

Re: Win32 Application CryptoAPI

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2004-11/0306.html>

From: Doug Barlow (*soft_pedal_at_hotmail.com*)

Date: 11/25/04

Date: Thu, 25 Nov 2004 18:04:50 GMT

Darren,

I haven't tried running your programs yet, but I do have a few suggestions.

First, you've probably chosen the worst case algorithm for compatibility -- The old Microsoft CSPs mess with 40-bit RC2 to try to make it stronger, giving it an 88-byte salt, so you've got to manage the salt values, too. You might have better luck moving up to a 128-bit RC2 key, which doesn't default to a special salt value. Take a look at the MSDN documentation for CryptDeriveKey for details.

Next, I wouldn't assume the .NET PasswordDeriveBytes class derives the same key as the Win32 CryptDeriveKey service. In fact, I'd bet against it. You should come up with a common method for deriving a key, and make sure you use the same key and salt in both applications. You can import a plain-text session key into CryptoAPI by following the example shown in <http://support.microsoft.com/default.aspx?scid=kb:en-us:228786>.

I hope that helps,

Doug Barlow
The Soft Pedal Shop
<http://www.softpedal.net>

"Darren Bennett" <darren@work.com> wrote in message
news:167A699B-452A-4574-8FE4-00AE6ACBA4DC@microsoft.com...

> *Hi There,*

>

> *I have been scanning the newsgroups for a solution to my problem and have
> found that a few others are also experiencing the same problem but none of
> the solutions provided to them seem to work for me.*

> ...