

pointers on DSA and assymetric signature validation needed

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2002-10/1593.html>

From: Alex Crookes (alex_Crookes@hotmail.com)

Date: 10/28/02

From: "Alex Crookes" <alex_Crookes@hotmail.com>

Date: Mon, 28 Oct 2002 06:34:11 -0800

I'm sure this is straight forward but crypto just scares me...

Basically, I am putting together a little app for a client for which I need to receive some command line params. To prevent tampering, there is a DSA hash passed as a signature. I have the public key, and I know how the information passed is being used to create the signature. How can I verify it? I've checked over the `system.security.cryptography.DSA` namespace but can't see anything that looks quite like what I need, specifically where to put the public key (it's in a file, not a certificate). Anyone have any code snippets or guidelines on this?