

Re: SQL 2005 – Searching Encrypted SSN

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2006-07/msg00020.html>

- *From:* "Laurentiu Cristofor [MSFT]" <laur@xxxxxxxxxx>
 - *Date:* Thu, 6 Jul 2006 12:35:11 -0700
-

Because we did not find any compelling reason to provide this option. We have considered it, but we decided not to provide such a feature, because for most uses, it would not be a safe option. We recommend randomly generating IVs, so we did not want to add ambiguity by providing an option to specify custom IVs.

Thanks

—

Laurentiu Cristofor [MSFT]
Software Design Engineer
SQL Server Engine
<http://blogs.msdn.com/lcris/>

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

"Mike C#" <xyz@xxxxxxx> wrote in message
<news:ORer7OQoGHA.1208@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

"Laurentiu Cristofor [MSFT]" <laur@xxxxxxxxxx> wrote in message
<news:uNLoccGoGHA.2364@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Of course you are better: if you have two pieces of data encrypted with different IVs, you're not going to be able to tell whether they're identical or not, but if you use a fixed IV, the blobs will be identical. Storing the IVs with the data is ok, they're not supposed to be secret; the encryption key is the secret.

Thanks

That said, why is there no option to allow programmers to specify their own IV at encryption time?