Automatic encryption of outgoing emails with S/MIME

iQ.Suite Tips & Tricks for IBM Domino

If required, all the emails destined for the Internet can be automatically encrypted, provided the recipient has a public S/Mime certificate. The way to do this is to set up a group which lists all the email recipients with a public certificate.

The alternative option is to query the certificate database, as described here:

Step by step:

iQ.Suite Address Rule

<table>
<thead>
<tr>
<th>Basics</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>S-Mime Certificate Available</td>
</tr>
<tr>
<td>Status</td>
<td>Active  Not active</td>
</tr>
<tr>
<td>Log level</td>
<td>Loglevel 0 (value from NOTES.IN)</td>
</tr>
<tr>
<td>Execution mode</td>
<td>Dependent on job or global parameter</td>
</tr>
<tr>
<td>Sender</td>
<td>All</td>
</tr>
</tbody>
</table>

Recipients By database
Recipient condition at least one included
Resolve groups for address filtering Yes No
Resolve forward addresses only Yes No
Database iQSuiteig_cert.nsf
View CertificatesInternetadress

The certificate database (default is g_cert.nsf in the iQ.Suite data directory)

The information must be entered relative to the Domino data directory. The view "CertificatesInternetadress" contains all the active S/Mime certificates sorted by Internet address.

Crypt Mail Job
Select the rule created above (you can add your own rules if you need to).

'SGroup - Auto S/MIME Encrypt'  

CRYPT MAIL JOB

**Basics | Operations | Advanced | Misc. | Comments**

**Basics**
- **Job name**: Group - S/MIME Encrypt
- **Status**: Active
- **Priority**: 2
- **Runs on**: All mails
- **Attachment dependency**: All
- **Controls for rules**: Select, Deselect all, Edit, New
- **Positive selection rule dependency**: All true
- **Negated selection rule dependency**: All false
- **Rule summary**: (S-Mime Certificate Available)
- **Rule execution mode**: Set in global parameter
- **Upon error in rule evaluation**: Do not run job
- **Runs in a replicated environment**: on all servers

**Operations**
- **Mode**: S/MIME encryption
- **On Error**: Stop mail, Notify administrator, Notify sender
- **Category in Quarantine report**: Crypt
- **Crypt Engine**: SMIME Engine

**Settings**
- **Person / key combinations**: 
- **Notification**: 
- **Subject upon success**: Encrypted automatically
- **Notifications upon system errors**: Admin: S/MIME encryption error
If you want the email to be sent even if the active public certificate does not have "Trusted" status, you need to deactivate the following fields:

- On Error – Stop Mail
- On Error – Notify Sender

Also, the "Subject upon success" field should be EMPTY, so that the recipient does not incorrectly receive the message that the email has been encrypted.

From now on, all the emails sent to recipients with an active S/Mime certificate will be encrypted.

**Note:** As already mentioned, all the active S/Mime certificates are used, irrespective of other statuses or validity.