

Re: How to exchange certificate ?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.platformsdk.security/2004-01/0106.html>

From: Richard Grossman (*richard_at_goldmail.net.il*)

Date: 01/12/04

Date: Mon, 12 Jan 2004 10:52:53 +0200

Hi,

"Michel Gallant" <neutron@NOSPAMistar.ca> wrote in message
news:Om9PH%23F2DHA.3216@TK2MSFTNGP11.phx.gbl...

> *Hi Richard,*

> *Which functions cause problems and what error messages?*

> *There is pretty good documentation and samples on this at:*

>

>

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/creating_and_receiving_enveloped

Look my problem is clear, I cannot used the microsoft api to envelop the
data cause the other part use java to decrypt
data. Thus I really want to do it manually I mean :

Without CryptoAPI : Generate a symmetric 128 bit key

 Encrypt (symmetric) the bulk data (payload)

with Rijndael symmetric algorithm

With Crypto API : Get the Public key from a particular certificate in
certificate store (I own ONLY a public key).

 Encrypt the symmetric key with RSA encryption

(Asymmetric)

> *Note that the emphasis in CryptoAPI is on CMS/PKCS#7 Enveloped Data*

> *messages (whereas standard Java 2 does not natively support directly*
generating

> *PKCS#7 messages, but only basic PKCS1 signatures and encryption blocks).*

Yes the default sun JCE doesn't provide PKCS#7 but free JCE provider like
Bouncy castle do it perfectly.

> *Are you specifying the correct certificate and store of the recipient*
after

> *you import the cert?*

Yes I found my certificate in store but I don't know how to get the public
key from it

As you have answered in my precedent post :

microsoft.public.platformsdk.security: Re: How to exchange certificate ?

>The *CERT_KEY_PROV_INFO_PROP_ID* is only available for a certificate
>contained in a certificate store AND having an associated private key.
>In fact, you can test any cert for an associated private key using:
>if (CertGetCertificateContextProperty(hCertCntxt,
CERT_KEY_PROV_INFO_PROP_ID,
>typically, certs in the AddressBook store are certs received from others
>(which of course you would/should NOT possess the corresponding private
key).

It's exactly the problem in PKI the sender doesn't have the private key only
the public. This key is contained in my certificate how can I access the key
??. I only want to encrypt the data, I only need the public key not the
private.

> If you want to compare with Java you should really be comparing Java
against
> .NET crypto :-)

Yes I've understand that .NET provide a really security framework
Unfortunately I don't write application with .NET but with delphi and I've
only access to Crypto API and not .NET framework.

Thank's for you time