

## Re: SQL Server 2000 / 2005 Encryption

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2008-03/msg00011.html>

---

- *From:* "Rubens" <[rubensrose@xxxxxxxxxxxx](mailto:rubensrose@xxxxxxxxxxxx)>
  - *Date:* Mon, 3 Mar 2008 21:32:30 -0500
- 

Ok, encrypting the connection makes sense to me. So on to the data at rest.

2) You're also talking about encrypting the data stored "at rest" in the database. This is possible on SQL 2005 via built-in T-SQL statements and functions, but requires 3rd-party tools, usually some sort of extended procedures (XPs).

You require 3rd-party tools even when using the native SQL 2005 encryption to encrypt the data "at rest"? I thought SQL 2005 supported that natively, but SQL 2000 required the 3rd party tools to accomplish this?

The certificates used to encrypt your data stored on SQL Server 2005 and to encrypt your SSL connections will be different. SQL Server can generate its own self-signed certificates though, and that should make the SSL encryption/connectivity easier for you. Excel does not know how to decrypt data stored in SQL Server 2005 in encrypted form.

Ok, I can figure out the details on the certificates when I get to that point. But you mentioned Excel cannot decrypt this information. If we have end users using Tablet PC's that need to decrypt this data, are they going to have to use a T-SQL statement calling the decrypting functions / XP's through QA or SSMS to get it? Or is there a means of having this done seamlessly for them? They are not technical at all.

Many thanks again Mike,  
Rubens

"Mike C#" <[xyz@xxxxxxx](mailto:xyz@xxxxxxx)> wrote in message [news:OTIzEyYfiHA.6136@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OTIzEyYfiHA.6136@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

"Rubens" <[rubensrose@xxxxxxxxxxxx](mailto:rubensrose@xxxxxxxxxxxx)> wrote in message [news:CA7939A8-A98C-4202-9CC2-8D7052735B8E@xxxxxxxxxxxxxxxxxxxx](mailto:news:CA7939A8-A98C-4202-9CC2-8D7052735B8E@xxxxxxxxxxxxxxxxxxxx)

Excellent, thank-you Mike! This definitely points me in the right direction. Let me take a step back and explain what I am trying to accomplish and see if this makes sense. We will initially be doing this on a SQL 2000 machine.

We have data in a table that needs to be encrypted. Ultimately, this information needs to end up on a Tablet PC in Excel for users that have

## Re: SQL Server 2000 / 2005 Encryption

permission. So here is how I think we can accomplish this.

After I go through the steps you listed below, we need to distribute the certificate to the Tablet PC's and install it.

Once it is on the Tablet, does Excel just know to use this certificate because the information in the data dump / pivot table needs to be decrypted?

Is the same certificate used to secure the connection as well as decrypting the data in the table?

Does this make sense?

We need to separate these two issues you're talking about here:

1) You're talking about encrypting the connection to SQL Server, which is possible on SQL 2000 and SQL 2005 through SSL.

2) You're also talking about encrypting the data stored "at rest" in the database. This is possible on SQL 2005 via built-in T-SQL statements and functions, but requires 3rd-party tools, usually some sort of extended procedures (XPs).

The certificates used to encrypt your data stored on SQL Server 2005 and to encrypt your SSL connections will be different. SQL Server can generate its own self-signed certificates though, and that should make the SSL encryption/connectivity easier for you. Excel does not know how to decrypt data stored in SQL Server 2005 in encrypted form.