Sure, you can implement your own cryptographic service provider for a standard algorithm, but why would you?

devblogs.microsoft.com/oldnewthing/20181105-00

November 5, 2018

Raymond Chen

A customer wanted to write their own custom implementation of an existing standard encryption algorithm. The customer liaison noted that this custom implementation would presumably produce results identical to the built-in implementation because it is, after all, a standard. But if that's the case, there doesn't seem to be much point to the undertaking.

There was some speculation as to why the customer wanted to reimplement a standard algorithm. Maybe they thought they could do a better job by taking advantage of special-purpose instructions in the CPU for encryption and decryption? But a member of the security team confirmed that the built-in providers already take advantage of those instructions if available. "Unless your customer wants to use a mode that the built-in providers don't support, there is no technical reason for them to write their own implementation."

The customer liaison reported that the customer was trying to close a deal with a client. The client wants to be able to configure Exchange to use a customized encryption algorithm. "They might not end up creating such a customized encryption algorithm, but they want to be sure that it's possible, so they need a proof-of-concept demonstration." The customer found the Cryptographic Provider Development Kit and was working through the sample provider.

One person contributed to the discussion with a story from personal experience:

> I worked at a company where custom cryptography was a government requirement. Don't do it. Developing and supporting custom cryptography is a multi-year undertaking. It is technically possible, but I don't think your customer is willing to invest so much. You need to position the solution differently.

Aaron Margosis agreed. "Sometimes, people take technical requirements too literally when they should be looking at the bigger-picture business requirement, which can often be met with existing technologies."

Raymond Chen

Follow