

Re: protocol for proofing sending a document

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-06/2027.html>

From: Thomas Pornin (*pornin_at_nerim.net*)

Date: 06/28/05

Date: Tue, 28 Jun 2005 14:15:24 +0000 (UTC)

According to David Wagner <daw-usenet@taverner.cs.berkeley.edu>:

- > *No problem. If Bob wants to cooperate, he can sign a statement*
- > *saying "I, Bob, have received the following document: <...>".*
- >
- > *If Bob doesn't want to cooperate, he might receive the document and*
- > *then refuse to sign such a statement. Is it a security goal to prevent*
- > *that? If so, I think your problem as stated is going to be unsolvable.*

You can still get workable approximations. For instance, you can send the document byte by byte, and require a signed receipt for each byte before sending the next one. Thus, Alice can prove that even an uncooperating Bob has received the document, except maybe the last byte.

Another way to solve the problem is to use a "trusted publisher" whose role is to publish incoming messages, for everybody, and to never erase them. Alice sends the message to the publisher, who signs the message (with a timestamp). That signature is enough for Alice to prove that Bob is able to get the message at will. It all depends on how you define "send".

--Thomas Pornin