

Re: How to create signed crypto message (p7m)

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.platformsdk.security/2005-11/0112.html>

From: Leonid (*lkryvelyov_at_gmail.com*)

Date: 11/18/05

Date: 18 Nov 2005 03:02:02 -0800

Hi Rounner,

rounner@yahoo.com wrote:

> Leonid,

>

> *Is your question:*

> *How do I use MS API to compose an SMIME message? If so:*

My question is: How do I use MS Win32 CryptoAPI to compose PKCS#7 message from original data, signed hash of this data and signer's certificate with public key (without private key)?

> *Have you read rfc 2633?*

Yes, I read it and 3851, also 2315. But there is nothing about MS Win32 CryptoAPI in these documents, because they are recommendations/standards, not implementation.

> *I dont know what you mean when you say signing is encryption. Do you*

> *have a key pair (RSA for SMIME)? Does the receiver have the public key,*

> *or are they to receive it as a certificate?*

I meant that signing is encryption of HASH of original data to be signed with private key.

Key pair is inside smart card. Signing (encryption of hash) is performed inside smart card, it is never possible to get private key from smart card, but it is possible to get certificate with public key from smart card.

> *Will the receiver be getting this message as an email (using an smime*

> *compatible email client), or are you writing the client as well?*

My task is not sending messages by email. The task is the following: documents to be signed are stored in a database or filesystem on a server and accessible for read/sign via web application. Users can download either original data or signed data in PKCS#7 format. Users have to co-sign original data, in this case signatures and certificates must be added to PKCS#7 data on a server. I need to develop application, which will consist of two parts: client part and server part. Client part has to download data from server, show data to user and sign it in smart card. After sign, signed hash and certificate with public key must be uploaded to server. Server part must receive signed

hash and certificate and add this new co-signer's information to existing PKCS#7 data.

I know how to extract ANY existing information from PKCS#7 format by Win32 CryptoAPI, but I don't know how do I compose PKCS#7 signed data by Win32 CryptoAPI without access to private key. I wonder, whether is it possible at all with Win32 CryptoAPI? Because all functions require access to private key.

I know that it is possible to use OpenSSL or other open source libraries to perform required task, but my question is about Win32 CryptoAPI.

- > *The private and public keys are mathematically linked, you cant just*
- > *use one and any old number for the other. Note that the signing and*
- > *encryption key pairs need not be the same.*