

Re: What does the MAC in IES or ECIES achieve ?

Re: What does the MAC in IES or ECIES achieve ?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-10/msg00947.html>

- *From:* fabrice.gautier@xxxxxxxxxx
 - *Date:* 30 Oct 2006 12:34:03 -0800
-

Tom St Denis wrote:

fabrice.gaut...@xxxxxxxxxx wrote:

Hi,

What does the addition of a MAC achieve for IES/ECIES ?

IIRC IES is just DH with a MAC strapped on. The goal is to ensure both the privacy and integrity of the message are in tact.

It doesn't give you nonrepudiation qualities since the authenticity is anonymous.

Tom

I understand how it could bring integrity, but how does that gives you privacy ?

Also, If I also use ECDSA (or whatever signature) to authenticate the message, I also get integrity, so could I do away with the MAC ?

I also noticed that the MAC is done on the encrypted text, while I assumed the Signature would be on the Clear Text, does that make any difference ?

.