

microsoft.public.security: RSA frustrations – encrypt with private, decrypt with public – possible?

RSA frustrations – encrypt with private, decrypt with public – possible?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-10/0656.html>

From: mRislan (*random_at_discordant.org*)

Date: 10/25/05

Date: Mon, 24 Oct 2005 21:03:58 -0400

OK – I've seen signs of numerous people being stuck pounding their heads against desks with the same problem as I have, but I haven't seen any definitive answers on the subject.

I don't need lectures on Alice and Bob; I'd prefer if someone give me a simple answer to what is, I think, a simple question. Can the following be implemented with framework Cryptography methods (or even interop on underlying Win32 DLLs)?

For e.g. software registration purposes, it seems simple and effective to do the following:

- User with name "Foo" requests license.
- Provider hashes "Foo" & some other license info, encrypts with private key, delivers it.
- User has public key (distributed with application), and decrypts hash with it. Program is happy and works.

Yes, program code can still be modified to subvert this in various ways – what can't, really?. But short of that, license information itself cannot (realistically) be forged assuming a sufficiently large keysize.

It seems clear that RSACryptoServiceProvider can't do this, and effectively only works the other way round. Nevermind CSP – I don't want anything to do with the 'keystore', I simply want server to sign, and client to decrypt with only the public key rolled up and obfuscated in the assembly delivered to them.

SignData and VerifyData work in the direction I want, but don't seem sufficient – I want to encrypt / decrypt a small amount of arbitrary data, not leave it in the clear and merely sign a hash on it.

Googling for "decrypt with public" and a hundred other variants, numerous people are answering people with the same question to the effect of "this is the wrong way to use RSA", "use the keystore",

microsoft.public.security: RSA frustrations – encrypt with private, decrypt with public – possible?

"distribute private key, hide and encrypt with public". The latter response at least makes me feel certain that I am not the world's most crypto-challenged individual after all... but I guess the root problem is that most responders are not paying attention to the quite clear descriptions of usage (ie as a software licensing mechanism) before they start talking about Alice and Bob and which directions make sense.

Clearly programs have used and continue to use RSA for precisely this kind of protection scheme for some time. It has been done in the pre-managed Win32 world for some time, and the approach seems to be becoming popular on other platforms:

<http://aquaticmac.com/>

<http://macromates.com/sigpipe/archives/2004/09/05/using-openssl-for-license-keys/#more-5>

RSACryptoServiceProvider looks to be a dead end for my purposes.

Is there any way to massage the kind of functionality I want out of the framework, or am I going to have to do the now so-very-familiar DotNet dance of reinventing the wheel? Please, somebody answer this clearly and definitively – so that nobody else has to waste days upon days swimming through documentation and toy code, getting nowhere fast.

Risl.