

Re: Cryptography.

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2005-10/0171.html>

From: Bala Nagarajan (*baladotnet_at_newsgroups.nospam*)

Date: 10/17/05

Date: Mon, 17 Oct 2005 11:42:36 -0500

Thanks a lot guys for helping me out.
My situation is as follows.

My application will require users to logon to the system by supplying their windows credentials. Since i will have a loaded user profile can i use DPAPI user specific key to encrypt and decrypt data? Is this a correct approach?

I want to actually encrypt the whole configuration file during set up. I intend to encrypt the configuration file and save the encrypted contents to a different file and delete config file during the set up. Is this a good approach? If so how can perform this step (namely file delete and save) during my set up process?

Thanks

-Bala

"Paul Glavich [MVP ASP.NET]" <glav@aspalliance.com-NOSPAM> wrote in message news:OYtRtGjzFHA.1040@TK2MSFTNGP14.phx.gbl...

> Brock is correct. I have a managed wrapper for V1.x here

> (http://www.theglavs.com/glavtech/Downloads/DPAPI_Wrapper.zip)

> FYI, in V2.0, look into the ProtectedData and ProtectedMemory classes for

> equivalent DPAPI functionality built into the framework.

>

> --

> - Paul Glavich

> MVP ASP.NET

> <http://weblogs.asp.net/pglavich>

> ASPInsiders member - <http://www.aspinsiders.com>

>

>

> "Brock Allen" <ballen@NOSPAMdevelop.com> wrote in message

> news:b8743b113b4908c797fa88e90fbc@msnews.microsoft.com...

>> Oops, should read "Data Protection" API.

>>

>> *-Brock*
>> *DevelopMentor*
>> *<http://staff.develop.com/ballen>*
>>
>>> *Yeah, key management is a big problem. The way many of the built-in*
>>> *keys are managed for ASP.NET is to encrypt them per-machine with yet*
>>> *another key and let that key be managed by the LSA. This sounds odd,*
>>> *but I think it's the best thing we have. So, look into the DPAPI*
>>> *(DataProtected API) in Win32. I think Dominick has a managed wrapper*
>>> *for v1.x and IIRC there's a managed wrapper built into v2.0.*
>>>
>>> *-Brock*
>>> *DevelopMentor*
>>> *<http://staff.develop.com/ballen>*
>>>> *Hello,*
>>>> *I am using .NET's cryptography classes(Symmetric algorithm) to*
>>>> *encrypt/decrypt strings and streams. I want to know the place i*
>>>> *should*
>>>> *store*
>>>> *the Key and the IV values for the algorithms?Since these values are*
>>>> *sensitive information i definitely cannot store them in the code or*
>>>> *config files. Please elucidate me on this.*
>>>> *Thanks*
>>>>
>>
>>
>
>