

SECUREMAIL USER GUIDE

BACKGROUND

NBIM sends and receives sensitive and business critical information to and from central authorities, collaborating organisations and business partners. It is critical that the information is secured against misuse.

To be able to exchange confidential information with external parties via e-mail, NBIM has installed the product "Ironport Encryption Appliance". The system consists of a special key server residing at NBIM, where external parties can log in to decrypt e-mails sent to them from NBIM. All external parties will be given an e-mail account on this server as soon as a NBIM user sends the first encrypted e-mail to them. The same system can be used by external parties to send encrypted e-mail back to NBIM

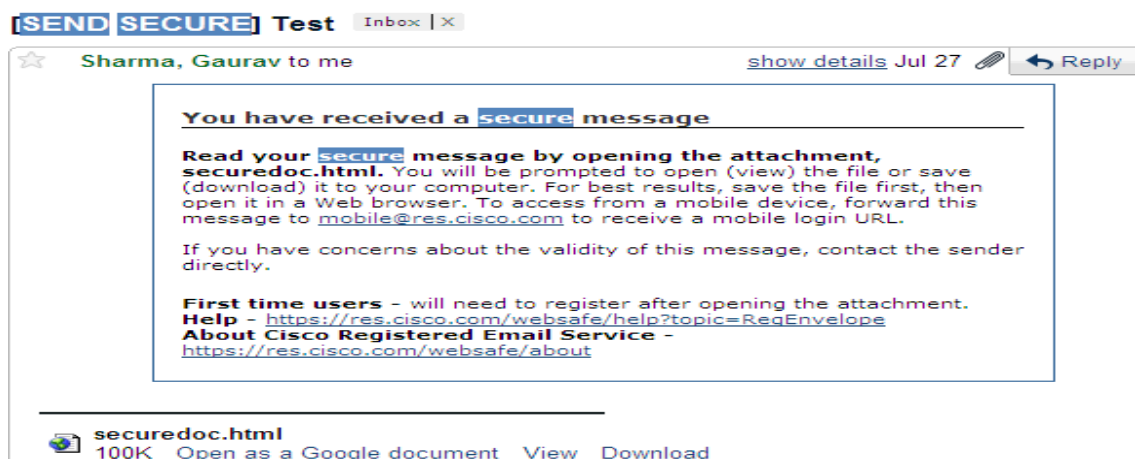
The following sections describe how secure information is exchanged:

A NBIM USER SENDS A SECURE E-MAIL TO THE EXTERNAL USER *N.N@EXTERNAL.COM*

The mails are routed for encryption by one of the following:

- a. By the use of Outlook Plug-in "SEND SECURE" distributed to NBIM's users.
- b. By tagging the mail with keyword [SEND SECURE] / [SECURED] in the subject field of the message.

The e-mail will then be encrypted and sent to the user's email address n.n@external.com in the form of Registered Envelope with Encrypted payload as attachment. When the external user receives the e-mail, they will see a text informing them of the encrypted e-mail, and instructions on how to open the e-mail attachment.



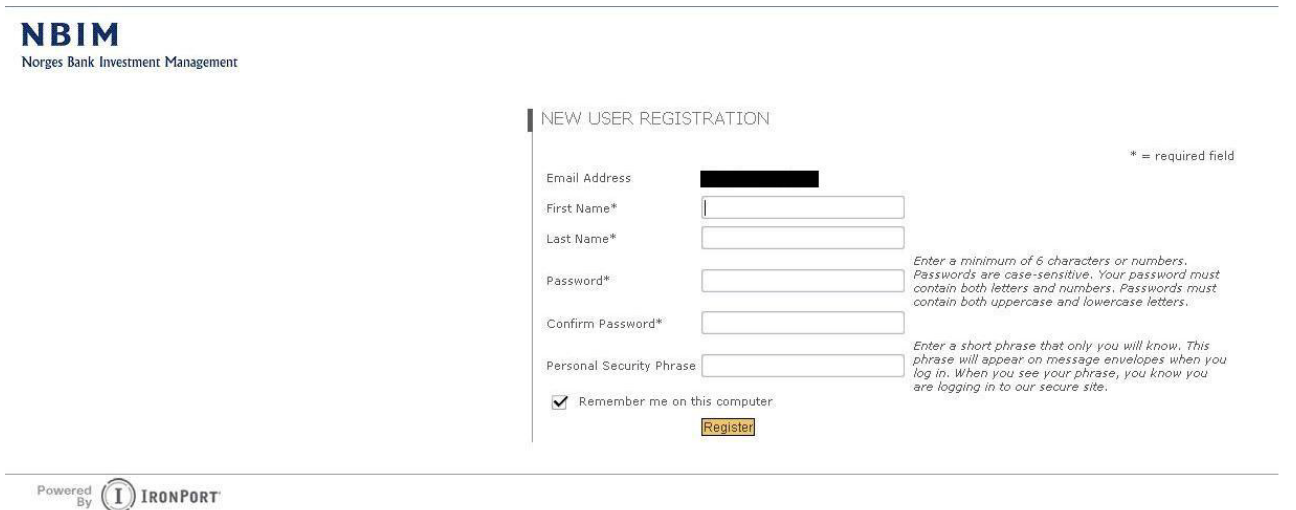
If this is the first time the user receives encrypted e-mail, they will be instructed to register with the system. As soon as the external user registers, he will receive an automated mailer of registration, and can now re-open the encrypted e-mail and log on to decrypt the contents.

THE EXTERNAL USER REGISTERS AT THE SECURE SERVER

When opening the securedoc.html for the first time, the user will get the following screen:



The user must press “Register” to register:



The e-mail address is fixed to the e-mail that received the encrypted message and cannot be changed. The user will have to fill in First and Last name as well as a password which complies with the password policy stated in the registration page.

After registering, the user will be notified he has been successfully registered with Ironport Encryption Appliance.

THE EXTERNAL USERS ACCESSES THE SECURE E-MAIL SERVER AT NBIM

The external user opens the securedoc.htm attachment previously received and is presented with a logon page:

The screenshot shows a web interface for NBIM (Norges Bank Investment Management) with an Ironport Email Encryption logo. The page includes a header with the NBIM logo and name, a date and time stamp (February 4, 2009, 8:20:28 AM CET), and a message security indicator (Message Security: High). The main content area features a logon form with fields for From, To, Subject, and Password. A 'Remember me on this computer' checkbox is present, along with a 'Forgot password?' link. A 'Personal Security Phrase' warning is displayed, stating 'Your personal phrase is not enabled on this machine.' and providing a 'More info' link. An 'OPEN' button is located below the form. At the bottom, there is a footer with the Ironport logo and copyright information (© 2000-2008 Cisco Systems, Inc. All rights reserved.).

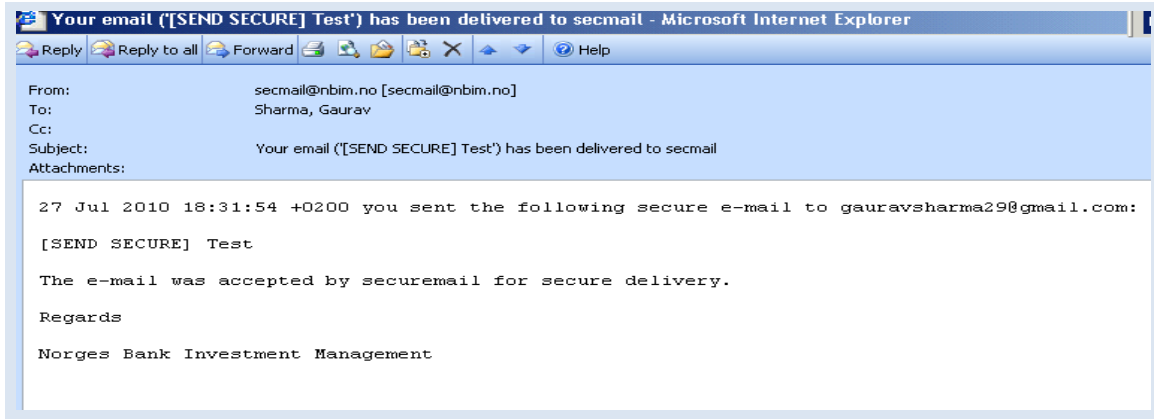
The external user can now log in using the password used during registration.

The e-mail is presented to the external user. The external user can reply to the e-mail in the same GUI if needed. The reply is sent back to NBIM.

Note: - A secured copy of the same replied email is sent to external user for his own future reference.

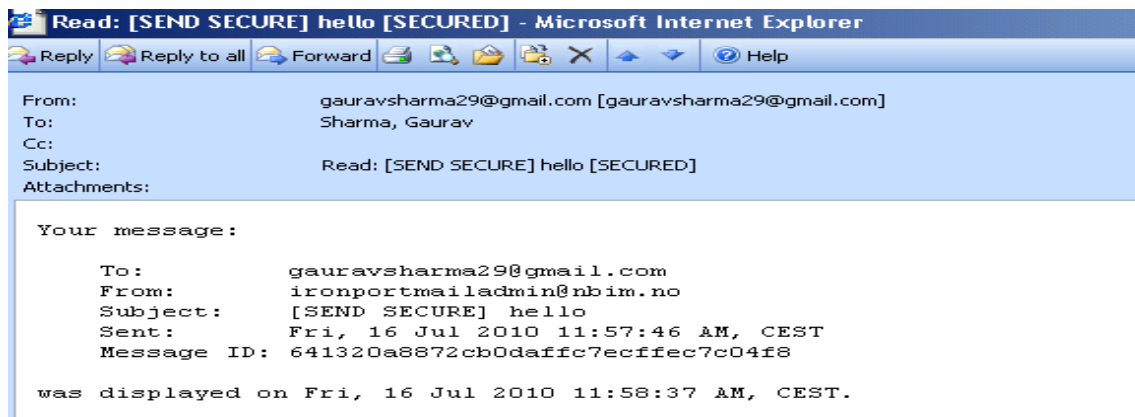
THE NBIM USER GETS A RECEIPT WHEN THE MAIL IS RECEIVED BY THE SYSTEM

When the mail is received by the secure email system, the user will get a confirmation:



THE NBIM USER GETS A RECEIPT WHEN THE MAIL IS READ BY THE EXTERNAL USER

When the mail is opened by the external user, the sender will get a receipt:



SECURE MAILS FROM THE EXTERNAL USERS

External Users should use <https://securemail.nbim.no> to send encrypted messages to NBIM Users.

Note: - A secured copy of the same replied email is sent to external user for his own future reference.



The screenshot displays the NBIM webmail interface. At the top left is the NBIM logo and 'Norges Bank Investment Management'. At the top right is a 'Welcome' message. A left sidebar contains navigation options: 'Manage Messages', 'Compose Message' (highlighted), and 'Edit Profile'. The main area is titled 'COMPOSE MESSAGE' and features a 'Send' button. The form includes fields for 'To:', 'CC:', 'BCC:', and 'Subject:'. Below these is an 'Attachments' section showing '(none)'. A note states: 'To add or remove attachments, click on Attachments. In the popup window, select the file(s) to attach or select and remove attachments you have already added.' A large text area for the message body is at the bottom.

ERROR HANDLING

There should be no specific errors. The standard e-mail interface will have help information to cover standard procedures like forgotten passwords etc.

REQUIREMENT AT USER END

- User's machine should be installed with the most current version of Java
- Java scripting should be enabled in Internet Advance Options in the control panel.
- User's machine should be connected with Internet.

NBIM POLICY FOR EMAIL COMMUNICATION

- a) Maximum Message size for incoming emails is 25 MB
- b) Maximum Message Size for outbound emails is 25 MB
- c) The Blocked attachments in Inbound as well as Outbound Email are as follows :-

pif|scr|386|ade|adp|bas|bat|chm|cmd|cpl|crt|drv|hlp|hta|inf|ini|ins|isp|js|jse|mde|mp3|mp3|msc
|msp|mst|pcd|reg|sct|shb|shs|sys|vb|vbe|vbs|wsc|wsf|wsh|qt|mp5|mp2|mpa|css|nws|zib|clp|
pcl|exe|java|msi|pif|dll|scr|com.

- d) No other form of Encryption such as PGP is allowed either from NBIM to Internet or from Internet to NBIM.
- e) No password protected attachments are allowed either from NBIM to internet or Internet to NBIM.
- f) If you believe the communication is critical to NBIM's business, you could request for adding your email address into "whitelist". Request could be sent to helpdesk@nbim.no

SERVICES AND SUPPORT

- a. All incidents may be reported to NBIM Helpdesk via Footprints or by calling Helpdesk at +47 2407 3333
- b. A USD Ticket can be opened for any issue related to secure mail / Simple email communication between the Internet and NBIM. The USD queue for CSC is : - [CSC.All.Eur.Dces.Msg.Svcs](#)

FAQ

Q. Do I still need to password protect my document while sending secure mail?

A. No. The Secure mail system is solely responsible and capable for the data protection. All such emails will be blocked. However NBIM user shall be notified.

Q. Does my external partners need to send password protected attachments?

A. No, when they reply to NBIM user's email by logging onto web portal, the email is delivered in a secure environment of NBIM. All such emails will be blocked. However NBIM user shall be notified.

Q. I am still using PGP encryption to encrypt emails, will it work?

A. No other form of encryption is allowed in NBIM except Ironport secure mail. All such emails will be blocked. However NBIM user shall be notified.

Q. Can my external email partner use any form of encryption?

A. No other form of encryption is allowed in NBIM except Ironport securemail. All such emails will be blocked. However NBIM user shall be notified.