

Re: RSA/RC2 key exchange

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2002-10/1649.html>

From: George Zheng [MS] (georgezh@online.microsoft.com)

Date: 10/31/02

From: georgezh@online.microsoft.com (George Zheng [MS])

Date: Thu, 31 Oct 2002 00:54:35 GMT

Hi,

The Crypto function packaged on .NET is under System.Security.Cryptography. As for the key exchange class, it is RSAPKCS1KeyExchangeFormatter and RSAPKCS1SignatureDeformatter. However, the encrypted result of the key is different to the original key format which was generated by CryptImportKey.

As for the original format, please refer to the following link

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/Security/base_provider_key_blobs.asp. As for the format of the BLOB on .NET, I need to do more research on it to know detailed information. It may takes a long time because I need analyze the BLOB and compare with the standard.

In addition, would you please let me know which key exchange algorithm you used?

This posting is provided "AS IS" with no warranties, and confers no rights.

George Zheng [MS]