologación.

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions targetNamespace="https://wsaa.afip.gov.ar/ws/services/LoginCms"
xmlns:apachesoap="http://xml.apache.org/xml-soap" xmlns:impl="https://wsaa.afip.gov.ar/ws/services/LoginCms"
xmlns:intf="https://wsaa.afip.gov.ar/ws/services/LoginCms"
xmlns:tns1="http://wsaa.view.sua.dvadac.desein.afip.gov" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:wsdlsoap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<!--WSDL created by Apache Axis version: 1.4
Built on Apr 22, 2006 (06:55:48 PDT)-->
 <wsdl:types>
  <schema elementFormDefault="qualified" targetNamespace="http://wsaa.view.sua.dvadac.desein.afip.gov"
xmlns="http://www.w3.org/2001/XMLSchema">
   <import namespace="https://wsaa.afip.gov.ar/ws/services/LoginCms"/>
   <element name="loginCms">
    <complexType>
     <sequence>
      <element name="in0" type="xsd:string"/>
     </sequence>
    </complexType>
   </element>
   <element name="loginCmsResponse">
    <complexType>
     <sequence>
      <element name="loginCmsReturn" type="xsd:string"/>
     </sequence>
    </complexType>
   </element>
  </schema>
  <schema elementFormDefault="qualified" targetNamespace="https://wsaa.afip.gov.ar/ws/services/LoginCms"
xmlns="http://www.w3.org/2001/XMLSchema">
   <complexType name="LoginFault">
    <sequence/>
   </complexType>
   <element name="fault" type="impl:LoginFault"/>
  </schema>
 </wsdl:types>
   <wsdl:message name="loginCmsResponse">
      <wsdl:part element="tns1:loginCmsResponse" name="parameters"/>
   </wsdl:message>
   <wsdl:message name="loginCmsRequest">
      <wsdl:part element="tns1:loginCms" name="parameters"/>
   </wsdl:message>
   <wsdl:message name="LoginFault">
      <wsdl:part element="impl:fault" name="fault"/>
   </wsdl:message>
   <wsdl:portType name="LoginCMS">
      <wsdl:operation name="loginCms">
         <wsdl:input message="impl:loginCmsRequest" name="loginCmsRequest"/>
         <wsdl:output message="impl:loginCmsResponse" name="loginCmsResponse"/>
         <wsdl:fault message="impl:LoginFault" name="LoginFault"/>
      </wsdl:operation>
   </wsdl:portType>
   <wsdl:binding name="LoginCmsSoapBinding" type="impl:LoginCMS">
      <wsdlsoap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
      <wsdl:operation name="loginCms">
         <wsdlsoap:operation soapAction=""/>
         <wsdl:input name="loginCmsRequest">
            <wsdlsoap:body use="literal"/>
         </wsdl:input>
         <wsdl:output name="loginCmsResponse">
            <wsdlsoap:body use="literal"/>
         </wsdl:output>
         <wsdl:fault name="LoginFault">
            <wsdlsoap:fault name="LoginFault" use="literal"/>
         </wsdl:fault>
      </wsdl:operation>
   </wsdl:binding>
   <wsdl:service name="LoginCMSService">
      <wsdl:port binding="impl:LoginCmsSoapBinding" name="LoginCms">
         <wsdlsoap:address location="https://wsaa.afip.gov.ar/ws/services/LoginCms"/>
      </wsdl:port>
   </wsdl:service>
</wsdl:definitions>
```

Flujo Principal

A continuación se describen los pasos que se deberán seguir para solicitar un TA al WSAA. Cada uno de los puntos es explicado detalladamente en los apartados siguientes.

1. Generar el mensaje del TRA (LoginTicketRequest.xml)
2. Generar un CMS que contenga el TRA, su firma electrónica y el certificado X.509 (LoginTicketRequest.xml.cms)
3. Codificar en Base64 el CMS (LoginTicketRequest.xml.cms.bse64)
4. Invocar WSAA con el CMS y recibir LoginTicketResponse.xml
5. Extraer y validar la información de autorización (TA).

Generación del documento del TRA (LoginTicketRequest.xml)

El primer paso para solicitar un TA es preparar el documento del TRA (denominado LoginTicketRequest.xml). Se puede utilizar una estructura XML ya definida que puede ser obtenida de un archivo externo o declarada como constante en el propio código. El esquema (schema, XSD) que describe dicho XML es el siguiente:

```
<?xml version="1.0" encoding="UTF8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:annotation>
    <xsd:documentation xml:lang="es">
     Esquema de Ticket de pedido de acceso a un WSN
     por parte de un CEE.
     Nro revision SVN: $Rev:1869 $
    </xsd:documentation>
  </xsd:annotation>
  <xsd:element name="loginTicketRequest" type="loginTicketRequest" />
  <xsd:complexType name="loginTicketRequest">
    <xsd:sequence>
          <xsd:element name="header" type="headerType" minOccurs="1" maxOccurs="1"/>
          <xsd:element name="service" type="serviceType" minOccurs="1"maxOccurs="1"/>
    </xsd:sequence>
    <xsd:attribute name="version" type="xsd:decimal" use="optional"default="1.0" />
  </xsd:complexType>
  <xsd:complexType name="headerType">
    <xsd:sequence>
          <xsd:element name="source" type="xsd:string" minOccurs="0" maxOccurs="1" />
          <xsd:element name="destination" type="xsd:string" minOccurs="0" maxOccurs="1"/>
          <xsd:element name="uniqueId" type="xsd:unsignedInt" minOccurs="1" maxOccurs="1"/>
          <xsd:element name="generationTime" type="xsd:dateTime" minOccurs="1" maxOccurs="1"/>
          <xsd:element name="expirationTime" type="xsd:dateTime" minOccurs="1" maxOccurs="1" />
    </xsd:sequence>
  </xsd:complexType>
  <xsd:simpleType name="serviceType">
    <xsd:restriction base="xsd:string">
      <xsd:pattern value="[az,AZ][az,AZ,\,_,09]*"/>
      <xsd:minLength value='3'/>
      <xsd:maxLength value='32'/>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:schema>
```

A continuación se detalla la descripción de los atributos. Los mismos deben respetar el formato definido en el XSD:

- ***source***: Campo opcional. Indica el DN del certificado que será utilizado por WSAA para verificar la firma electrónica del TRA generado por el computador (CEE) que realiza el requerimiento. Si no se incluye, se utilizará el primer certificado de firma incluido en el CMS. Si se incluye, deberá corresponder a uno de los certificados de firma incluidos en el CMS.
- ***destination***: Campo opcional. Indica el DN del WSAA, En caso de utilizarse, deberá ser "cn=wsaa,o=afip,c=ar,serialNumber=CUIT 33693450239" para el ambiente de producción y

  "cn=wsaahomo,o=afip,c=ar,serialNumber=CUIT 33693450239" para el ambiente de homologación.
- ***uniqueId***: Entero de 32 bits sin signo que junto con "***generationTime"*** identifica el requerimiento.
- ***generationTime***: Momento en que fue generado el requerimiento. La tolerancia de aceptación será de hasta 24 horas previas al requerimiento de acceso.
- ***expirationTime***: Momento en el que expira la solicitud. La tolerancia de aceptación será de hasta 24 horas posteriores al requerimiento de acceso.
- ***service***: Identificación del WSN para el cual se solicita el TA.

El siguiente es un ejemplo del documento LoginTicketRequest.xml generado por la EE *Empresa SA* cuya CUIT es *30123456789* y el DN del CEE es *cn=srv1,ou=facturacion,o=empresa s.a.,c=ar,serialNumber=CUIT 30123456789* solicitando acceso al WSN *wsfe*:

```
<?xml version="1.0" encoding="UTF8"?>
<loginTicketRequest version="1.0">
  <header>
    <source>cn=srv1,ou=facturacion,o=empresa s.a.,c=ar,serialNumber=CUIT 30123456789</source>
    <destination>cn=wsaa,o=afip,c=ar,serialNumber=CUIT 33693450239</destination>
    <uniqueId>4325399</uniqueId>
    <generationTime>20011231T12:00:0003:00</generationTime>
    <expirationTime>20011231T12:10:0003:00</expirationTime>
  </header>
  <service>wsfe</service>
</loginTicketRequest>
```

Generación del Ticket de Requerimiento de Acceso (TRA)

Se deberá generar un mensaje CMS del tipo "SignedData" que contenga el mensaje anteriormente generado (LoginTicketRequest.xml) y su firma electrónica utilizando SHA1+RSA. De esta forma, se obtiene el TRA (LoginTicketRequest.xml.cms).

Codificación en Base64 el TRA

Para poder enviar el TRA al WSAA, el mismo deberá ser codificado en Base64 (LoginTicketRequest.xml.cms.base64)

Envió del TRA al WSAA

Se debe invocar el método LoginCMS del WSAA. El mismo recibe como parámetro una cadena correspondiente a la codificación en Base64 del TRA (LoginTicketRequest.xml.cms.base64) y devuelve una cadena denominada LoginTicketResponse.xml. De esta última se deberá extraer el Ticket de Acceso (TA).

En caso de encontrarse algún error, el mensaje SOAP devolverá un “SoapFault” conteniendo código y descripción del error producido. La descripción podrá contener adicionalmente detalles mas específicos del error (ej: el XML expiró hace 10 minutos). La tabla siguiente lista los códigos de errores y su correspondiente descripción. En caso de que ARCA considere necesario, nuevos códigos de errores y su descripción serán agregados.

Los CEE que reciban códigos de errores diferente a wsaa.* o wsn.unavailable, no deberán solicitar nuevos TA hasta que no hayan solucionado el inconveniente, ya sea gestionando las autorizaciones de acceso al servicio mediante el Administrador de Relaciones, sincronizando la fecha y hora de los CEE, validando sus desarrollos, etc.

Para el resto de los errores, los CEE no deberán solicitar nuevos TA dentro de los siguientes 60 segundos.

Código	Descripción
coe.notAuthorized	CEE no autorizado a acceder los servicios de ARCA. No deberá solicitar nuevos TA hasta que no haya gestionado el acceso WSN correspondiente.
coe.alreadyAuthenticated	El CEE ha solicitado un ticket de acceso para el cual ya dispone de TA validos. No deberá solicitar nuevos TA mientras disponga de TA validos para ese WSN correspondiente.
cms.bad	El CMS no es valido
cms.bad.base64	No se puede decodificar el BASE64
cms.cert.notFound	No se ha encontrado certificado de firma en el CMS
cms.sign.invalid	Firma inválida o algoritmo no soportado
cms.cert.expired	Certificado expirado
cms.cert.invalid	Certificado con fecha de generación posterior a la actual
cms.cert.untrusted	Certificado no emitido por AC de confianza
xml.bad	No se ha podido interpretar el XML contra el SCHEMA
xml.source.invalid	El atributo 'source' no se corresponde con el DN del Certificado
xml.destination.invalid	El atributo 'destination' no se corresponde con el DN del WSAA
xml.version.notSupported	La versión del documento no es soportada
xml.generationTime.invalid	El tiempo de generación es posterior a la hora actual o posee más de 24 horas de antigüedad
xml.expirationTime.expired	El tiempo de expiración es inferior a la hora actual
xml.expirationTime.invalid	El tiempo de expiración del documento es superior a 24 horas
wsn.unavailable	El servicio al que se desea acceder se encuentra momentáneamente fuera de servicio
wsn.notFound	Servicio informado inexistente
wsaa.unavailable	El servicio de autenticación/autorización se encuentra momentáneamente fuera de servicio
wsaa.internalError	No se ha podido procesar el requerimiento

Extracción y validación del TA

LoginTicketResponse.xml es descripto en el siguiente esquema (schema, XSD):

```
<?xml version="1.0" encoding="UTF8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <xsd:annotation>
                <xsd:documentation xml:lang="es">
                        Esquema de Ticket de respuesta al pedido de acceso a un
                        WSN por parte de un CEE
                        Nro revision SVN: $Rev: 695 $
                </xsd:documentation>
        </xsd:annotation>
        <xsd:element name="loginTicketResponse" type="loginTicketResponse" />
        <xsd:complexType name="loginTicketResponse">
            <xsd:sequence>
               <xsd:element name="header" type="headerType" minOccurs="1" maxOccurs="1" />
               <xsd:element name="credentials" type="credentialsType" minOccurs="1" maxOccurs="1" />
            </xsd:sequence>
             <xsd:attribute name="version" type="xsd:decimal" use="optional" default="1.0" />
        </xsd:complexType>
        <xsd:complexType name="headerType">
            <xsd:sequence>
               <xsd:element name="source" type="xsd:string" minOccurs="1" maxOccurs="1" />
               <xsd:element name="destination" type="xsd:string" minOccurs="1" maxOccurs="1" />
               <xsd:element name="uniqueId" type="xsd:unsignedInt" minOccurs="1" maxOccurs="1" />
               <xsd:element name="generationTime" type="xsd:dateTime" minOccurs="1" maxOccurs="1" />
               <xsd:element name="expirationTime" type="xsd:dateTime" minOccurs="1" maxOccurs="1" />
            </xsd:sequence>
        </xsd:complexType>
        <xsd:complexType name="credentialsType">
                <xsd:sequence>
                        <xsd:element name="token" type="xsd:string" minOccurs="1" maxOccurs="1" />
                        <xsd:element name="sign" type="xsd:string" minOccurs="1" maxOccurs="1" />
                </xsd:sequence>
        </xsd:complexType>
</xsd:schema>
```

Los datos incluidos son los siguientes:

- ***source***: DN correspondiente al WSAA que generó el documento (producción / homologación)
- ***destination***: DN correspondiente del CEE autenticado por el WSAA
- ***uniqueId***: Entero de 32 bits sin signo que junto a "***generationTime"*** identifica al requerimiento.
- ***generationTime***: Momento en que fue generado el TA.
- ***expirationTime***: Momento en el que expira el TA.
- ***token*** y ***sign***: cadenas de caracteres que deben ser informadas al WSN (como variables TOKEN y SIGN). Las mismas componen el TA. El formato interno de estas cadenas puede diferir de un servicio a otro y su información contenida es interpretada por el WSN.

Se deberá verificar que el mensaje de respuesta, que incluye al TA, no se encuentre expirado mediante la variable "expirationTime" y su momento de generación sea válido mediante la variable "generationTime".

Un ejemplo de respuesta al requerimiento expuesto anteriormente es el siguiente:

```
<?xml version="1.0" encoding="UTF8"?>
<loginTicketResponse version="1.0">
  <header>
    <source>cn=wsaa,o=afip,c=ar,serialNumber=CUIT 33693450239</source>
    <destination>cn=srv1,ou=facturacion,o=empresa s.a.,c=ar,serialNumber=CUIT 30123456789</destination>
    <uniqueId>383953094</uniqueId>
    <generationTime>20011231T12:00:0203:00</generationTime>
    <expirationTime>20020101T00:00:0203:00</expirationTime>
  </header>
  <credentials>
    <token>cES0SSuWIIPlfe5/dLtb0Qeg2jQuvYuuSEDOrz+w2EnAQiEeS86gzYf7ehiU3UaYit5FRb9z/3zq</token>
    <sign>a6QSSZBgLf0TTcktSNteeSg3qXsMVjo/F5py/Gtw7xucTrUWbsrVCdIoGE8Cm1bixpuVPlr58k6n</sign>
  </credentials>
</loginTicketResponse>
```

El tiempo de validez de los TA emitidos es de 12 horas desde la fecha de emisión. Los CEE que hayan obtenido TA para un determinado servicio, deberán utilizarlo mientras sea valido, antes de solicitar uno nuevo.

Requerimientos de los certificados pertenecientes a los CEE

La autenticación de los CEE, se realizara mediante certificados “X.509v3”. Los mismos deberán cumplir con los siguientes requerimientos:

1. Ser emitido por una autoridad certificante reconocida por ARCA.
2. El DN deberá enmarcarse dentro de la RFC 2253 (http://www.ietf.org/rfc/rfc2253.txt)
3. El contenido del DN se debe cumplir los siguientes requisitos establecidos por la “Oficina Nacional de Tecnologías de Información” (ONTI), disponible en http://www.sgp.gov.ar/contenidos/onti/productos/docs/infraestructura/Anexo_III_Perfil_Minimo_de_Certificados_y_CRLs_v1.pdf
4. Los campos obligatorios son los siguientes:

- Campo 'commonName': DEBE corresponder al nombre del servicio o aplicación (ej. Sistema de Consulta) o al nombre de la unidad operativa responsable del servicio (ej. Gerencia de Compras).
- Campo 'serialNumber' (OID 2.5.4.5: Nro de serie): DEBE contener el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: "CUIT numero_de_cuit"

  (ej: “CUIT 20123456780”)
- Campo 'organizationName': DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada.
- Campo 'countryName': DEBE representar el país en el cual está constituida la Persona Jurídica, codificado según el estándar [ISO3166].

Requerimientos de canal seguro comunicación para los CEE, WSAA y WSN.

La comunicación entre los CEE y el WSAA , así también como entre los CEE y los WSN, debe realizarse mediante un canal de comunicación seguro SSL/TLS, empleando el protocolo HTTPS. La URL de acceso a los servicios deberá realizarse mediante su FQDN (fully qualified domain name).

Los certificados utilizados en dicha comunicación podrán contener extensiones SAN (Subject Alternative Name) sin que el CN corresponda al FQDN de la URL de acceso. Asimismo, deben cumplir con la siguientes características:

- Haber sido emitidos por una Autoridad certificante definida por el prestador de los servicios WSAA y los WSN. El listado de laS autoridades certificantes estarán disponibles en la página de ARCA.
- Haber sido emitidos para su utilización en servidores SSL/TLS.
- Estar vigentes.
- No estar revocados.

Los clientes que accedan al WSAA y a los diferentes WSN deberán verificar que cumplan con lo establecido en el párrafo precedente, como así también verificar que la URL de acceso corresponda a la del certificado SSL/TLS presentando por servicio, ya sea en el CN o en la lista de SAN para los certificados con dichas extensiones. De esta forma, podrán garantizar la identidad de los servidores a los cuales acceden.