

Re: DP API Security queries

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2006-02/msg00192.html>

- *From:* "Sachin Chavan" <sachinrchavan@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 21 Feb 2006 06:55:27 -0800
-

Hi Henning,

Thanks a lot for the info.

One more thing that I forget to mention was, I have already hard coded additional entropy in my code while encrypting and decrypting the plain text.

So, this means that even Microsoft, even though they have the key wont be able to decrypt the things right?

Thanks a lot once more for the quick reply.

Thanks,
Sachin Chavan.

"Henning Krause [MVP]" wrote:

Hi Aachin,

The encryption key is, as you said, maintained by Windows. Depending on the scope you are using (I assume you use machine, since you are in an ASP.NET application), any process on that machine can decrypt that value. Thats why you can pass along an array of bytes for additional security.

The other two questions have one answer: Base64. Just convert the byte array you get to a BASE64 string, and you will have no problem at all (use Convert.ToBase64String() method).

Greetings,
Henning

"Sachin Chavan" <sachinrchavan@xxxxxxxxxxxxxxxxxxxx> wrote in message <news:36FDD5EC-4C92-4395-9B50-5D44EC127230@xxxxxxxxxxxxxxxxxxxx>

Re: DP API Security queries

Hi,

In my application, I am using a .net wrapper class (a dll) which internally calls the Win32 DP API for encryption and decryption.

Now, my client has following queries:

1. Since the encryption Key is managed by Windows internally what is the security of the Key used for encryption?

i.e. Microsoft can be able to access such keys and therefore, the information is not secure.

2. What is the guarantee that the encrypted text thus generated won't contain characters not supported by xml. This may create problem, if they do generate such characters, since we store them to web.config which is an xml file.

And,

3. What is the guarantee that the encrypted text thus generated won't contain a double quote which denote end of the Value field in web.config. If it generates one, you will have a bad xml file.

Please help me, I am stuck up with this issues.

Thanks,
Sachin R. Chavan.