

Re: nonce in aes-ccm

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-06/2053.html>

From: Henrick Hellström (henrick.hellstrm_at_telia.com)

Date: 06/28/04

Date: Mon, 28 Jun 2004 17:13:50 GMT

Gelo Ilzi wrote:

> *Can anybody explain if the nonce value in aes-ccm protocol must be
> stored in secret?*

No. It can, in principle, be treated in the same way you would treat an IV for e.g. aes-cbc. That is, it can be public but for every new message the nonce should be independent of past cipher texts. (One difference is that the aes-ccm nonce doesn't necessarily have to be random, but might just as well be an message counter. Another difference is that the aes-ccm nonce is always smaller than the block size.)