

Referenced security token could not be retrieved

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2005-09/>

- *From:* "Nuno Guerreiro" <Nuno.Guerreiro@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 21 Sep 2005 08:05:04 -0700
-

Hi,

I'm attempting to call a .Net Web Service from a Java client and I always receive the above message.

I've already read many posts/replies about this issue and tried many suggestions, but none worked for me.

Here's what I've done:

I created a simple Hello World Web Service and then enabled WSSE for the project and, for the sake of simplicity, used the WSSE Configuration Tool and only required incoming SOAP messages to be signed (not encrypted). I didn't mark signature or encryption in outgoing messages. The fully generated "policyCache.config" file is below.

Then I generated a key/pair with a Java tool (keytool.exe) and a self-signed certificate. I exported this certificate to a file and then imported it (using MMC) to the "Local Machine | Other People" folder. I've also added it to the "Local Computer | Trusted Root Certification Authorities" folder so that the certificate can be trusted.

For obvious reasons, the imported certificate doesn't contain the private key.

Afterwards, I went back to the WSSE Configuration Tool and selected a specific Web Method to use the imported certificate from the "Local Machine | Other People".

Everything looks fine, but .Net keeps producing the "Referenced security token could not be retrieved" error message. Full Java-produced SOAP message is below.

Things I've already checked, based on suggestions on the Net:

.. "Grant access to the private key, via file permissions" – this suggestions doesn't make any sense in my case, since the Server is not supposed to have access to the private key.

ASP.Net is running with the Network Service account, not ASPNet. I'm assuming it has rights to read the Local Machine | Other People certificate

Referenced security token could not be retrieved

store.

.. Enabled policy tracing in Diagnostics, but no useful information is produced in SendPolicy.webinfo file. I don't see any ReceivePolicy.webinfo file being created.

.. The issuer name and serial number fields in the SOAP request match with the required ones in the policyCache.config file. I've used the X509 Certificate Tool to confirm that the RFC3280 Key Identifier matches the one expected by policyCache.config file.

My configuration is as follows:

.. .Net Framework 1.1.4322.2300 Version 1.1 Post-SP1 (Windows Server 2003 SP1)
.. WSSE 2.0 SP3
.. Java 1.5.0_05; Axis 1.2.1; WSS4J 1.1.0

Any help would be greatly appreciated.

Thanks in advance,

Nuno Guerreiro

BEGIN FULL SOAP MESSAGE REQUEST

POST /WebServices/BCP.B2B.WebServices/TestService.asmx HTTP/1.0
Content-Type: text/xml; charset=utf-8
Accept: application/soap+xml, application/dime, multipart/related, text/*
User-Agent: Axis/1.2.1
Host: localhost:8080
Cache-Control: no-cache
Pragma: no-cache
SOAPAction: "urn:bcpcorp.net/ws/B2B/TestService/Hello"
Content-Length: 1921

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Header>
    <wsse:Security
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
soapenv:mustUnderstand="1">
      <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>
```

Referenced security token could not be retrieved

Referenced security token could not be retrieved

```
<ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>
<ds:Reference URI="#id-28899428">
<ds:Transforms>
<ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Transform>
</ds:Transforms>
<ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>

<ds:DigestValue>pOOWxdXIgW/pHMXNHTECOPvW4UI=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>

<ds:SignatureValue>Ir5Au7k/hXes3YC19L+FSBBcB5jxhg/9LeYknRJett5/cxI04h9CR8Bjqnu0dvNAKz5OIf6p+r7W
<ds:KeyInfo Id="KeyId-5041714">
<wsse:SecurityTokenReference
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
wsu:Id="STRId-21764429">
<ds:X509IssuerSerial>
<ds:X509IssuerName>CN=Nuno
Guerreiro.OU=DCSD.O=MillenniumBCP.L=Oeiras.ST=Lisboa.C=PT</ds:X509IssuerName>
<ds:X509SerialNumber>1127311171</ds:X509SerialNumber>
</ds:X509IssuerSerial>
</wsse:SecurityTokenReference>
</ds:KeyInfo>
</ds:Signature>
</wsse:Security>
</soapenv:Header>
<soapenv:Body
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
wsu:Id="id-28899428">
<Hello xmlns="urn:bcpcorp.net/ws/B2B/TestService">
<subject>world</subject>
</Hello>
</soapenv:Body>
</soapenv:Envelope>
```

END FULL SOAP MESSAGE REQUEST

BEGIN policyCache.config FILE

```
<?xml version="1.0" encoding="utf-8"?>
<policyDocument xmlns="http://schemas.microsoft.com/wse/2003/06/Policy">
<mappings xmlns:wse="http://schemas.microsoft.com/wse/2003/06/Policy">
<!--The following policy describes the policy requirements for the
service: http://localhost/WebServices/BCP.B2B.WebServices/TestService.asmx
.-->
<endpoint
```

Referenced security token could not be retrieved

Referenced security token could not be retrieved

```
uri="http://localhost/WebServices/BCP.B2B.WebServices/TestService.asmx">  
<defaultOperation>  
<request policy="#Sign-X.509" />  
<response policy="" />  
<fault policy="" />  
</defaultOperation>  
</endpoint>  
</mappings>  
<policies  
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd  
xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy  
xmlns:wssp="http://schemas.xmlsoap.org/ws/2002/12/secext  
xmlns:wse="http://schemas.microsoft.com/wse/2003/06/Policy  
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd  
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing">  
<wsp:Policy wsu:Id="Sign-X.509">  
<!--MessagePredicate is used to require headers. This assertion should  
be used along with the Integrity assertion when the presence of the signed  
element is required. NOTE: this assertion does not do anything for  
enforcement (send-side) policy.-->  
<wsp:MessagePredicate wsp:Usage="wsp:Required"  
Dialect="http://schemas.xmlsoap.org/2002/12/wsse#part">wsp:Body()  
wsp:Header(wsa:To) wsp:Header(wsa:Action) wsp:Header(wsa:MessageID)  
wse:Timestamp()</wsp:MessagePredicate>  
<!--The Integrity assertion is used to ensure that the message is  
signed with X.509. Many Web services will also use the token for  
authorization, such as by using the <wse:Role> claim or specific X.509  
claims.-->  
<wssp:Integrity wsp:Usage="wsp:Required">  
<wssp:TokenInfo>  
<!--The SecurityToken element within the TokenInfo element  
describes which token type must be used for Signing.-->  
<wssp:SecurityToken wse:IdentityToken="true">  
  
<wssp:TokenType>http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3</w  
<wssp:TokenIssuer>C=PT, S=Lisboa, L=Oeiras, O=MillenniumBCP,  
OU=DCSD, CN=Nuno Guerreiro</wssp:TokenIssuer>  
<wssp:Claims>  
<!--By specifying the SubjectName claim, the policy system can  
look for a certificate with this subject name in the certificate store  
indicated in the application's configuration, such as LocalMachine or  
CurrentUser. The WSE X.509 Certificate Tool is useful for finding the correct  
values for this field.-->  
<wssp:SubjectName MatchType="wssp:Exact">C=PT, S=Lisboa,  
L=Oeiras, O=MillenniumBCP, OU=DCSD, CN=Nuno Guerreiro</wssp:SubjectName>  
<wssp:X509Extension OID="2.5.29.14"  
MatchType="wssp:Exact">z4WiMIXsNrhXIK4OgBtiS8qpI0E=</wssp:X509Extension>  
</wssp:Claims>  
</wssp:SecurityToken>  
</wssp:TokenInfo>  
<wssp:MessageParts
```

Referenced security token could not be retrieved

Dialect="http://schemas.xmlsoap.org/2002/12/wsse#part>wsp:Body()
wsp:Header(wsa:Action) wsp:Header(wsa:FaultTo) wsp:Header(wsa:From)
wsp:Header(wsa:MessageID) wsp:Header(wsa:RelatesTo) wsp:Header(wsa:ReplyTo)
wsp:Header(wsa:To) wse:Timestamp()</wssp:MessageParts>
</wssp:Integrity>
</wsp:Policy>
</policies>
</policyDocument>

END policyCache.config FILE

BEGIN WSSE SECTION IN WEB.CONFIG

<microsoft.web.services2>
<diagnostics>
<detailedErrors enabled="true" />
<policyTrace enabled="true" input="ReceivePolicy.webinfo"
output="SendPolicy.webinfo" />
</diagnostics>
<security>
<x509 storeLocation="LocalMachine" allowTestRoot="true"
useRFC3280="true" />
</security>
<tokenIssuer>
<autoIssueSecurityContextToken enabled="true" />
</tokenIssuer>
<policy>
<cache name="policyCache.config" />
</policy>
</microsoft.web.services2>

END WSSE SECTION IN WEB.CONFIG

.

-
- Prev by Date: **RE: FOLLOW UP – Re: what certificate to buy from Verisign ?**
 - Next by Date: **Re: how can we restrict what certificate WSE will use?**
 - Previous by thread: **Certificates for WSE**
 - Next by thread: **Re: WSE 2.0 SP3 and .NET Framework 2.0**
 - Index(es):
 - ◆ **Date**
 - ◆ **Thread**