The Computer Services Centre will release a new email system for IITD starting January 2, 2010. The new mail system will use user and mailing list definitions from the IITD LDAP and use Kerberos for authentication.

Some of the prominent features of the new set up are:

- The new mail set up supports mailing lists for individual groups and courses. Please see the LDAP group definitions for group mailing.
- *mailstore.iitd.ernet.in* is the new server where emails are stored and *smtp.iitd.ernet.in* is the new server (actually a group of servers) for mail delivery.

- All mails originating from our smtp servers will be for authenticated senders and will be digitally signed. The receiving servers will be able to verify that the mails originating with addresses like *.iitd.{ac,ernet}.in have indeed originated from IITD.
- We support IMAP for mail reading and smtp for mail transfer.
- One can either set up one's favourite mail client to access mail using IMAP and smtp, or use the Webmail from a browser. The CSC also supports Roundcube webmail .
- We support mail reading thorugh a Dovecot IMAP server . Direct login/ssh to the server *mailstore.iitd.ernet.in*
is not allowed. All mail reading from the server is supported through IMAP only over a secure SSL
encrypted channel to ensure that passwords and mails never travel in clear text.

- We require SASL authentication over a TLS/SSL channel for smtp (sending emails). This is a departure from the earlier practice where no authentication was required for sending mails. We are stopping the earlier practice of permitting relaying without authentication if the mail originated from trusted networks (within IITD).

- With both way secure authentication, it will now be possible to read/send mails even from outside IITD using your favourite mail client software like Thunderbird, Outlook or Apple mail. No change of configuration will be required.
- We support opportunistic TLS encryption for all mail transfers. Mail exchange with other servers will use TLS if the other party supports it, and use plain text otherwise.

- We use **Amavis and Clamav based virus scanning** for both inbound and outbound mails. The virus definitions are automatically updated on a daily basis. All mails which are detected to contain a virus are purged outright.

- We use two popular spam filters: Spamassassin and DSPAM . We use a Spamassassin's cocktail rules for spam filtering and use DSPAM for user specific statistical SPAM definition learning and filtering. Spamassassin's spam rules are updated on a daily basis.

For DSPAM to be really effective the users will need to train their individual filters with training examples.

- Delivery to user mailboxes are done using procmail , after depositing the detected SPAM messages in a folder called **SPAM** in the user's ~/**mail** directory.

- Forwarding of emails using **.forward** is not supported; users are advised to set up their email forward address in their LDAP profile .
- There is a limit of 20MB on attachments. There is also a size limit of 300KB on mails to lists and groups.
- There is a limit of 60 mails per user per hour.