

Re: X509 and SSL

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2004-10/>

From: Softwaremaker (*msdn_at_removethis_softwaremaker.net*)

Date: 10/20/04

Date: Wed, 20 Oct 2004 19:41:34 +0800

When you enable SSL / HTTPS on a particular folder, you are effectively encrypting the transport layer from client to your server for pages of that particular folder.

ALL content on that transport channel is encrypted, regardless of whether its HTML, XML or SOAP. This is achieved through a Handshake Protocol which exchanges asymmetric keys and challenge messages amongst others until a shared secret (Symmetric Key) is achieved. Thereafter anything that goes along this channel gets encrypted with this shared secret (Symmetric Key).

I could sit here and talk about the Handshake Protocol of SSL / HTTPS but this is not the right newsgroup to do it and it would take too long ;)

There can be good and bad things with SSL. Tremendous overheads is one. Another is, you are authenticating via machines, not users.

If you need to authenticate your clients via signatures, you may need client certs which may NOT be feasible. DO TAKE NOTE tho, you are authenticating requests via machines, not user, if you invoke SSL / HTTPS.

Singapore Coffee == Starbucks Coffee; Brazilian Cofee;
In other words, we import them like it is since we cannot grow them here :)

It is a different answer if you ask about food, that, my friend, it is a paradise here.

--

Thank you.

Regards,

Softwaremaker

<http://www.softwaremaker.net/blog>

=====

"andrea" <a.canade@retis.it> wrote in message

news:5c884a8f.0410200209.1e519a7c@posting.google.com...

> > > must i buy one certificate for sign response messages and one

> > > certificate to enable IIS

> > >

> > > or can i buy one certificate and configure IIS too?

> > >

> > > thank you for patience i'm a newbie on https and digital signing... i

> > > know :)

Re: X509 and SSL

microsoft.public.dotnet.framework.webservices.enhancements: Re: X509 and SSL

```
> > > andrea
> >
> > One certificate is sufficient is you don't need to identify the signing
> > application distinctly from the web server.
>
> [Andrea]
> SoftwareMaker correct me if i'm wrong,
> you tell me that i can buy only one certificate for signing server
response
> and that certificate must contain the SSL-Enabling feature
>
> with this "feature" i can configure an https environment on IIS and
> receive unsigned requests from clients
> and send signed response messages from webservice to clients
>
> right?
>
> ehm..
> I 've received no response about Singapore coffee quality :-)
> maybe i really came to visit you ;-)
>
> thanks a lot
> andrea
```