

Digital signing of emails

Written by Subhashis Banerjee

Tuesday, 15 February 2011 15:22 - Last Updated Wednesday, 30 March 2011 20:24

All emails originating from the CSC mail servers will henceforth be digitally signed by default using [DKIM](#) signature, and the recipients will be able to verify both i) the authenticity of sender and ii) that the message has been received unaltered.

To be sure that the email has originated from IITD, users can examine the full mail headers and look for the lines:

```
Authentication-Results: mailstore.iitd.ernet.in (amavisd-new); dkim=pass  
header.i=@xyz.iitd.ernet.in and DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=  
xyz.iitd.ernet.in; .....
```

If the *DKIM-Signature* is missing then the mail has not been sent through the IITD email servers.

Alternatively, to verify the authenticity of the sender and the content, users may save the email as a text file with full headers and submit the saved mail to the URL <https://userm.iitd.ernet.in/cgi-bin/mail/email-verify.pl>

Please note that most email clients, including Squirrelmail (View message details -> Save message), allow saving of emails with full headers as text files (eml format) which can then be submitted to the above URL for verification.