

RE: Unable to unwrap a symmetric key using the private key of an X.509

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2006-08/>

- *From:* MHoque <MHoque@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 18 Jul 2006 09:42:02 -0700
-

I am having the same problem while using Hands on Lab doc. Plus the Hands on Doc seems to be poorly written since it is skipping few important steps. Does any one know of a reworked Hands on lab doc.

"Chris Fink" wrote:

I have walked through all of the WSE 3 Hands on Labs and got everything working fine. When I create my own certificate and install it in the stores, my client application that is consuming my WSE enabled webservice receives the following error (noted at the very bottom of this post).

My objective here is to create and secure a service application (webservice) using an x509 test cert that requests a client certificate; and to create a test client to consume this service.

Following the makecert command that I used:
makecert -pe -n "CN=DecisionOne Corporation" -ss root -sr localmachine
DecisionOneEBSServices.cer

I installed this cert along with the embedded private key to the following stores:

Current User – personal, trusted root, and other people stores
Local Computer – personal, trusted root, and other people stores

Using the WSE 3.0 certificates tool, I gave FULL access to Everyone and the ASPNET user for all the 6 stores.

I enabled allow test roots in my WSE 3.0 settings>security for BOTH the client and the webservice.

Following is the policy file for my client:

```
<policies xmlns="http://schemas.microsoft.com/wse/2005/06/policy">  
  <extensions>  
    <extension name="usernameForCertificateSecurity"  
      type="Microsoft.Web.Services3.Design.UsernameForCertificateAssertion,  
      Microsoft.Web.Services3, Version=3.0.0.0, Culture=neutral,
```

RE: Unable to unwrap a symmetric key using the private key of an X.509

```
PublicKeyToken=31bf3856ad364e35" />  
<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="DellCertPolicy">  
<mutualCertificate11Security establishSecurityContext="false"  
renewExpiredSecurityContext="true" requireSignatureConfirmation="true"  
messageProtectionOrder="SignBeforeEncrypt" requireDerivedKeys="true"  
ttlInSeconds="300">  
<clientToken>  
<x509 storeLocation="CurrentUser" storeName="My"  
findValue="CN=DecisionOne Corporation"  
findType="FindBySubjectDistinguishedName" />  
</clientToken>  
<serviceToken>  
<x509 storeLocation="LocalMachine" storeName="AddressBook"  
findValue="CN=DecisionOne Corporation"  
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>
```

Following is the policy file for my webservice:

```
<policies xmlns="http://schemas.microsoft.com/wse/2005/06/policy">  
<extensions>  
<extension name="usernameForCertificateSecurity"  
type="Microsoft.Web.Services3.Design.UsernameForCertificateAssertion,  
Microsoft.Web.Services3, Version=3.0.0.0, Culture=neutral,  
PublicKeyToken=31bf3856ad364e35" />  
<extension name="mutualCertificate11Security"  
type="Microsoft.Web.Services3.Design.MutualCertificate11Assertion,
```

RE: Unable to unwrap a symmetric key using the private key of an X.509

RE: Unable to unwrap a symmetric key using the private key of an X.509

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="DellCertPolicy">
<mutualCertificate11Security establishSecurityContext="false"
renewExpiredSecurityContext="true" requireSignatureConfirmation="true"
messageProtectionOrder="SignBeforeEncrypt" requireDerivedKeys="true"
ttlInSeconds="300">
<serviceToken>
<x509 storeLocation="LocalMachine" storeName="My"
findValue="CN=DecisionOne Corporation"
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>

And finally, the ERROR from the event viewer.

Event Type: Error

Event Source: Microsoft WSE 3.0

Event Category: None

Event ID: 0

Date: 6/12/2006

Time: 2:27:58 PM

User: N/A

Computer: WMDVFRA002

Description:

System.ApplicationException: WSE841: An error occured processing an outgoing

fault response. ----> System.Web.Services.Protocols.SoapException:

System.Web.Services.Protocols.SoapException: Server was unable to process

request. ----> System.Security.Cryptography.CryptographicException: WSE600:

Unable to unwrap a symmetric key using the private key of an X.509

certificate. Please check if the account 'WMDVFRA002\ASPNET' has permissions

RE: Unable to unwrap a symmetric key using the private key of an X.509

to read the private key of certificate with subject name 'CN=DecisionOne Corporation' and thumbprint '32213F525B6DD6A8FDCA2D1E0876B873F44C759B'. ---->
System.Security.Cryptography.CryptographicException: WSE593: Unable to decrypt the key. Please check if the process has the right permission to access the private key. ---->
System.Security.Cryptography.CryptographicException: Bad Key.

at
System.Security.Cryptography.CryptographicException.ThrowCryptographicException(Int32 hr)
at System.Security.Cryptography.Utils. DecryptKey(SafeKeyHandle hPubKey, Byte[] key, Int32 dwFlags)
at System.Security.Cryptography.RSACryptoServiceProvider.Decrypt(Byte[] rgb, Boolean fOAEP)
at
Microsoft.Web.Services3.Security.Cryptography.RSA15KeyExchangeFormatter.DecryptKey(Byte[] cipherKey)
---- End of inner exception stack trace ----
at
Microsoft.Web.Services3.Security.Cryptography.RSA15KeyExchangeFormatter.DecryptKey(Byte[] cipherKey)
at Microsoft.Web.Services3.Security.EncryptedKey.Decrypt()
---- End of inner exception stack trace ----
at Microsoft.Web.Services3.Security.EncryptedKey.Decrypt()
at Microsoft.Web.Services3.Security.Security.LoadXml(XmlElement element)
at Microsoft.Web.Services3.Security.Security.CreateFrom(SoapEnvelope envelope, String localActor, String serviceActor)
at
Microsoft.Web.Services3.Security.ReceiveSecurityFilter.ProcessMessage(SoapEnvelope envelope)
at Microsoft.Web.Services3.Pipeline.ProcessInputMessage(SoapEnvelope envelope)
at Microsoft.Web.Services3.WseProtocol.FilterRequest(SoapEnvelope requestEnvelope)
at Microsoft.Web.Services3.WseProtocol.RouteRequest(SoapServerMessage message)
at System.Web.Services.Protocols.SoapServerProtocol.Initialize()
at System.Web.Services.Protocols.ServerProtocolFactory.Create(Type type, HttpContext context, HttpRequest request, HttpResponse response, Boolean& abortProcessing)
---- End of inner exception stack trace ----
---- End of inner exception stack trace ----

Any help is appreciated. I am out of options. My thoughts are that I created the certificate or installed it incorrectly.
Thanks very much!