

# Bad Key

**Source:**

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2004-05/>

---

**From:** Softwaremaker (*msdn\_at\_removethis\_softwaremaker.net*)

**Date:** 05/10/04

Date: Mon, 10 May 2004 22:14:04 +0800

Dear fellows,

OK, after working on WSE for some time, I found myself totally stumped by this problem which seems easy to solve BUT I just dont have the solution for it.

I am working on a demo with WSE using WS-Security. I use makecert.exe to make a cert with this command

```
makecert -n "CN=SomeCompany" -pe -ss root -sr localmachine WSETest.cer.
```

This was then installed in the local computer under the Trusted Root Directory. Then I publish a web service which uses this same cert to encrypt the soap message. Then I developed a client app on the same local computer to consume the secured Web Service using WSE1.0 sp1. The web service generated the Web Service fine as I could view the output file...However, the client throws an exception "Bad Key".

What do I do from here ?

WebService Code – This works fine

```
Public Function GetXmlDocumentX509() As XmlDocument
```

```
    'Create a simple XML Document to return
    Dim myDOC As XmlDocument = New XmlDocument
    myDOC.InnerXml = "<EncryptedResponse>X509 Asymmetric Encryption : This
is sensitive data.</EncryptedResponse>"
    Dim myContext As SoapContext = HttpContext.Current.ResponseContext
```

```
    'Open and read the Personal certificate store for
    the local machine account.
```

```
    Dim store As X509CertificateStore = _
    X509CertificateStore.LocalMachineStore(X509CertificateStore.RootStore)
    store.OpenRead()
```

```
    Return store.FindCertificateBySubjectName("CN=Softwaremaker.NET Pte
Ltd").Count
```

```
Dim cert As X509Certificate = store.FindCertificateBySubjectName _  
("CN=SomeCompany")(0)
```

```
'Make sure that we have a certificate that can be used for encryption.  
If cert Is Nothing Or cert.SupportsDataEncryption = False Then  
    Throw New ApplicationException("Service is not able to encrypt the  
response")  
    Return Nothing  
Else  
    'Use the valid certificate to create a security token.  
    Dim tok As X509SecurityToken = New X509SecurityToken(cert)  
  
    'Encrypt the message body using this security token.  
    'WSE will use this token to encrypt the message body.  
    'WSE generates a KeyInfo element used to request the  
    'certificate at the client used to decrypt the message.  
    Dim myEncData As EncryptedData = New EncryptedData(tok)  
  
    'Add the encrypted data element to the SoapContext of the  
    'response message.  
    myContext.Security.Elements.Add(myEncData)  
End If  
  
Return myDOC  
End Function
```

Web.Config File

```
<x509 storeLocation="LocalMachine" verifyTrust="false" allowTestRoot="False"  
>
```

ClientApp

```
Try  
    Dim a As localhost.WSE1WSSecurityWse = New localhost.WSE1WSSecurityWse  
    MessageBox.Show(a.GetXmlDocumentX509().InnerText)  
Catch ex As Exception  
    MessageBox.Show(ex.Message)  
End Try  
End Sub
```

App.Config File

```
<x509 storeLocation="LocalMachine" verifyTrust="false"  
allowTestRoot="false"/>
```

Should the app.config file be LocalMachine cos I installed the cert via makecert in the local machine root store. I have given proper permissions to both private keystores BUT yet still got the "Bad Key" exception.

Will appreciate any help. Thanks so much.

Regards.