Best Practice for Database Encryption in SQL Server 2005

Asked 16 years, 2 months ago Modified 10 years, 10 months ago

Viewed 6k times

8

I need to develop an application which stores data in a SQL Server 2005 database (the app itself will be either a WCF Service or an Asp.Net Web Service).

Now, this data is supremely confidential, and I need to have it stored in an encrypted form in the database.

So, I am wondering what the best practices are around this. I know that there is some encryption capabilities that SQL Server has in-built. Is there a 'for dummies' type of resource for this so that I can quickly get going.

Alternatively I was thinking that I could encrypt/decrypt in my C# code and not in the database - maybe have a layer which handles this just above the data access layer (is that a good idea)?

sql-server-2005 encryption

Share

Improve this question

Follow

edited Oct 17, 2008 at 14:16

Rontologist

3,558 ● 1 ● 22 ● 24

asked Oct 16, 2008 at 8:49

Vaibhav

11.4k ● 11 ● 53 ● 71

4 Answers

Sorted by: Highest score (default)

3

Look at this link for a good introduction with samples.

I think doing the data encryption in the application is better, because in that case the transferred data is already encrypted. Otherwise you have to use a secure channel between your app and the database server.

It depends on your needs, i would say.

Share Improve this answer

Follow

answered Oct 16, 2008 at 9:57

Jan

16k ● 5 ● 37 ● 59

1

Have you considered encrypting your data at the file-system level?

It's Windows 2008/Vista only, but it should give you what you need and it's what it's designed for.

Share Improve this answer

Follow

answered Oct 16, 2008 at 11:22

Alan

13.7k ● 9 ● 45 ● 51

NEVER use bit locker, if you even read the wikipedia article you posted you should have known this. – Chris Marisic Dec 18, 2008 at 14:57

@ChrisMarisic, Why? I just read the article and see no problem mentioned on there which affects this scenario. – Ben Dec 5, 2012 at 11:16

0

Before you decide on an encryption method, you need to access what parts of the system are vulnerable. If the potential for unauthorized access to the database exists, does the same threat exist for your application? Someone could run your code through Reflector and determine what methods were being used to encrypt and decrypt. You can mitigate that exposure to some extent with the code obsfucators. If that concern is not a risk, then you may find it easier to encrypt your data at the application level.

Share Improve this answer

Follow

answered Nov 5, 2008 at 18:20

Chris Miller

4,899 ● 4 ● 34 ● 50

0

Encryption needs to happen in a few different places depending on the application. For example a consumer site using credit card info needs to encrypt the connection over the network to prevent man in the middle attacks or snooping. when the data is stored in the database you need to encrypt the data so that a low level sales rep cant read and access the customers credit card info , in which

you might want to implement column level encryption as appropriate permission in addition to this if your worried that one day the janitor at your data centre might steal one of your backups then you need TDE implement to encrypt data at the disk level.

Encryption has a performance overhead esp with regard to CPU usage more importantly the overhead depends on the alogrithim being used for exncryption.

Share Improve this answer

Follow

answered Feb 7, 2014 at 15:01

Jayanth Kurup

1