

## Re: SQL 2005 – Searching Encrypted SSN

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2006-06/msg00213.html>

---

- *From:* Ron Brent <[RonBrent@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:RonBrent@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 28 Jun 2006 00:24:02 -0700
- 

Thanks guys!

The bottom line is that I think I will do it with a third party database encryption solution. We have several hundreds of applications that use this data, and it does seem like a lot of work, if it is at all possible. I'd rather do it with a solution and vendor that has "real-life" experience.

Cheers,

Ron

"Remus Rusanu [MSFT]" wrote:

Usually this is done by storing a cryptographic hash (e.g. SHA256) of the clear text, in a separate column in addition to the encrypted column. The search is performed on the hash column, not on the encrypted column. The hash can be used only to find exact matches. The performance penalty is the cost of computing one hash to be searched for (e.g hash the clear text SSN, then search the hash value)

You should realize that this schema allows an attacker to validate whether a known SSN number is in the database or not, since he can compute the hash and search for it.

--

This posting is provided "AS IS" with no warranties, and confers no rights.

HTH,  
~ Remus Rusanu

SQL Service Broker  
[http://msdn2.microsoft.com/en-us/library/ms166043\(en-US,SQL.90\).aspx](http://msdn2.microsoft.com/en-us/library/ms166043(en-US,SQL.90).aspx)

"Ron Brent" <[RonBrent@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:RonBrent@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:E9D1C567-4499-4076-A67C-E72E38ABB104@xxxxxxxxxxxxxxxxxxxxx](mailto:news:E9D1C567-4499-4076-A67C-E72E38ABB104@xxxxxxxxxxxxxxxxxxxxx)

Hi,

Re: SQL 2005 – Searching Encrypted SSN

SQL 2005.

I would like to encrypt the SSN column (the PK).

Currently, I have an application that searches according to SSN (i.e. – the user types her SSN for verification, and then her details are retrieved from the SQL Server table).

So, the column that is encrypted is the only column that I can use to search according to, plus it should be the PK.

Is it possible to do it with the SQL 2005 encryption?

How do I solve the performance issue of searching (select \*...) on an encrypted column?

Many thanks,

Ron