

## Re: A question about CryptAcquireCertificatePrivateKey

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.platformsdk.security/2005-06/0118.html>

---

**From:** lelteto (lelteto\_at\_discussions.microsoft.com)

**Date:** 06/09/05

Date: Thu, 9 Jun 2005 10:35:09 -0700

Windows stores the CSP and private key associated with the certificate in the cert property CERT\_KEY\_PROV\_INFO\_PROP\_ID (you can get it using CertGetCertificateContextProperty).

This is, of course, true only when WINDOWS stores the cert. If you get the plain X509 cert from some data than you won't find this info.

Many CSPs associate their certs and private key on the SAME token; so if you get the cert the CSP will find the associated key.

Laszlo Elteto  
SafeNet, Inc.

"smveloso@gmail.com" wrote:

> *Hi Mitch,*  
>  
> *That would explain why the keycontainer with the corresponding*  
> *private key is not located by the "component" when I pass it a*  
> *"certificate object" that was created from a x509 file, since the file*  
> *itself would not contain the required extended properties...*  
>  
> *What puzzles me is that, sometimes, the "component" does find the*  
> *private key ! It seems to depend on the CSP being used (it works for a*  
> *smart card manufacturer's CSP but not with another's).*  
>  
> *The real problem I am facing is: I cannot rely on the certificate*  
> *being in a "system store" when a user needs my application to validate*  
> *a signature... so I look for the certificate in a corporate database*  
> *(where a certificate is stored as a base64 encoded x509 der). From the*  
> *"blob", a "certificate" is created and the public key extracted to*  
> *perform the validation. I would like to use the same approach for*  
> *signing (create a "certificate" from the blob, acquire the private key*  
> *handle and then sign), but since it is not certain that a private key*  
> *will be found (even if available), I guess I will have to use two*  
> *different approaches for certificate lookup...*  
>

microsoft.public.platformsdk.security: Re: A question about CryptAcquireCertificatePrivateKey

> *Thank you very much for you help !*

>

>

> *Michel Gallant escreveu:*

>> *Not sure about the accuracy of the following details, but my understanding*

>> *is that CryptAcquireCertificatePrivateKey checks the pCert provided, and*

>> *determines if the certificate EXTENDED PROPERTY:*

>> *CERT\_KEY\_PROV\_INFO\_PROP\_ID*

>> *exists. This indicates that the certificate has a matching and accessible private*

>> *key. I \*think\* this extended property is stored in the associated cert (or as part of the*

>> *proprietary public cert blob file at:*

>> *C:\Documents and Settings\<userid>\Application Data\Microsoft\SystemCertificates\My\Certificates*

>> *with the keycontainer name embedded in that blob. The exact location of this "blob"*

>> *and the extended properties (which are not part of the X509 binary der cert) to my*

>> *understanding is WinOS specific and can change (some earlier OS stored that blob in*

>> *registry??)*

>> *That keycontainer name then uniquely determines the corresponding private key blob file which*

>> *has a "unique key container" name, derived from SID and hash of keycontainer name, at:*

>> *C:\Documents and Settings\mgallant\Application Data\Microsoft\Crypto\RSA\<userSID>*

>>

>> *- Mitch Gallant*

>> *MVP Security*

>>

>

>