

Re: Use Dpapi with Shared Asp.Net Web Host?

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2005-01/0250.html>

From: Phil C. (*charlestek_at_rcn.com*)

Date: 01/24/05

Date: Mon, 24 Jan 2005 14:05:26 -0500

Thanks, Svein

Since the only directory I have access to on the web host server is a given asp.net directory for my files, I seriously doubt I would for security reasons be allowed to access the registry. Therefore, my alternatives do not look good at all.

Phil

"Svein Terje Gaup" <stgaup@broadpark.no.spam> wrote in message news:%23QKBVBkAFHA.1452@TK2MSFTNGP11.phx.gbl...

> *If you need to write your own DPAPI library, this might help:*

>

> <http://msdn.microsoft.com/security/securecode/dotnet/default.aspx?pull=/library/en-us/dnnetsec/html/SecNetHT08.as>

>

> *DPAPI is only suitable for encrypting and decrypting stuff on the same machine. If you need to decrypt on a different machine, DPAPI is useless.*

>

> *This article explains how to encrypt and store the connection string in the registry:*

> <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod25.asp>

>

> *HTH,*

> *Svein Terje Gaup*

>

> *"Phil C." <charlestek@rcn.com> wrote in message*

> *news:OXd0npeAFHA.2076@TK2MSFTNGP15.phx.gbl...*

>> *Hi.*

>>

>> *I'd like to use an encrypted database connection string. I'd also like*

>> *use an encrypted set of customer tables with a symmetric algorithm (and a*

>> *secure symmetric key) generated by .Net in my sql server database from*

>> *asp.net code stored on a shared host asp.net server.*

>>

>> *I've downloaded a set of vb.net code that is a rewrite of the c# dpapi*

>> *code posted on msdn. The dpapi should enable me to encrypt the*

>> *connection string, but the portion of the code that calls the encryption*

microsoft.public.dotnet.framework.aspnet.security: Re: Use Dpapi with Shared Asp.Net Web Host?

>> *class and encrypts a given string is a console application.*
>>
>> *The article accompanying the code states: "Note that you'll need to run*
>> *the console application on the IIS server to generate the encrypted*
>> *base-64-encoded string. this is because the EncryptString function*
>> *instructs the DPAPI to use the machine-wide key, so the encryption and*
>> *encryption will be valid only on the same machine.*
>>
>> *Since this is on a shared host thousands of miles away, and I don't*
>> *believe I can run any local console code on it,*
>> *does this mean I'm sunk????*
>>
>> *Basically I need some secure way of storing my encrypted connection*
>> *string and storing*
>> *my symmetric encryption key. I know how to write the code to use the*
>> *keys and algorithms to encrypt and decrypt things.*
>>
>> *I suppose I could hide bits and pieces of the each key*
>> *in different places in the code or database and append them together by*
>> *hardcoding, but*
>> *I believe that that could be discovered???? by disassembling my code*
>> *unless I use a professional obfuscator???*
>>
>> **HELP!**
>>
>> *--Insecure in Boston, MA*
>> *-->GO PATRIOTS!!!!!!!!!!!!!!!*
>>
>
>