

Re: Security – Best Encryption Tool

Source: <http://www.tech-archive.net/Archive/VB/microsoft.public.vb.general.discussion/2004-06/0222.html>

From: Alek Davis (alek_xDOTx_davis_xATx_intel_xDOTx_com)

Date: 06/01/04

Date: Tue, 1 Jun 2004 10:17:10 -0700

Guarav,

If you go with Olaf's suggestion (deriving encryption key from the user's password hash), make sure that the password is protected within a session (I assume that the user does not enter password on the page which uses the credit card number). Also, take a look at CipherSafe.NET (<http://www.obviex.com/ciphersafe/>); it can give you some ideas.

Alek

"gaurav khanna" <gaurav.khanna@wipro.com> wrote in message news:dc575aed.0406010641.4d6cda4b@posting.google.com...

> *Hi*

>

> *I need to store the credit card information in my database. I have been looking for some third party tools which could provide encryption for credit card numbers.*

>

> *The help I need is:*

>

> *a) What is the most secure encryption tool that can be used to store credit card information?*

>

> *b) Any tool which implements AES and does not expect a private key to be supplied as shown in the sample application provided by Microsoft. But in this case customize tool needs to be provided as anybody can buy the tool and decrypt the information.*

>

> *c) What is the best way to secure a private key used by the algorithm like storing in RAM, registry, isolated storage etc? And how to implement it.*

>

> *d) If some code implementation, which allows encrypting securely is available.*

>

>

> *The client is ready to invest in Third Party Tool.*

> *I short listed two third party .Net components for encryption:*

>
> *Chilkat Software* (<http://www.chilkatsoft.com/dotNetCrypt.asp>)
>
> *ezCrypto .NET*
> (<http://www.componentsource.com/Catalog.asp?fl=A200&gf=+BUSFUNCDATAPC&gd=Encryption&bc=A100~A200~BUSFUNCDATAPC&sc=CS&PO=514745&option=10444&RC=FCSR&POS=1&bhcp=1>)
>)
>
>
>
> *Both the above are c# implemented tools and implement AES algorithm.*
>
> *But the problem is both ask for private key to be supplied. And I need*
> *to store the private key in a secure manner.*
>
>
> *The work round I decided was to use the dll provided by the tool.*
> *Write some login to generate dynamically private key for each of the*
> *registered users based on his profile. Store this logic in a dll and*
> *some how secure this logic, so that no body is able to access it. But*
> *how to secure the logic is a concern, as dll can also be hacked to*
> *view its contents.*
>
> *One option I was looking at was to use isolated storage as provided by*
> *.Net.*
> *But I'm not sure can we store and access a dll using isolated storage.*
>
>
> *It would be great if somebody can help me with the above problem.*
>
> *Regards*
> *Gaurav*