

Certificates? Need guidance...

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2005-02/0246.html>

From: Larry David (*MysteriousAilment_at_HealthyChoice.org*)

Date: 02/08/05

Date: Mon, 7 Feb 2005 16:08:37 -0800

Hi,

This is one of those posts where not only do I not know the answer, I don't fully understand the *question* that I should be asking... but I'll try my best:

I've designed a web site which authenticates users via a login page. The users can then access their account information. The types of reports that the user can run depend upon the user's access level. I'm currently storing all usernames, passwords, and access levels in a SQL Server database. I've been told that the web site needs to be made more "secure" in two ways:

- 1) ALL web requests/responses need to be encrypted via SSL.
- 2) A certain class of users, those with the highest access level, need to be authenticated in a manner that is more sophisticated than a simple username/password.

Now #1 was pretty straight-forward. I purchased a digital certificate from Thawte. I bound it to the ISA listener interface. All SSL connections are now terminated at the firewall and forwarded to the internal web server as plain HTTP. Great!

I'm stumped on #2 though. I've done some research and have learned that there are at least two ways to add EXTRA security to web sites. I can a) require client certificates and/or b) require the use of a smart card. Can anyone point me in the right direction on either of these options? Does ISA need to be configured in a particular way to allow certificate and/or smart card information to pass through? When ISA "bridges" the connection from SSL to plain HTTP, will this information be lost in transit? Is my ASP.NET web site supposed to ask the user to "swipe your smart card now?" If so, since this action is taking place on the client side, how will my ASP.NET page know when the swipe has taken place? How is the data transmitted? I'm utterly confused.

Mr. David