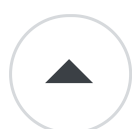


Encryption algorithm/library for .NET 2.0 + C++

Asked 16 years ago Modified 15 years, 7 months ago Viewed 2k times



2

I need a standard, Microsoft delivered, encryption library that works for both .NET 2.0 and C++. What would you suggest?



We find that AES is only offered in .NET 3.5 (and available in C++)



We find that Rijndael is used in .NET 2.0 but not available in the standard C++ libraries.

If I am wrong (very good chance), can you point me in the right direction?

Worst case scenario, I suppose I can call the Rijndael algorithm from .NET using PInvoke but I would rather have a native solution.

c++

encryption

.net-2.0

aes

rijndael

Share

Improve this question

asked Dec 1, 2008 at 17:02



Jason

4 Answers

Sorted by: Highest score (default)



We successfully do a similar thing that I hope might help you:

3



C++ CryptoAPI



- [CryptoAPI](#) is pure Win32 (c/c++), native to all Microsoft OS's.
- Use [Enhanced Cryptographic Provider](#) (`MS_ENHANCED_PROV`)
- Use [Triple DES](#) (`CALG_3DES`) algorithm

.NET TripleDes Provider

- Use [TripleDESCryptoServiceProvider](#) on the .NET side.

Side Notes

- We **avoid CAPICOM** like the plague as the deployment nightmares that come with it are not worth the hassle.
- Byte order on the .NET side can come into play at times. For example, to consume a key that is generated on the C++ (CryptoAPI) side, you need to

reverse the byte array prior to using it within the TripleDESCryptoServiceProvider.

If you would like more details please leave a comment and I can give more. Happy crypto!

Share Improve this answer

edited Jun 20, 2020 at 9:12

Follow



Community Bot

1 • 1

answered Dec 1, 2008 at 19:36



Scott Saad

18.3k • 11 • 66 • 85

Thank you. I will look into this... and of course, any other information you could provide, I would be delighted.

– Jason Dec 1, 2008 at 20:18

don't forget the AES Crypto Provider - also available as part of Windows. [msdn.microsoft.com/en-us/library/aa386979\(VS.85\).aspx](https://msdn.microsoft.com/en-us/library/aa386979(VS.85).aspx)

It delivers AES algorithms, which is what the OP wanted I think. – Cheeso May 13, 2009 at 15:36

True, but it's worth noting that AES algorithms are not supported on Windows 2000/NT. – Scott Saad May 14, 2009 at 14:50



3

AES and Rijndael are essentially the same algorithm with a restriction on block size and cipher mode. So as long as you can live with the [restrictions](#) (which are not onerous) you can use them interchangeably.



Share Improve this answer

answered Dec 1, 2008 at 17:25



Follow



[Stephen Martin](#)

9,645 ● 3 ● 28 ● 36



0

3DES is available via Capicom. See [here](#) for info.

Share Improve this answer

answered Dec 1, 2008 at 17:16

Follow



[Brian](#)

25.8k ● 18 ● 86 ● 178



0

Windows includes a C/C++ AES encryption library, as part of the [AES Cryptographic Services Provider](#). It is suitable for use from within native C/C++ applications.



Share Improve this answer

answered May 13, 2009 at 15:37

Follow



[Cheeso](#)

192k ● 105 ● 483 ● 734

