

Re: Object contains only the public half of a key pair. A private

Re: Object contains only the public half of a key pair. A private

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2006-07/>

- *From:* Chris Fink <ChrisFink@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 6 Jul 2006 09:06:02 -0700
-

Hi Pablo,

Thanks for your help. Being said that my objective is to consume my customers WSE 3 webservice and that they have provided me their public key, when I configuring my client to consume their webservice, what do I select for the client key and server key? I wouldn't think that the customer would need to provide me their private key?

Thanks

"Pablo Cibraro" wrote:

Hi,

You need to deploy the certificates in the following way:

1. Client Side:

- Client public and private keys
- Server public key

2. Service Side

- Client public key
- Service public and private keys

The mutualCertificate assertion works as follow:

1. The client signs the message using the client public and private keys. It encrypts the message using the service public key
2. The service decrypts the message using the service private key. It verifies the signature using the client public key
3. The service signs the response message using the service public and private keys. It encrypts the message using the client public key
4. The client decrypts the message using the client private key. It verifies the signature using the service public key

Re: Object contains only the public half of a key pair. A private

Re: Object contains only the public half of a key pair. A private

Regards,
Pablo Cibraro
<http://weblogs.asp.net/cibrax>

"Chris Fink" <ChrisFink@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:D125BF8C-20A3-4F95-9958-8C7A15F8A9A4@xxxxxxxxxxxxxxxxxxxx>

I am attempting to call a webservice secured with the WSE 3.0 toolkit and
am
receiving the following error message. My assumption is that I installed
the
certs in the wrong location. I placed my public + private key cert in
the
localmachine my store and placed the customer's public key in the
localmachine address store. I used cert tools to grant everyone full
access
to my cert on the machine.

```
<?xml version="1.0" encoding="utf-8"?>
<log>
<outputMessage utc="7/5/2006 6:34:50 PM"
messageId="urn:uuid:27867ccf-fcc5-400e-ba0c-739e005ab59d">
<processingStep description="Unprocessed message">
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Body>
<Dispatch xmlns="http://xxx/webservices/>
<messageType>test</messageType>
<correlationId>test</correlationId>
<messageBody>test</messageBody>
<userName>test</userName>
<applicationName>test</applicationName>
<instance>test</instance>
<postBackUrl>test</postBackUrl>
</Dispatch>
</soap:Body>
</soap:Envelope>
</processingStep>
<processingStep description="Entering SOAP filter
Microsoft.Web.Services3.Design.MutualCertificate11Assertion+ClientOutputFilter"
/>
<processingStep description="Exception thrown: Object contains only the
public half of a key pair. A private key must also be provided."> at
System.Security.Cryptography.RSACryptoServiceProvider.SignHash(Byte[]
rgbHash, String str)
at
Microsoft.Web.Services3.Security.Cryptography.RSASHA1SignatureFormatter.SignHash(Byte[]
rgbHash)
at
```

Re: Object contains only the public half of a key pair. A private

Re: Object contains only the public half of a key pair. A private

```
Microsoft.Web.Services3.Security.Cryptography.RSASHA1SignatureFormatter.Sign(Stream  
data)  
at  
Microsoft.Web.Services3.Security.MessageSignature.BuildSignedInfo(SignatureFormatter  
formatter)  
at  
Microsoft.Web.Services3.Security.MessageSignature.ComputeAsymmetricSignature(AsymmetricKey  
key)  
at Microsoft.Web.Services3.Security.MessageSignature.ComputeSignature()  
at Microsoft.Web.Services3.Security.Security.SerializeXml(SoapEnvelope  
document)  
at Microsoft.Web.Services3.Security.Security.Execute(SoapEnvelope  
envelope)  
at  
Microsoft.Web.Services3.Security.SendSecurityFilter.ProcessMessage(SoapEnvelope  
envelope)  
at Microsoft.Web.Services3.Pipeline.ProcessOutputMessage(SoapEnvelope  
envelope)</processingStep>  
</outputMessage>  
</log>
```

My policy file is as follows:

```
<policies xmlns="http://schemas.microsoft.com/wse/2005/06/policy>  
<extensions>  
<extension name="mutualCertificate11Security"  
type="Microsoft.Web.Services3.Design.MutualCertificate11Assertion,  
Microsoft.Web.Services3, Version=3.0.0.0, Culture=neutral,  
PublicKeyToken=31bf3856ad364e35" />  
<extension name="x509"  
type="Microsoft.Web.Services3.Design.X509TokenProvider,  
Microsoft.Web.Services3, Version=3.0.0.0, Culture=neutral,  
PublicKeyToken=31bf3856ad364e35" />  
<extension name="requireActionHeader"  
type="Microsoft.Web.Services3.Design.RequireActionHeaderAssertion,  
Microsoft.Web.Services3, Version=3.0.0.0, Culture=neutral,  
PublicKeyToken=31bf3856ad364e35" />  
</extensions>  
<policy name="MyPolicy">  
<mutualCertificate11Security establishSecurityContext="false"  
renewExpiredSecurityContext="true" requireSignatureConfirmation="true"  
messageProtectionOrder="SignBeforeEncrypt" requireDerivedKeys="true"  
ttlInSeconds="300">  
<clientToken>  
<x509 storeLocation="LocalMachine" storeName="My"  
findValue="CN=PublicKeyClient"  
findType="FindBySubjectDistinguishedName"  
/>  
</clientToken>  
<serviceToken>  
<x509 storeLocation="LocalMachine" storeName="AddressBook"
```

Re: Object contains only the public half of a key pair. A private

```
findValue="E=webfarm@xxxxxxx, CN=XXX, OU=Information  
Technology, O=Compl  
Inc., L=Austin, S=TX, C=US"  
findType="FindBySubjectDistinguishedName" />  
</serviceToken>  
<protection>  
<request signatureOptions="IncludeAddressing, IncludeTimestamp,  
IncludeSoapBody" encryptBody="true" />  
<response signatureOptions="IncludeAddressing, IncludeTimestamp,  
IncludeSoapBody" encryptBody="true" />  
<fault signatureOptions="IncludeAddressing, IncludeTimestamp,  
IncludeSoapBody" encryptBody="false" />  
</protection>  
</mutualCertificate11Security>  
<requireActionHeader />  
</policy>  
</policies>
```