3.2 Data Transmission

What happens if an e-mail concerning a confidential matter has been tampered with along the way ?

3.2.1 E-mail

Policy All official e-mails must be transmitted in a secure manner to ensure **integrity**, **authentication** and **non-repudiation** on the part of the sender; and **non-denial of receipt** on the part of the recipient. In addition to that **confidentiality** for all classified official e-mails must be ensured also.

Standard All official e-mails must be signed using private key and all classified e-mails must be encrypted using public key before being sent. The minimum key length is 128 bits. For the purpose of compatibility , there should be only one asymmetric cryptographic system to be used throughout the state government. The sender must be notified of successful delivery of official e-mail.

Procedure Steps to use asymmetric cryptographic system for official e-mail transmission are as follows :

(1) Register, Install and Publish Digital Certificate

- Every government staff will be given a digital certificate, installed and published where necessary.

(2) Sender Signs, Encrypts, and Sends E-mail

- Sender must ensure that all official e-mails are signed (and encrypted for classified e-mails), and set request for return receipt before sending.
- Sender must report to the mail administrator upon failure of receiving a return receipt within 5 working days.
- If any e-mail bounces back, the sender must refer to the mail administrator.

(3) Recipient Receives Signed and/or Encrypted E-mail

- Recipient must acknowledge the receipt of all official e-mails.
- Upon receipt of official e-mails which are not signed, the recipient must inform the sender to resend with a signed version.
- Upon receipt of e-mails which are suspected of being tampered with, the recipient must :
  i report to sgCERT
  ii inform the mail administrator
  iii not do anything to the suspected e-mail

- Upon receipt of e-mails which are suspected of containing malware (e.g., viruses, worms, malicious code, etc.), the recipient must :
  i inform the mail administrator
  ii delete the e-mail

Guidelines

(1) The cryptographic system used must be reviewed yearly or as and when deemed necessary by the government.
(2) Classified e-mails are official e-mails which are categorized as “Rahsia Besar”, “Rahsia”, “Sulit” or “Terhad”.
(3) All e-mails bearing the sabah.gov.my domain are considered as official e-mails.
(4) Refer to www.sgCERT.org for information on how to make reports to sgCERT.