

# X.509 Certificate based authentication

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2007-05/msg00091.html>

---

- *From:* [gudujarlson@xxxxxxxxxx](mailto:gudujarlson@xxxxxxxxxx)
  - *Date:* 18 May 2007 15:19:09 -0700
- 

I want to use X.509 certificates to authenticate and then subsequently authorize HTTP requests between a Windows Forms client and a ASP.NET server. So far I have accomplished all of the following:

- created and installed a server certificate
- setup a virtual directory to require client certificates
- created a ASP.NET web form that displays information about the client certificate
- created and installed a client certificate
- created a Windows Form application that looks up and passes the client certificate in a HTTP request to the server

Here's the guts of my client:

```
Dim aRequest As System.Net.HttpWebRequest =  
CType(System.Net.WebRequest.Create("https://localhost/ssl/  
default.aspx"), System.Net.HttpWebRequest)  
aRequest.ClientCertificates.Add(certificate)
```

Here's the guts of my web form:

```
Dim cs As HttpClientCertificate = Request.ClientCertificate  
Response.Write("Certificate = " & cs.Certificate.ToString() &  
"<br>")
```

All is working well. The cert gets passed over the wire and the server can read its contents. Now what?

How do I authenticate the client?

How to I use information from the certificate to identify the client? In other forms of authentication there is user identifier. What is the analogy with X.509 certificates? My first guess was that the "subject" property is the identifier, but I'm not sure that is correct because it does not appear to be globally unique. For example, the subject of my client cerificate is "localhost". I'm guessing I am not the only person on the planet with the same subject. How do I verify that the client is the right "localhost"?

## X.509 Certificate based authentication

How do I validate that the certificate was sent to me by it's owner?

Does calling `System.Net.HttpWebRequest.ClientCertificates.Add()` cause the HTTP request to be signed or does it simple cause the certificate to be passed in the request?

Does IIS do anything with the certificate or does it just pass it through the web form? I.e. does it perform any sort of validation/ authentication?

All help will be greatly appreciated.

.