

Re: X.509 Certificate based authentication

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2007-05/msg00109.html>

- *From:* "Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 23 May 2007 12:24:13 -0500
-

I hear what you are saying. The docs basically assume you already know a lot about the underlying mechanism (SSL) and don't bother to explain any of those details.

FWIW, there isn't really anything to have issue over with the actual implementation. It is just straight stock SSL with client certificate authentication. It will interoperate with other platforms that also use SSL client certificate authentication, as there is nothing proprietary here. You are limited in the algorithms that your MS operating system will use for the symmetric portion of the encryption and you have to work with Microsoft's approach to certificate and key stores as opposed to something like OpenSSL key stores, but the implementation of the algorithms are based on the standards.

Joe K.

Joe Kaplan-MS MVP Directory Services Programming
Co-author of "The .NET Developer's Guide to Directory Services Programming"
<http://www.directoryprogramming.net>

<gudujarlson@xxxxxxxxx> wrote in message
news:1179940215.170604.16040@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Yes, exactly. That is also the way I understand public-private keys to work. I think you misunderstand where I am at. My issue is with how Microsoft implemented these ideas in .NET and IIS. I have found nothing in Microsoft's documentation that says they implemented the ideas/mechanisms you describe. I've read nothing that says System.Net signs the HTTPS request with the certificate I provide. I have found nothing that says that IIS authenticates that the certificate it received is from the "owner" of the private key. If I don't read between the lines, the document says that System.Net sends a certificate to IIS and IIS makes it available to the ASP.NET application. This implies to me that I need to do all the work of signing and authenticating, however I have found no documentation on how to do that. I haven't found the signing API or the authentication

Re: X.509 Certificate based authentication

API. I've also not found any examples of server-side ASP.NET code that uses client certificates to do authentication and authorization.

I did however, find a blog written by someone have many of the very same questions as me (URL below).

http://www.codeproject.com/useritems/Certificate_Setup_HTTPS_.asp?df=100&forumid=395031&exp=0&s