ID Control

ID Control MailID

with integrated MessageID

Trademarks
ID Control Authentication Server, MailID, HandyID, KeystrokeID, MessageID, RiskID, ID Control OTP Key are trademarks of ID Control BV. All other brand names and product names are trademarks or registered trademarks of their respective owners.

Licence Conditions
Please read your licence agreement with ID Control carefully and make sure you understand the exact terms of usage.

Disclaimer
This document is provided “as is” without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the document. ID Control BV may make improvements of and/or changes to the product described in this document at any time.

Contact
If you wish to obtain further information on this product or any other ID Control BV products, you are always welcome to contact us.

ID Control BV
Van Diemenstraat 202
2518 VH DEN HAAG
The Netherlands

Tel: +31-888-SECURE (732873)
www.idcontrol.com
support@idcontrol.com

Table of Contents

Introduction

MailID email encryption server is an email gateway (MTA) that encrypts and decrypts your incoming and outgoing email. Because MailID serves as a general SMTP email server, it is compatible with any existing email infrastructure and can easily be placed before or after existing email servers. MailID is typically installed as a “store and forward” server. Email is therefore only temporarily stored until it is forwarded to it's final destination.

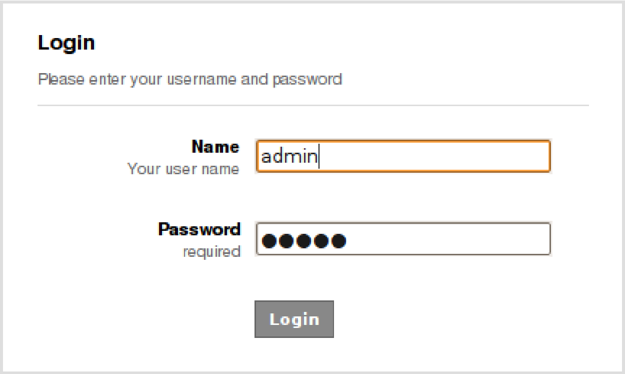
MailID currently supports two encryption standards; S/MIME and PDF encryption. S/MIME provides authentication, message integrity and non-repudiation (using X.509 certificates) and protection against message interception (using encryption). S/MIME uses public key encryption (PKI) for encryption and signing. PDF encryption can be used as a light-weight alternative to S/MIME encryption. PDF allows you to decrypt and read encrypted PDF documents. PDF documents can even contain attachments embedded within the encrypted PDF. The password for the PDF can be manually set per recipient or a password can be randomly generated and sent to the recipient via SMS.

Setup

We assume that MailID has already been installed and that the user can login to the admin pages. For installation instructions of MailID see the installation guide.

You can login to the administration page by opening a URL similar to:

https://192.168.1.1:8443[1] (the IP address is probably different in your situation)



Login

Please enter your username and password

Name: admin
Your user name

Password: ●●●●●
required

Figure 1: Login page

A login page should appear (see Figure 1: Login page).

Login with following credentials name: admin, password: admin

[1] If you are using the MailID virtual appliance you can also access the administration page on the default https port.

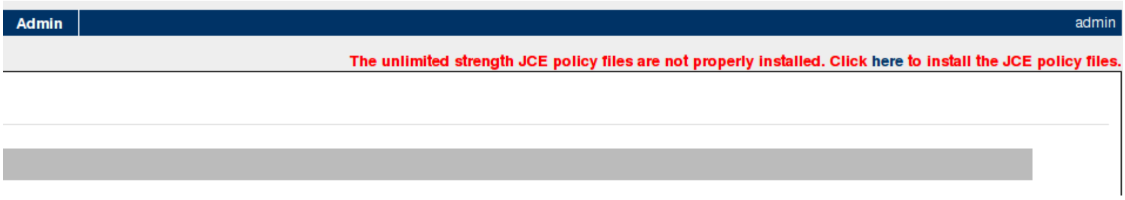
The first time someone logs into the system it will take some time before the main page is shown (the system needs to initialize itself)[2]. After a successful login you will be redirected to the user page.

Unlimited Strength Jurisdiction Policy Files

Due to import control restrictions by the governments of a few countries, the jurisdiction policy files shipped with Java SE from Sun Microsystems specify that "strong" but limited cryptography may be used. An "unlimited strength" version of these files indicating no restrictions on cryptographic strengths is available for those living in eligible countries (which is most countries). MailID checks if the "unlimited strength jurisdiction policy files" are installed and if not, a warning is given (see Figure 2: Limited encryption strength warning).

NOTE THAT EXPORT/IMPORT AND/OR USE OF STRONG CRYPTOGRAPHY SOFTWARE IS ILLEGAL IN SOME PARTS OF THE WORLD. IT'S YOUR RESPONSIBILITY TO MAKE SURE YOU ARE ALLOWED TO USE STRONG CRYPTOGRAPHY. THE AUTHORS OF MAILID ARE NOT RESPONSIBLE FOR ANY VIOLATIONS YOU MAKE.

In order to remove this restriction the "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files" must be downloaded from SUN's website[3] and installed into Java. You can use the MailID web admin "JCE policy manager" page to install the downloaded file. The "JCE policy manager" page can be opened by either clicking on the warning link (see Figure 2: Limited encryption strength warning) or by selecting the Admin menu and then selecting "JCE policy".



The unlimited strength JCE policy files are not properly installed. Click here to install the JCE policy files.

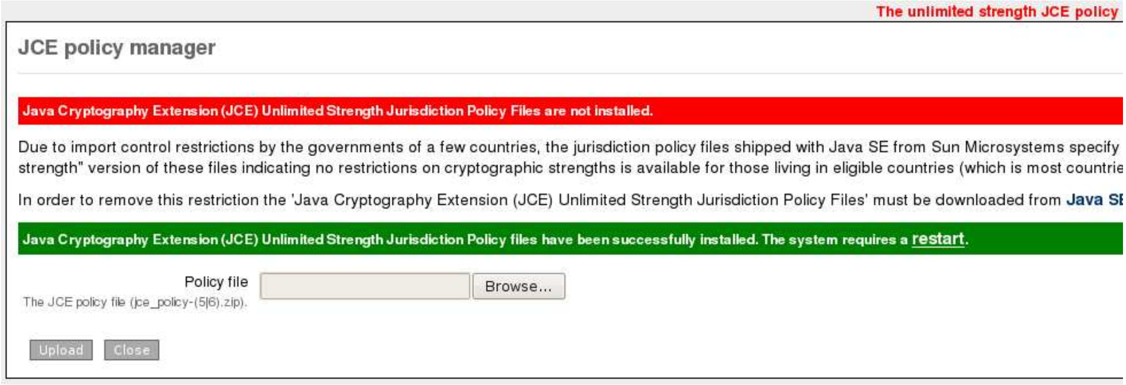
Figure 2: Limited encryption strength warning

It should be noted that MailID requires unlimited strength encryption to be enabled.

JCE policy manager

[2] Java uses a JIT compiler which takes some time to optimize.

[3] http://java.sun.com/javase/downloads/index.jsp and go to "other download".



The unlimited strength JCE policy

JCE policy manager

Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files are not installed.

Due to import control restrictions by the governments of a few countries, the jurisdiction policy files shipped with Java SE from Sun Microsystems specify strength" version of these files indicating no restrictions on cryptographic strengths is available for those living in eligible countries (which is most countrie

In order to remove this restriction the 'Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files' must be downloaded from **Java SE**

Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy files have been successfully installed. The system requires a restart.

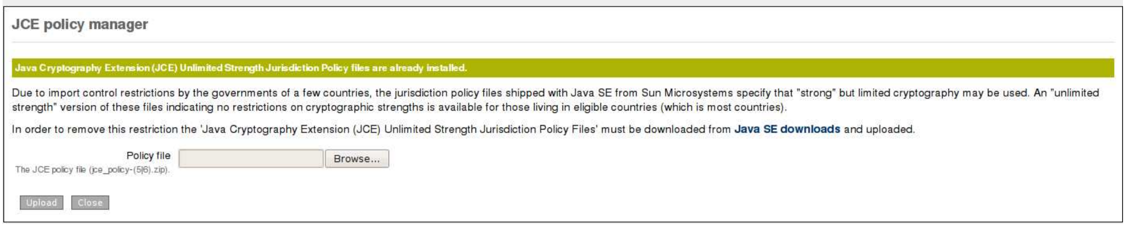
Policy file
The JCE policy file (jce_policy-(5|6).zip).

Figure 4: JCE policy files uploaded

You can use the JCE policy manager to install the “Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files”. If the unlimited strength policy files are not yet installed a warning will be shown (see Figure 3: JCEL policy manager). To install the downloaded policy file you should select the file (“jce_policy-6.zip”) and click the upload button. After the file has been successfully uploaded a message will be shown that the system should be restarted[4] (see Figure 4: JCE policy files uploaded).

The system can be restarted by clicking “restart” (restarting takes about 30 seconds). The system can also be restarted by opening the “Admin” page and click “Restart” on the left-side menu. If you are using MailID Virtual Appliance you can restart by selecting “Restart services” in the virtual appliance console.

After the restart the “Unlimited strength..” warning should no longer be shown. If you open the “JCE policy manager” page again a message should be shown that the policy files are already installed (see Figure 5: JCE policy files already installed).



JCE policy manager

Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy files are already installed.

Due to import control restrictions by the governments of a few countries, the jurisdiction policy files shipped with Java SE from Sun Microsystems specify that "strong" but limited cryptography may be used. An "unlimited strength" version of these files indicating no restrictions on cryptographic strengths is available for those living in eligible countries (which is most countries).

In order to remove this restriction the 'Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files' must be downloaded from **Java SE downloads** and uploaded.

Policy file
The JCE policy file (jce_policy-(5|6).zip).

Figure 5: JCE policy files already installed

Note that every time Java is updated you should make sure that the unlimited policy files are properly installed[5].

[4] To be precise, MailID and Jetty have to be restarted to make them use the unlimited strength policy files. When the MailID virtual appliance is used you can use “Other → Restart services...” to restart MailID.

[5] If Java is updated and the JCE policy files are no longer installed after the update a restart will restore the JCE policy files from the backup.

MTA setup

MailID uses Postfix for receiving and sending of email (“Mail Transfer Agent”). Postfix need to be setup in such a way that all incoming email is 'filtered' by the encryption/decryption engine (“Mail Processing Agent”)[6]. MailID contains a “MTA config” page that can be used to configure most of the relevant Postfix parameters. The “MTA config” page can be opened from the Admin menu.

The “MTA config” page (see Figure 6: MTA config) contains most of the relevant Postfix parameters for a “store and forward” email server. Postfix parameters that cannot be set using the “MTA config” page can be set using the “MTA raw config page” (or by directly editing the Postfix configuration files).

We will briefly explain the relevant Postfix settings. For a more thorough explanation of all the Postfix settings see the Postfix documentation.

Relay domains

Relay domains are domains for which you receive email. These are the domains for which your internal users receive email.

Internal relay host A “store and forward” server normally has one or more relay domains (unless MailID is only used for sending email in which case you do not need to specify any relay domains).

My networks

Most email senders (users and other internal email servers) are not allowed to send email to domains not specified in “relay domains”. To allow outgoing email to be sent to external domains the senders IP address has to be “white listed”. The “My networks” list contains all the networks that are allowed to sent email to external domains. The networks must be specified in CIDR notation.

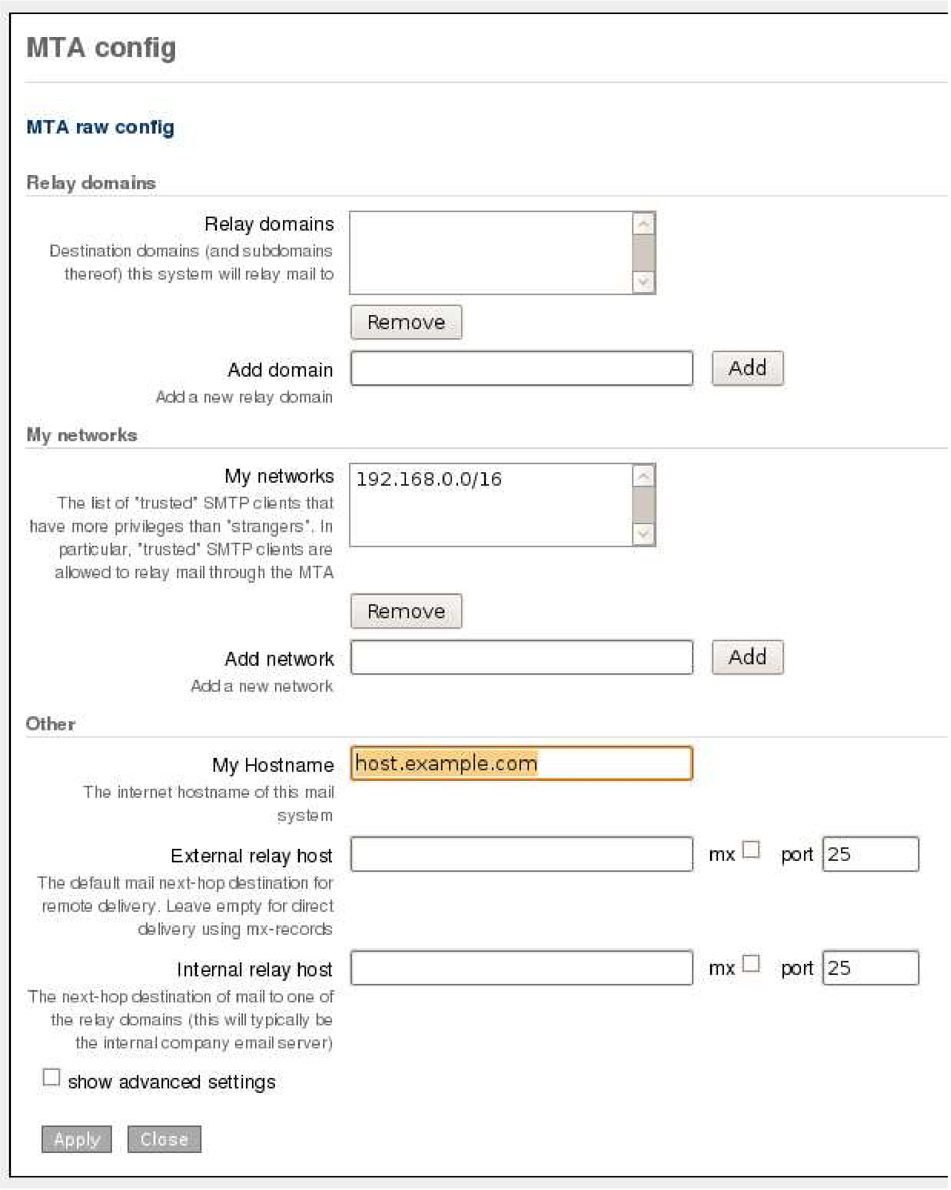
Example: 192.168.1.1/32, 10.1.2.0/24

Note: you should be careful only to allow internal email servers from sending email to external recipients otherwise your server will be used by spammers.

My Hostname This should be the fully qualified domain name of the email server and is used as the default value for many other configuration parameters.

Example: MailID.example.com

[6] For Postfix setup see “installation guide”



MTA config

MTA raw config

Relay domains

Relay domains
Destination domains (and subdomains thereof) this system will relay mail to

Add domain
Add a new relay domain

My networks

My networks: 192.168.0.0/16
The list of "trusted" SMTP clients that have more privileges than "strangers". In particular, "trusted" SMTP clients are allowed to relay mail through the MTA

Add network
Add a new network

Other

My Hostname: host.example.com
The internet hostname of this mail system

External relay host: mx □ port 25
The default mail next-hop destination for remote delivery. Leave empty for direct delivery using mx-records

Internal relay host: mx □ port 25
The next-hop destination of mail to one of the relay domains (this will typically be the internal company email server)

□ show advanced settings

Figure 6: MTA config

External relay host

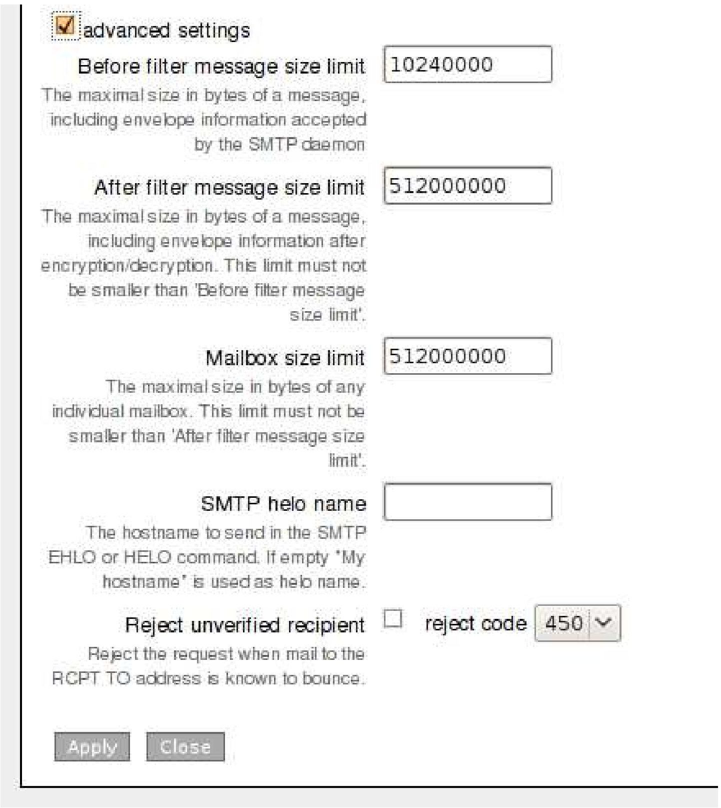
The external relay host is used when email has to be sent to an external domain (i.e. a domain that is not a relay domain). This can be your ISPs email server or some internal email server that is responsible for sending email to external domains. If “External relay host” is not specified email will be delivered using DNS mx-records. “External relay host” can be a IP address or a domain name. If the option “mx” is checked the mx-records of the “External relay host” will be used instead of the A-record (this setting is only used when the “External relay host” is specified). The “port” setting is the port the “External relay host” server listens on (which in most cases should be port 25).

Internal relay host

The internal relay host is used when email has to be sent to an internal domain (i.e. sent to a relay domain). Typically this will be your company or personal internal email server containing the user email boxes. If “Internal relay host” is not specified email will be delivered using DNS mx-records. “Internal relay host” can be a IP address or a domain name. If the option “mx” is checked the mx-records of the “ Internal relay host” will be used instead of the A-record (this setting is only used when the “ Internal relay host” is specified). The port is the port the “ Internal relay host” server listens on (which in most cases should be port 25).

Advanced settings

The advanced settings can be set when the “advanced settings” check-box is selected (see Figure 7: Advanced MTA settings).



☑ advanced settings

Before filter message size limit: 10240000
The maximal size in bytes of a message, including envelope information accepted by the SMTP daemon

After filter message size limit: 512000000
The maximal size in bytes of a message, including envelope information after encryption/decryption. This limit must not be smaller than 'Before filter message size limit'.

Mailbox size limit: 512000000
The maximal size in bytes of any individual mailbox. This limit must not be smaller than 'After filter message size limit'.

SMTP helo name:
The hostname to send in the SMTP EHLO or HELO command. If empty 'My hostname' is used as helo name.

Reject unverified recipient ☐ reject code 450
Reject the request when mail to the RCPT TO address is known to bounce.

Figure 7: Advanced MTA settings

Before filter message size limit

This is the maximum size of a message (in bytes) that the MTA accepts. A message that exceeds the maximum size is rejected by the MTA.

After filter message size limit

The mail processing agent of MailID is responsible for the encryption and decryption of messages. The size of a message after encryption/decryption can be larger than the size of the message before encryption/decryption. The "after filter message size limit" must therefore be larger than the "before filter message size limit". We advise that the "after filter message size limit" should be about 2 times larger than the "before filter message size limit".

Mailbox size limit

If mail is locally stored (only when "Local domains" are specified) the "Mailbox size limit" will be the maximum size (in bytes) of an individual mailbox. The "Mailbox size limit" should not be smaller than the "after filter message size limit". This setting is only required when Postfix receives email for a local domain. By default MailID does not allow you to specify any local domains.

SMTP helo name

The hostname to send in the SMTP EHLO or HELO command. If "SMTP helo name" is not specified "My Hostname" is used. The helo name reported by an email server must be equal to the reverse lookup of the IP address to prevent being filter by spam filters[7].

Reject unverified recipient

Normally an email server should know which recipient email addresses it should accept email for. When the email server is setup to relay email for certain domains **Relay domains**the email server should know which recipients will be accepted by the server it relays to (in other words it should be a smart relay host). If all email is accepted for relay without knowing whether the next email server will accept the email, you run the risk of generating "backscatter email". There are multiple ways for the server to known which recipient addresses are acceptable and which are not. One solution is to let the MailID server "learn" which recipient addresses are acceptable by querying the server it relays to. When an email is received for an unknown user, the server "asks" the server it relays to whether the recipient is a valid recipient or not. If it is a valid recipient it will accept the message, if it's an invalid recipient it will not accept the message. The result of this verification process is cached. By enabling "Reject unverified recipient" you enable this verification procedure. The "reject code" is the SMTP

[7] See http://cbl.abuseat.org/helocheck.html for more information and ways to check this.

result used when the email is not accepted. You should initially set this to 450, which result in a temporary error. Change it into 550 when you are confident that the verification procedure works correctly. See the Postfix documentation for more information on address verification[8]. There are other, and often better ways, for the the email server to know which recipients are valid, like for example using LDAP queries or by specifying relay_recipient_maps. These other options are however not directly supported by the "MTA config" form and should be configured using the "MTA raw config page" or by directly editing the Postfix configuration files.

Applying your settings

When you click the "Apply" button your settings will be checked and Postfix will be configured with the new settings. Clicking the "Close" button will bring you back to the "Admins" page and any changes made after applying the changes will be lost.

MTA raw config

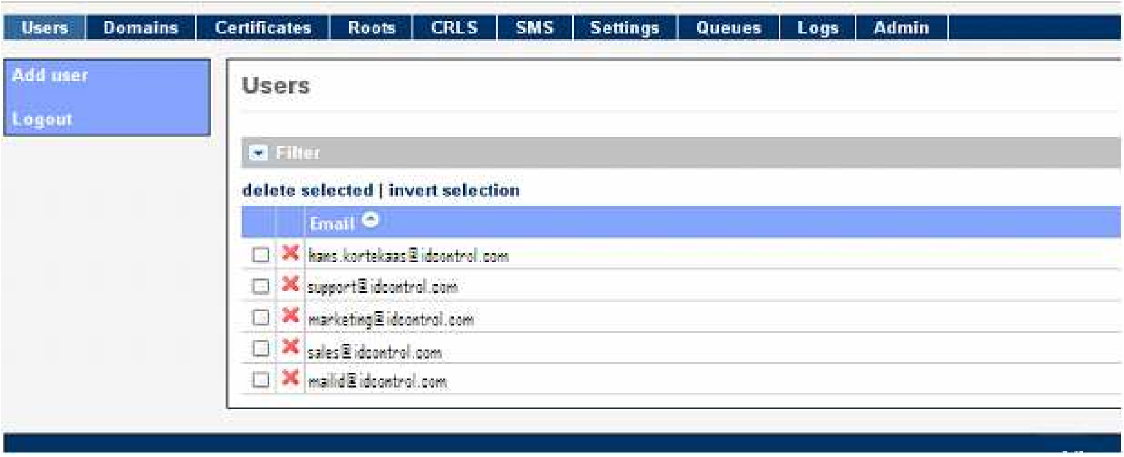
Postfix has a large number of settings. Because the "MTA config" page only supports a small number of these settings you can use the "MTA raw config" page for all other settings[9]. The "MTA raw config" page allows you to directly edit the Postfix main configuration file. MailID does not validate your changes and you should therefore be careful with any changes you make. The configuration file contains some specific MailID settings (the settings that start with MailID_). These settings are modified by the "MTA config" page when you apply your settings. These settings should therefore not be manually changed because they can be overwritten by the "MTA config" page. The MailID specific settings are used by other Postfix settings (they are referenced like ${MailID_*}).

Users

A user is a sender and/or a receiver of an email and is uniquely identified by an email address. Every user has a set of preferences that determine how email is handled for that particular user. The users page gives you an overview of all the users (see Figure 8: Users).

[8] See http://www.postfix.org/ADDRESS_VERIFICATION_README.html

[9] You can only edit settings for the main.cf file. All other settings should be done from the command line.



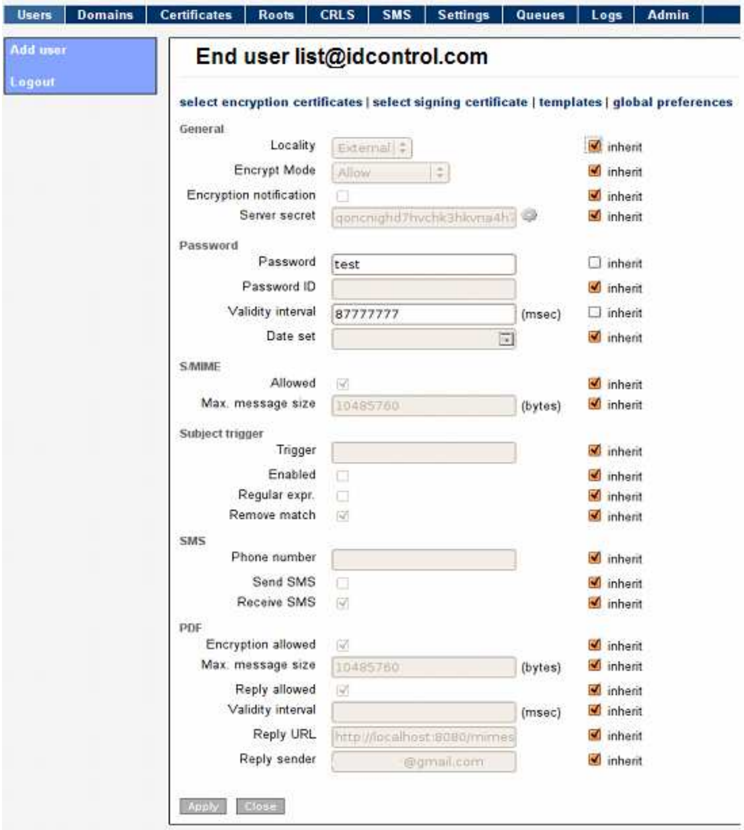
		Email
□	✗	kans.kortekaas@idcontrol.com
□	✗	support@idcontrol.com
□	✗	marketing@idcontrol.com
□	✗	sales@idcontrol.com
□	✗	mailid@idcontrol.com

Figure 8: Users

You can search for specific users with the user filter and remove users by clicking the 'cross' or by selecting users and clicking “delete selected”. New users can be added by clicking “Add user” on the left-hand side menu. Clicking a user opens the user preferences “Edit” page (see next section). Internal users are marked with a green star icon (see Locality property on page 15 for more info on internal and external users). Clicking the user certificate icon opens the certificate selection page for the user. If the user is an internal user the “Select signing certificate” page is opened. If the use is an external user the “Select encryption certificates” page is opened.

User preference

Every user has a set of preferences which determine how email is handled for that particular user. User preferences can inherit some or all of the preferences from higher level preferences. Users inherit from domain preferences, domain preference inherit from the global preferences and the global preferences inherit from factory preferences. The preferences for a user can be edited by clicking on the users email address (see Figure 9: User preferences)


Users
Domains
Certificates
Roots
CRLS
SMS
Settings
Queues
Logs
Admin
Add user
Logout
select encryption certificates | select signing certificate | templates | global preferences
Apply
Close

End user list@idcontrol.com

General			
Locality	External		☑ inherit
Encrypt Mode	Allow		☑ inherit
Encryption notification	□		☑ inherit
Server secret	qoncnighd7hvchk3hkvna4h		☑ inherit
Password			
Password	test		□ inherit
Password ID			☑ inherit
Validity interval	87777777	(msec)	□ inherit
Date set			☑ inherit
S/MIME			
Allowed	☑		☑ inherit
Max. message size	10485760	(bytes)	☑ inherit
Subject trigger			
Trigger			☑ inherit
Enabled	□		☑ inherit
Regular expr.	□		☑ inherit
Remove match	☑		☑ inherit
SMS			
Phone number			☑ inherit
Send SMS	□		☑ inherit
Receive SMS	☑		☑ inherit
PDF			
Encryption allowed	☑		☑ inherit
Max. message size	10485760	(bytes)	☑ inherit
Reply allowed	☑		☑ inherit
Validity interval		(msec)	☑ inherit
Reply URL	http://localhost:8080/mimes		☑ inherit
Reply sender	@gmail.com		☑ inherit

Figure 9: User preferences

Whether a preference is inherited or not is determined by the associated “inherit” check-box. If checked the property is inherited, and if not checked the property is not inherited. Some properties are only relevant for the sender of a message and some properties are only relevant for the receiver of a message. Most properties however are relevant for both sender and receiver. How and when the properties are exactly used can be seen in Appendix B (Mail flow).

The sender of a message is identified by the from header (and not the envelope sender) whereas the recipient is identified by the recipient of the SMTP envelopeThe preference inheritance diagram is as follows:

user ← domain ← wildcard[10] domain ← global ← factory

(where ← means inherits from)

You can use the "Edit user preference" page to set the preferences for a specific user. The page sub-menu ("select encryption certificates", "select signing certificate", "templates" and "global preferences") can be used to set additional preferences.

We will now give a brief explanation of the user preferences.

General

LocalityThe "locality" of a user can be external or internal. The "locality" preference is a very important preference because it determines whether mail coming into MailID should be encrypted or decrypted. If the recipient of an email is an internal user the email should be decrypted (if the message is encrypted and a suitable decryption key can be found). If the recipient of an email is an external user the message should be encrypted (whether the message will actually be encrypted depends on the user settings and/or whether a suitable encryption certificate for the recipient is available). Typically users for which you receive email will be internal users and all other users will be external users. The domain of a recipient is based on the SMTP envelope recipient. The domain of the sender is based on the "From" header[11].

Note: because the locality is such an important preference you should make sure that it's correctly setup. In most installations you should make all domains for which you receive email (the relay domains) "internal" domains. By default all users and domains are external.

Encrypt Mode

Encrypt mode determines whether a message sent to an external user (external locality) should be encrypted or not. You can choose between "No Encryption", "Allow", "Mandatory" and "Force". Encrypt mode is used for sender and receiver. If the encrypt mode is "No encryption" the message will not be encrypted by default (unless being overruled by the "subject trigger"). If mode is "Allow" the message is only encrypted if it is possible to encrypt the message (i.e. a valid recipient certificate is available, a PDF password is set or the recipient has a phone number set for SMS). With "Mandatory" mode the message must be encrypted and if it is not possible to encrypt the message the message will not be sent and the sender will be notified that the message has not been sent. The encrypt mode is a sender and receiver setting. This means that the settings for both the sender receiver must allow encryption. If for example the sender has

[10] An example of a wildcard domain is *.example which matches test.example.com.

[11] If there is no "From" header the "Sender" header will be used. If the "Sender" header is also missing the envelope sender will be used.

encrypt mode “Mandatory” but the recipient has encrypt mode “No Encryption” the message will not be encrypted and will therefore not be sent (because the sender encrypt mode was “Mandatory”). If the sender (or recipient) has encrypt mode “Force” the other encrypt mode is ignored and encryption is forced. “Force” encrypt mode is for example used when you want to make sure that all email sent to an external recipient is always encrypted[12].

Encryption notification

If set, the sender of the message will be notified (with an email) when the message is encrypted (see template “successful encryption” for the notification message).

Password

Password

The password for this user. Currently this is only used for PDF encryption. The password can be set by the administrator or it can be randomly generated by the system. If the current password has expired (see "Validity interval") a new password is generated. If you want to use a static password make sure you disable password expiration.

MessageID

When the one time password is randomly generated the one time password can be sent to the recipient using an SMS message. The recipient has to know which password should be used for which encrypted PDF. When a new password is generated a unique MessageID is generated as well.

Validity interval

The time (in minutes) the password is valid. If the password is no longer valid (expired) a new password will be generated. If the “Validity interval” is 0 a new password will be generated every time a message is PDF encrypted. If “Validity interval” is -1 the password never expires.

S/MIME

Allowed

If selected digital signing and encryption using S/MIME is allowed.

Auto select certificates

[12] You should select “Force” for the email address of the external recipient.

If checked encryption certificates will be automatically selected for this recipient (see Select encryption certificates).

Only sign when encrypt

If checked messages will only be digitally signed when they are S/MIME encrypted. If not checked, all messages will be digitally signed. The sender of the message must have a valid signing certificate to digitally sign a message.

Max. message size

If the email message is larger than the specified max. message size the message will not be S/MIME signed or encrypted. Large S/MIME messages can sometimes not be read by S/MIME capable email clients. Also encrypting and signing of large email messages can be resource intensive.

Subject trigger

A subject trigger can be used to "tell" the system that the sender wants to encrypt the message. This is useful when the default setting for a sender is "No encryption" or "Allow".

Trigger

If the subject contains the provided trigger message and the subject trigger is enabled encryption is forced for this message. If the message is really encrypted depends on the availability of certificates etc. If encryption is triggered but the message cannot be encrypted the message will not be sent and the sender will be notified.

Enabled

If checked the trigger functionality is disabled.

Regular expr.

If checked the trigger is interpreted as a regular expression and the subject is matched against the this regular expression.

Example regular expression trigger:

(?i)(\[secure\]|\[encrypt\])

This subject trigger will force encryption when the subject contains [secure] or [encrypt]. (?i) makes the check case insensitive.

Remove match

If checked the matching part will be removed from the subject.

Example:

Suppose the trigger equals "[encrypt]"

and the subject of the incoming message is ”your bank statement [encrypt]” the subject after encryption is ”your bank statement”.

SMS

Phone number

The phone number of the recipient to which SMS Text messages will be sent. Passwords for an encrypted PDF or passwords for encrypted private certificates can be sent via SMS Text messages. The phone number must be in international format (i.e. including the country code).

Send SMS

If checked the sender of the message is allowed to send SMS Text messages.

Receive SMS

If checked the recipient of the message is allowed to receive SMS Text messages.

PDF

Encryption allowed

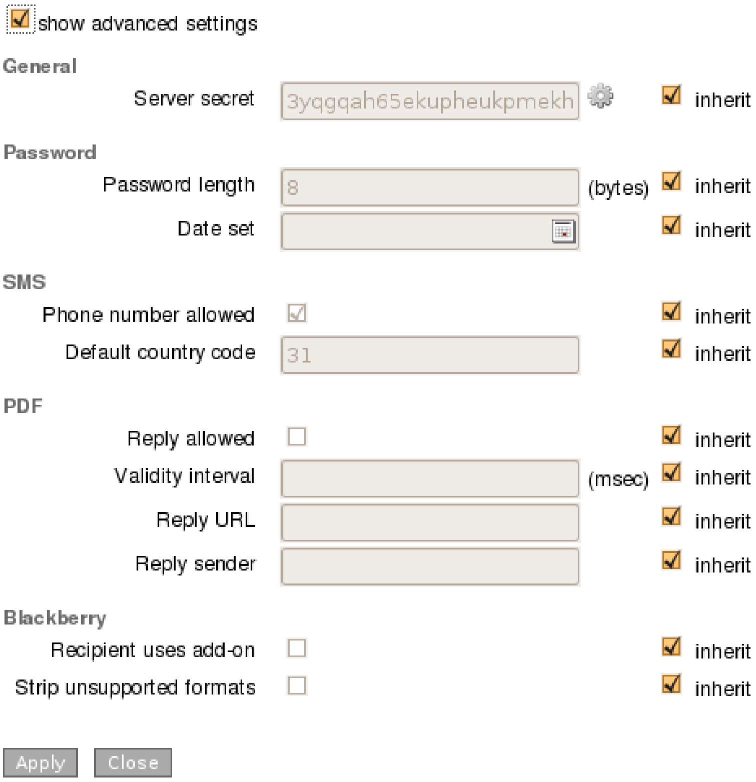
If checked PDF encryption is allowed.

max. message size

If the email message is larger than the specified max. message size the message will not be PDF encrypted. PDF encryption not only encrypts the message body but also encrypts all the message attachments. To prevent your PDF from becoming too large messages with large attachments, which in total exceeds the maximum message size, won't be PDF encrypted.

Advanced settings

The advanced settings sub-page contain settings which are only used in specialized setups.



☑ show advanced settings

General

Server secret 3yqgqah65ekupheukpmekh ☑ inherit

Password

Password length 8 (bytes) ☑ inherit

Date set ☑ inherit

SMS

Phone number allowed ☑ ☑ inherit

Default country code 31 ☑ inherit

PDF

Reply allowed □ ☑ inherit

Validity interval (msec) ☑ inherit

Reply URL ☑ inherit

Reply sender ☑ inherit

Blackberry

Recipient uses add-on □ ☑ inherit

Strip unsupported formats □ ☑ inherit

Figure 10: Advanced settings

General

Server secret

The server secret is used to protect external resources against tampering (using HMAC). For example the reply link in an encrypted PDF message is protected to make sure that a recipient can only reply to a message that was generated by the server. You can generate a secure random secret by clicking the icon next to the input box. In most cases it's best to generate a secret for the global preferences and inherit this secret for all other users and domains. Currently the server secret is only used for the PDF reply functionality. See the PDF encryption guide for more information.

Password

Password length

The length (in bytes) of the randomly generated passwords. This is used when a new password for PDF encryption is automatically generated.

Date set

The date at which the password was set. This is used in combination with the “validity interval” to determine whether the password is still valid. If “Date set” is empty the password will never expire.

SMS

Phone number allowed

If checked, senders are allowed to specify a telephone phone number on the subject. This telephone number is used by the PDF encryption functionality to sent the password via SMS Text message. The telephone number is only used when the subject trigger is specified (see "Subject trigger" setting above) and when the telephone number is at the end of the subject. The telephone number may start with a + and contain spaces, and the following characters (quotes excluded) "-()".

Examples:

Suppose that the subject trigger is [encrypt]. The following subject lines contain valid phone numbers:

This is a subject with a phone number [encrypt] +31123456

Another example [encrypt] +31-(123)456

The following subjects do not contain a valid telephone number:

This is a subject with an invalid phone number [encrypt] 31=456

Another example with an invalid phone number +31123456 [encrypt]

It should be noted that only one recipient is supported when the telephone number is in the subject. With multiple recipients it would be impossible to match the recipient with the correct telephone number. If the message has more than one recipient the message will not be sent and the sender will be notified.

Default country code

The telephone number in the subject should be in international format (i.e. including the country code) to make sure it's sent to the correct recipient. If the telephone number starts with a zero (0), which is not a country code, the server will add the default country code to the telephone number to make it a complete international telephone number. The "default country code" is only used with the phone number by the subject. It is not used with the telephone phone that has been set with the administration page (see setting above) because it must always be set in international format.

PDF

Reply allowed

If checked the encrypted PDF will contain a “Reply” link which can be used by the recipient to securely reply to the message.

Validity interval

When set the “Validity interval” determines how long (in milliseconds) a reply link is valid.

Reply URL

If you want to support replying from an encrypted PDF you should specify the URL of the reply service. By default this should be a URL similar to: https://192.168.1.1:8443/external/pdf/reply/ (the IP address should be different in your situation).

Reply sender

If the recipient replies to an encrypted PDF, by clicking the reply link in the PDF, the sender of the reply will be set to “Reply sender”. This allows you to enable encryption for the “Reply sender”.

See the PDF encryption guide for more information on how to setup PDF encryption.

Blackberry

Recipient uses add-on

If the recipient has installed the MailID Blackberry add-on and wants to receive S/MIME encrypted email on a Blackberry this option should be checked.

Strip unsupported formats

The MailID Blackberry add-on only supports some attachment and message types. When "Strip unsupported formats" is enabled unknown attachments and message types are removed from the message before encrypting the message. The Blackberry add-on does not support HTML email. HTML only email is converted to text before being encrypted. This setting is only valid when the above "recipient uses add-on" setting is enabled. For more information about the MailID Blackberry add-on see the additional guide.

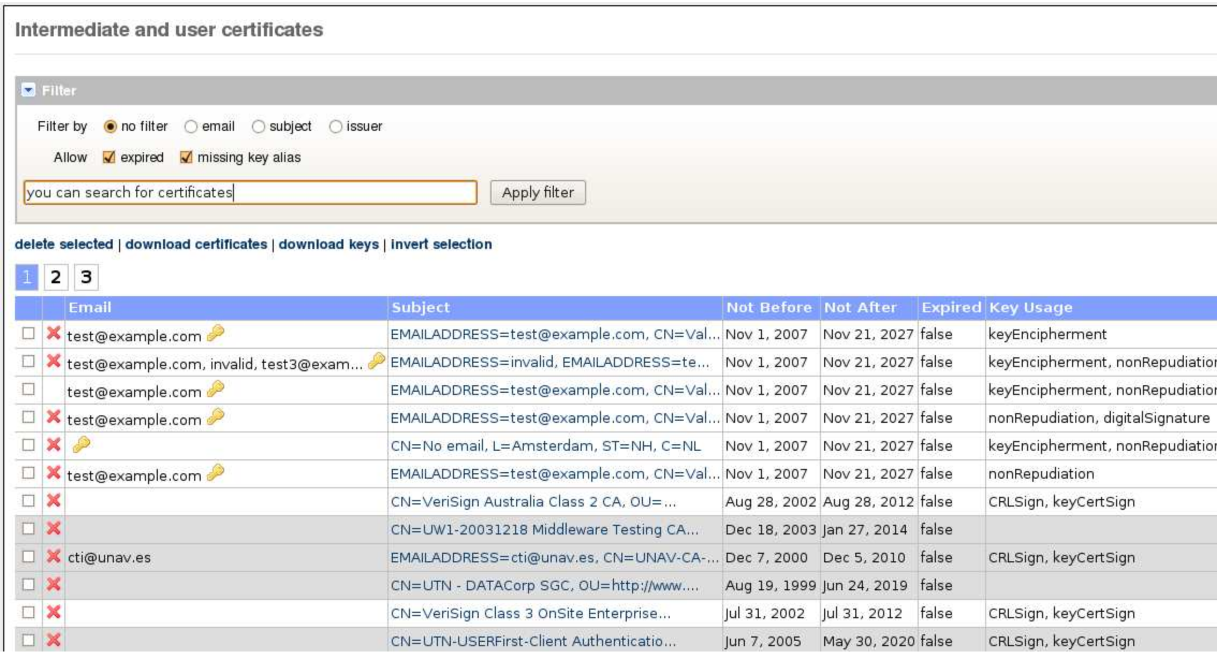
User preference sub-menu

The user preference sub-menus “select encryption certificates”, “select signing certificate”, “templates” will be explained in later paragraphs.

Certificates

MailID supports S/MIME for encryption and digital signing of email messages.

S/MIME is PKI based and uses X.509 certificates[13]. The system has a built in X.509 certificate store. Certificates can be manually added and removed by the administrator. The certificate store supports unlimited number of certificates[14]. Intermediate and end-entity certificates are stored in the "Certificates" store and root certificates are stored in the "Roots" certificate store. The Certificates page gives you an overview of all the certificates in the "Certificates" store (see Figure 11: Certificates store).



Intermediate and user certificates

Filter

Filter by ● no filter ○ email ○ subject ○ issuer

Allow ☑ expired ☑ missing key alias

you can search for certificates | Apply filter

delete selected | download certificates | download keys | invert selection

1 2 3

		Email	Subject	Not Before	Not After	Expired	Key Usage
□	✗	test@example.com 🔑	EMAILADDRESS=test@example.com, CN=Val...	Nov 1, 2007	Nov 21, 2027	false	keyEncipherment
□	✗	test@example.com, invalid, test3@exam... 🔑	EMAILADDRESS=invalid, EMAILADDRESS=te...	Nov 1, 2007	Nov 21, 2027	false	keyEncipherment, nonRepudiatio
□		test@example.com 🔑	EMAILADDRESS=test@example.com, CN=Val...	Nov 1, 2007	Nov 21, 2027	false	keyEncipherment, nonRepudiatio
□	✗	test@example.com 🔑	EMAILADDRESS=test@example.com, CN=Val...	Nov 1, 2007	Nov 21, 2027	false	nonRepudiation, digitalSignature
□	✗	🔑	CN=No email, L=Amsterdam, ST=NH, C=NL	Nov 1, 2007	Nov 21, 2027	false	keyEncipherment, nonRepudiatio
□	✗	test@example.com 🔑	EMAILADDRESS=test@example.com, CN=Val...	Nov 1, 2007	Nov 21, 2027	false	nonRepudiation
□	✗		CN=VeriSign Australia Class 2 CA, OU=...	Aug 28, 2002	Aug 28, 2012	false	CRLSign, keyCertSign
□	✗		CN=UW1-20031218 Middleware Testing CA...	Dec 18, 2003	Jan 27, 2014	false	
□	✗	cti@unav.es	EMAILADDRESS=cti@unav.es, CN=UNAV-CA-...	Dec 7, 2000	Dec 5, 2010	false	CRLSign, keyCertSign
□	✗		CN=UTN - DATACorp SGC, OU=http://www....	Aug 19, 1999	Jun 24, 2019	false	
□	✗		CN=VeriSign Class 3 OnSite Enterprise...	Jul 31, 2002	Jul 31, 2012	false	CRLSign, keyCertSign
□	✗		CN=UTN-USERFirst-Client Authenticatio...	Jun 7, 2005	May 30, 2020	false	CRLSign, keyCertSign

Figure 11: Certificates store

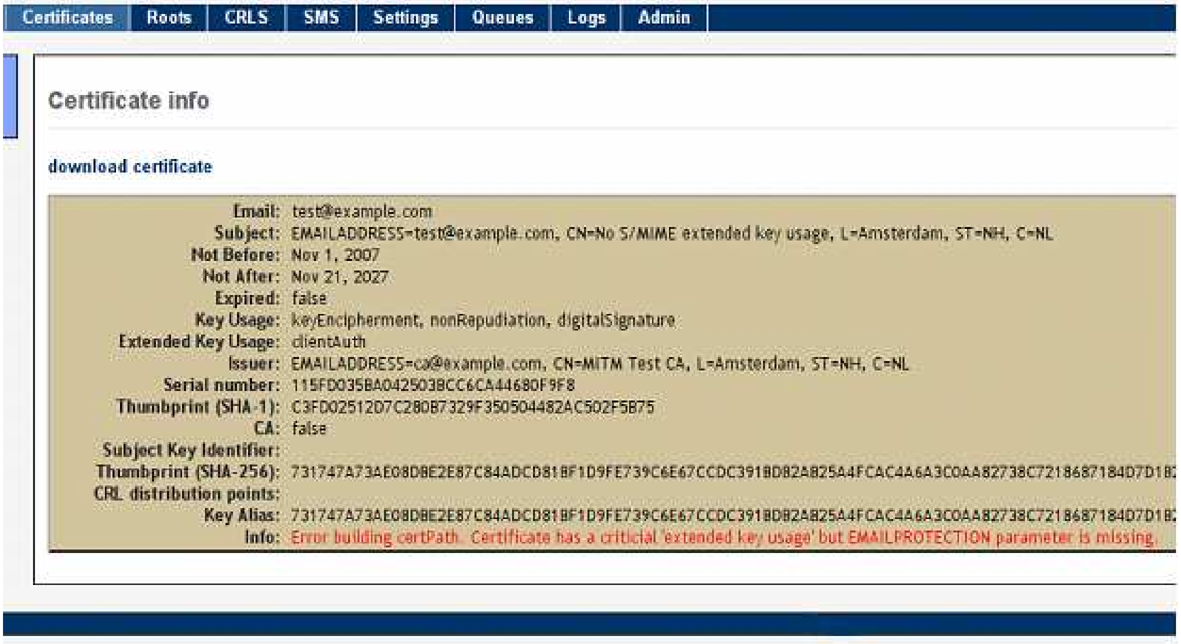
You can filter on certificate contents using the filter editor. Certificates which are not fully trusted (not signed by a trusted root, revoked, expired etc.) are shown in a gray color. Certificates with an associated private key are shown with a "key" icon. Certificates which are revoked are shown in red.

MailID follows RFC 3280 ("Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile").

Selected certificates can be downloaded or deleted. When a certificate is in use (by a user, domain or global settings) the certificate cannot be deleted (indicated by a missing 'red cross'). You can view the certificate details by clicking on the certificate subject (see Figure 12: Certificate details). By clicking the "usage" sub-menu item you can check which users and/or domains are using the certificate.

[13] For more info on S/MIME and X.509 see http://en.wikipedia.org/wiki/Smime and http://en.wikipedia.org/wiki/X.509

[14] Limited by the size of the database. If a HSM is used the HSM can impose a limit on the number of certificates.



Certificate info

download certificate

Email:	test@example.com
Subject:	EMAILADDRESS=test@example.com, CN=No S/MIME extended key usage, L=Amsterdam, ST=NH, C=NL
Not Before:	Nov 1, 2007
Not After:	Nov 21, 2027
Expired:	false
Key Usage:	keyEncipherment, nonRepudiation, digitalSignature
Extended Key Usage:	clientAuth
Issuer:	EMAILADDRESS=ca@example.com, CN=MITM Test CA, L=Amsterdam, ST=NH, C=NL
Serial number:	115FD035BA042503BCC6CA44680F9F8
Thumbprint (SHA-1):	C3FD02512D7C280B7329F350504482AC502F5B75
CA:	false
Subject Key Identifier:	
Thumbprint (SHA-256):	731747A73AE08D8E2E87C84ADCD81BF1D9FE739C6E67CCDC3918D82A825A4FCAC4A6A3C0AA82738C7218687184D7D18
CRL distribution points:	
Key Alias:	731747A73AE08D8E2E87C84ADCD81BF1D9FE739C6E67CCDC3918D82A825A4FCAC4A6A3C0AA82738C7218687184D7D18
Info:	Error building certPath. Certificate has a criticial 'extended key usage' but EMAILPROTECTION parameter is missing.

Figure 12: Certificate details

You can use the certificate details page for more info as to why a certificate is not trusted. For example, in Figure 12: Certificate details you can see that the certificate is not trusted because the certificate is not trusted by a root certificate (the certificate chain is incomplete).

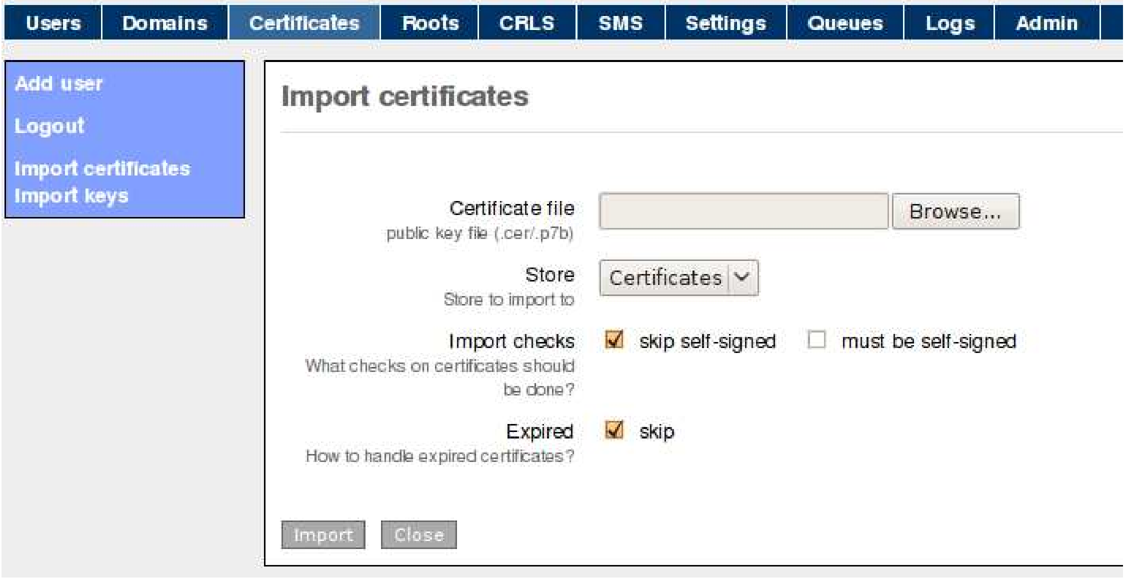
The “Certificates” store can also contain private keys associated with a X.509 certificate. Private keys can be used for the decryption of S/MIME encrypted messages or for digitally signing messages. An entry with an associated private key has a non-empty “Key alias” (see for example Figure 12: Certificate details). If you only want to see all entries with an associated private key entry you can uncheck the allow “missing key alias” check-box.

The “Roots” store contains certificates that MailID trusts. Root certificates are certificates that are “ultimately” trusted. The “Roots” store normally only contains certificates (“Key alias” is always empty).

Certificates can be manually imported by the administrator. Certificates can also be added to the certificate store when an incoming S/MIME protected email has attached certificates. Any attached certificates are extracted from the message and stored in the certificates store. Most S/MIME signed messages have the signing certificate attached to the signed message.

Importing certificates

Certificates can be imported into a store using the “Import certificates” page (see Figure 13: Import certificates). You should select a certificate file, select the store to import to, select additional import parameters and import the certificate. Files with just one certificate (DER or PEM encoded) and files with multiple certificates (.p7b) are supported. Importing a large number of certificates can take some time.



Import certificates

Certificate file
public key file (.cer/.p7b)

Store
Store to import to: Certificates

Import checks
What checks on certificates should be done?
☑ skip self-signed ☐ must be self-signed

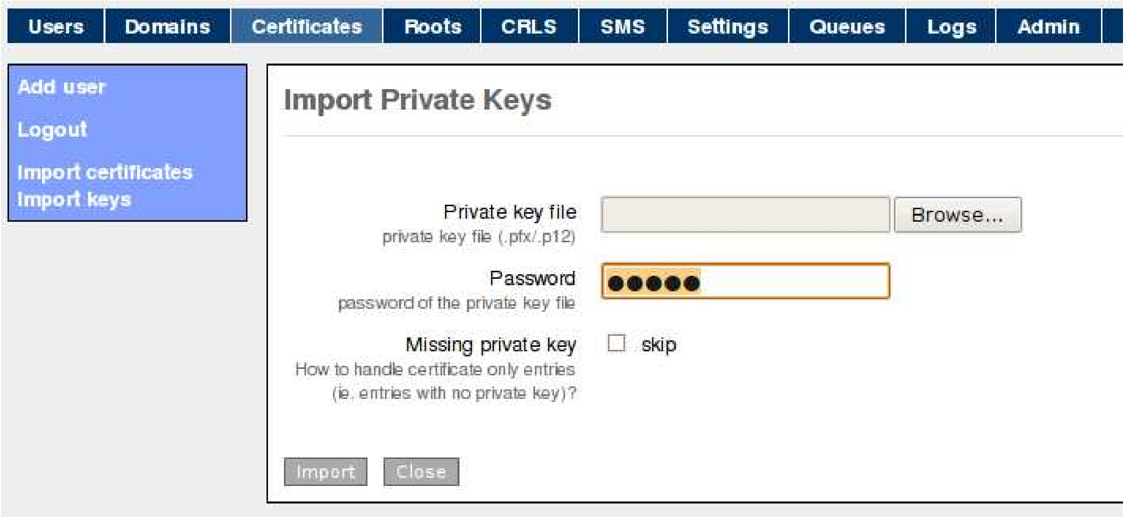
Expired
How to handle expired certificates?
☑ skip

Figure 13: Import certificates

After import a message will be shown telling you how many certificates were imported.

Importing keys

Certificates with associated private keys can be imported into the “Certificates” store using the “Import keys” page (see Figure 14: Import keys).



Import Private Keys

Private key file
private key file (.pfx/.p12)

Password
password of the private key file
●●●●●

Missing private key
How to handle certificate only entries
(ie. entries with no private key)?
□ skip

Figure 14: Import keys

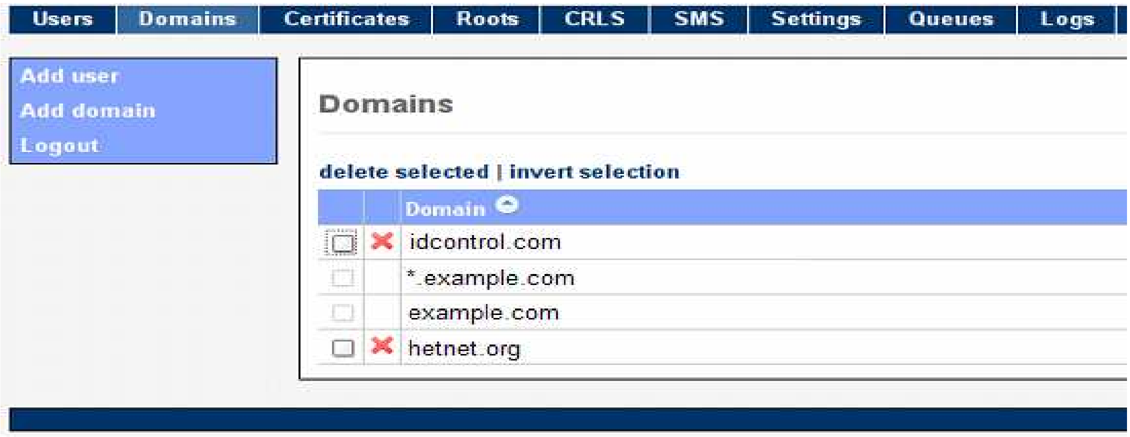
You need to select a password protected PKCS#12 private key file (.p12 or .pfx), enter the password of the private key file and click "Import".

Download keys

Certificates and associated private keys can be downloaded from MailID. You need to select the certificates you want to backup and select "download keys" from the sub-menu. The next page requires you to enter the password used to encrypt the private key file (p12) file with. After entering the password the download will be started.

Domains

Users inherit the settings from the domain of their email address. The domains page gives an overview of all the domains that have been explicitly added to the system (see Figure 9: User preferences)



Domains

		Domain
□	✗	idcontrol.com
□		*.example.com
□		example.com
□	✗	hetnet.org

Figure 15: Domains

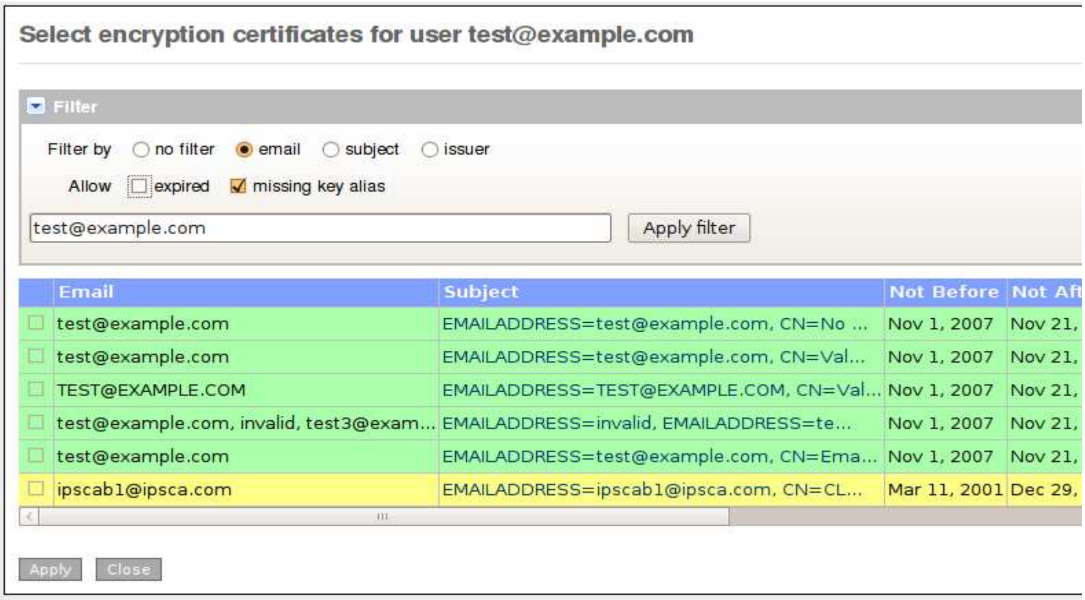
A domain can be used to setup preferences for all users of that domain. For example, a domain can be used to setup a secure S/MIME tunnel between two organizations. Because all users from a specific domain inherit the preferences and certificates from that domain every email sent to a user from that domain will be encrypted with the domain certificate. Normally a "virtual private network" (VPN, for example a TLS connection) is used to setup a secure tunnel between email servers. The problem with a VPN is that each intermediate email server has to support the VPN and each intermediate server needs to be fully trusted because all email is stored unencrypted until forwarded to the next hop. When email is sent to domains that are not under your control (like for example Hotmail or Yahoo) you cannot enforce the use of a secure connection. With S/MIME tunneling, the message itself is encrypted and not the channel. Because the message itself is protected it can be sent over an insecure channel.

Enabling a domain signing certificate on a sending domain allows you to digitally sign all outgoing email automatically (using the same domain signing certificate). By signing all outgoing email you protect yourself against email tampering. Also, receivers are now able to check that the email was really sent from your organization.

Wild-card domains are supported. For example user test@example.com inherits from the wild-card domain *.example.com and from example.com. Once a domain is in use (i.e. there is a user from a domain) the domain can no longer be removed (indicated by the missing red 'cross') until all users from that domain are removed.

Select encryption certificates

Encryption certificates can be selected for a user, a domain or the global settings. The “select encryption certificates” page can be opened by clicking the “select encryption certificates” sub-menu on the preference page (see Figure 9: User preferences). The “select encryption certificates” page shows you all the certificates that have been selected for the user (or domain or global settings when editing the domain or global settings). When editing certificates for a user the default filter will only show certificates with matching email addresses (see Figure 16: Select encryption certificates).



Select encryption certificates for user test@example.com

Filter by ○ no filter ● email ○ subject ○ issuer

Allow □ expired ☑ missing key alias

test@example.com

	Email	Subject	Not Before	Not Aft
□	test@example.com	EMAILADDRESS=test@example.com, CN=No ...	Nov 1, 2007	Nov 21,
□	test@example.com	EMAILADDRESS=test@example.com, CN=Val...	Nov 1, 2007	Nov 21,
□	TEST@EXAMPLE.COM	EMAILADDRESS=TEST@EXAMPLE.COM, CN=Val...	Nov 1, 2007	Nov 21,
□	test@example.com, invalid, test3@exam...	EMAILADDRESS=invalid, EMAILADDRESS=te...	Nov 1, 2007	Nov 21,
□	test@example.com	EMAILADDRESS=test@example.com, CN=Ema...	Nov 1, 2007	Nov 21,
□	ipscab1@ipsca.com	EMAILADDRESS=ipscab1@ipsca.com, CN=CL...	Mar 11, 2001	Dec 29,

Figure 16: Select encryption certificates

Each user can have an unlimited number of associated certificates. The system tries to automatically select the certificates for a user based on strict PKI rules (email address must match, certificate must be trusted up to a root certificate, not revoked, not expired etc.). If a certificate is not automatically selected for a user (for example the email address in the certificate does not match the email address of the user) the administrator can force the usage of a certificate by manually selecting the certificate for this particular user. Figure 16 Shows that multiple certificates are selected for user test@example.com. When a message is S/MIME encrypted all of the selected certificates for the recipient are used. This allows the recipient to open the message with one of the associated private keys. The main advantage of using all of the selected certificates is that it allows the recipient to use different keys to open the message with. For example the key used at home can be different from the key at work. The sender does not known at which location the recipient will open the email so it's better to encrypt the message with both certificates. The "Select encryption certificates" page allows you to create a new end-user certificate for external users using the built-in CA server or allows you to send a certificate to an end-user. For more information on the built-in CA functionality see the CA paragraph.

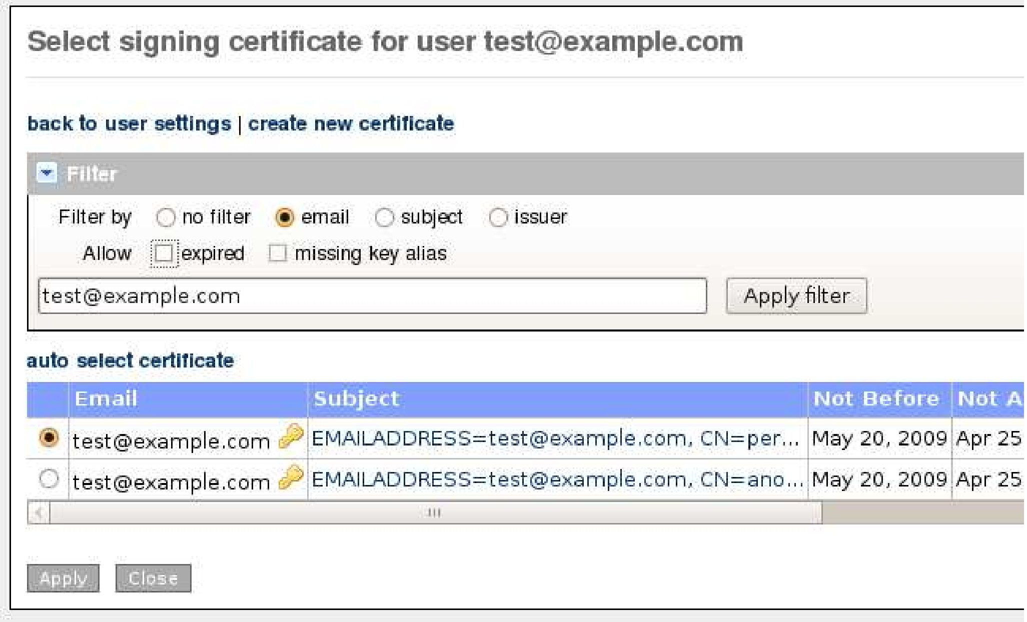
The selected certificates are color coded based on validity and inheritance of the certificates. The following color codes are used:

- green certificate is automatically selected.
- yellow certificate is inherited (from domain or global settings).
- gray certificate is not valid.
- red certificate is revoked.

Certificates can be manually selected and deselected by selecting the certificate checkbox and applying the settings. Automatically selected certificates cannot be deselected (you can remove the certificate if you no longer want to use the certificate). You can uncheck "Auto select certificates" for the user if you do not want to use the automatically selected certificates.

Select signing certificate

A signing certificate can be selected for a user, a domain or the global settings. The "select signing certificate " page can be opened by clicking the "select signing certificate" sub-menu on the preference page (see Figure 9: User preferences).



Select signing certificate for user test@example.com

back to user settings | create new certificate

Filter

Filter by ○ no filter ● email ○ subject ○ issuer

Allow □ expired □ missing key alias

test@example.com

auto select certificate

	Email	Subject	Not Before	Not A
●	test@example.com	EMAILADDRESS=test@example.com, CN=per...	May 20, 2009	Apr 25
○	test@example.com	EMAILADDRESS=test@example.com, CN=ano...	May 20, 2009	Apr 25

Figure 17: Select signing certificate

The "select signing certificate" page shows you the signing certificate that has been selected for the user (or domain or global settings when editing the domain or global settings). When editing the signing certificate for a user the default filter will only show certificates with matching email addresses (see Figure 17: Select signing certificate). Only certificates with an associated private key can be selected and only one certificate can be selected. The system tries to automatically select a signing certificate by searching for a valid certificate with matching email address. If there are multiple certificates suitable for signing, the first certificate found is selected. The administrator can select another certificate if the automatically selected certificate is not the correct one. If a certificate was manually selected you can revert to an automatically selected certificate by pressing "auto select certificate".

Signing certificate selection uses the following color codes:

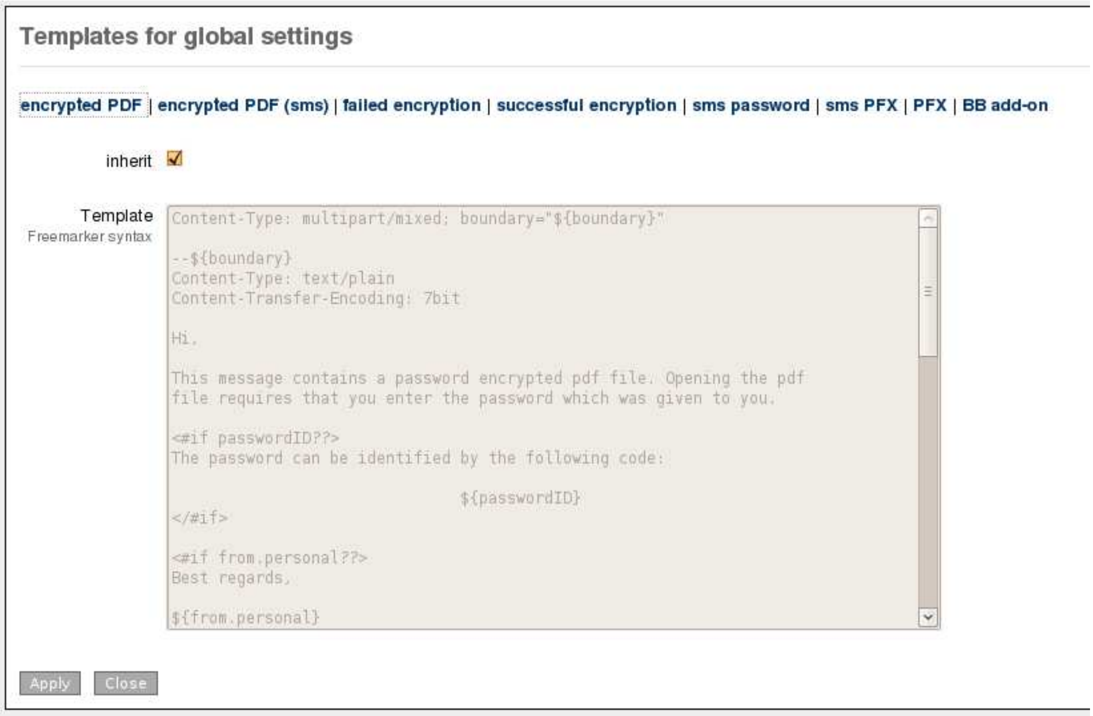
- yellow certificate is inherited (from domain or global settings).
- gray certificate is not valid.
- red certificate is revoked.

Templates

Some actions require the system to send out email or SMS Text messages. These messages are created from templates. These templates can be modified by the administrator[15]. The following templates can be edited: "encrypted pdf", "encrypted pdf (sms)", "failed encryption", "successful encryption", "sms password", "sms PFX"[16], "PFX" and "Blackberry add-on" (see Figure 18: Templates).

[15] The templates are based on the Freemarker template language (see http://freemarker.sourceforge.net/)

[16] sms PFX and PFX template can only be edited for the global settings



Templates for global settings

encrypted PDF | encrypted PDF (sms) | failed encryption | successful encryption | sms password | sms PFX | PFX | BB add-on

inherit ☑

Template
Freemarker syntax

```
Content-Type: multipart/mixed; boundary="${boundary}"

--${boundary}
Content-Type: text/plain
Content-Transfer-Encoding: 7bit

Hi,

This message contains a password encrypted pdf file. Opening the pdf
file requires that you enter the password which was given to you.

<#if passwordID??>
The password can be identified by the following code:

                                ${passwordID}
</#if>

<#if from.personal??>
Best regards,

${from.personal}
```

Figure 18: Templates

Encrypted PDF

This template is used for the email message when the source message is PDF encrypted. The PDF attachment in the template is just a ‘dummy’ PDF attachment which will be replaced by a new encrypted PDF when a new message is created.

Encrypted PDF (sms)

This template is used for the email message when the source message is PDF encrypted and the PDF password is sent by SMS Text.

Failed encryption

This template is used for the email message when the message could not be encrypted but encryption was mandatory.

Successful encryption

This template is used for the email message when the message was successfully encrypted and the sender of the message has “Encryption notification” enabled.

SMS password

This is a template for the SMS Text message with the generated PDF password. The complete SMS Text message should fit in one SMS Text message (maximum 160 characters). The template should therefore be small.

SMS PFX

This is a template for the SMS Text message with the password for the password encrypted private key file. The complete SMS Text message should fit in one SMS Text message (maximum 160 characters). The template should therefore be small. For more information see the CA paragraph.

PFX

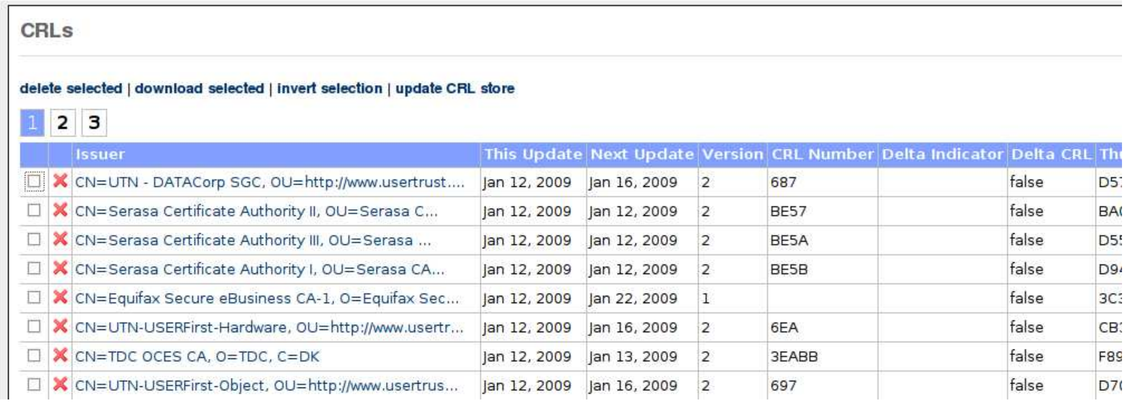
This is a template for the email containing the password encrypted private key file. For more information see the CA paragraph.

BB add-on

This template is used for the email message when the recipient preference "Recipient uses add-on" is enabled. Any S/MIME message sent to a recipient with "Recipient uses add-on" is converted to a message that can be read on a Blackberry with the MailID for Blackberry add-on. For more information see the MailID Blackberry add-on manual.

CRLs

A certificate revocation list (CRL) is a list of certificates that have been revoked and should therefore no longer be used. Certificates can contain CRL distribution points which stores the location of the latest CRL. MailID periodically scans all the trusted certificates[17] from the certificate stores, extracts the CRL distribution points, and downloads the latest CRLs from these distribution points[18]. The CRLs are stored in the CRL store (see Figure 19: CRL store).


CRLs
delete selected | download selected | invert selection | update CRL store
1 2 3

		Issuer	This Update	Next Update	Version	CRL Number	Delta Indicator	Delta CRL	Th
□	✗	CN=UTN - DATACorp SGC, OU=http://www.usertrust....	Jan 12, 2009	Jan 16, 2009	2	687		false	D5
□	✗	CN=Serasa Certificate Authority II, OU=Serasa C...	Jan 12, 2009	Jan 12, 2009	2	BE57		false	BA
□	✗	CN=Serasa Certificate Authority III, OU=Serasa ...	Jan 12, 2009	Jan 12, 2009	2	BE5A		false	D5
□	✗	CN=Serasa Certificate Authority I, OU=Serasa CA...	Jan 12, 2009	Jan 12, 2009	2	BE5B		false	D9
□	✗	CN=Equifax Secure eBusiness CA-1, O=Equifax Sec...	Jan 12, 2009	Jan 22, 2009	1			false	3C
□	✗	CN=UTN-USERFirst-Hardware, OU=http://www.usertr...	Jan 12, 2009	Jan 16, 2009	2	6EA		false	CB
□	✗	CN=TDC OCES CA, O=TDC, C=DK	Jan 12, 2009	Jan 13, 2009	2	3EABB		false	F89
□	✗	CN=UTN-USERFirst-Object, OU=http://www.usertrus...	Jan 12, 2009	Jan 16, 2009	2	697		false	D7

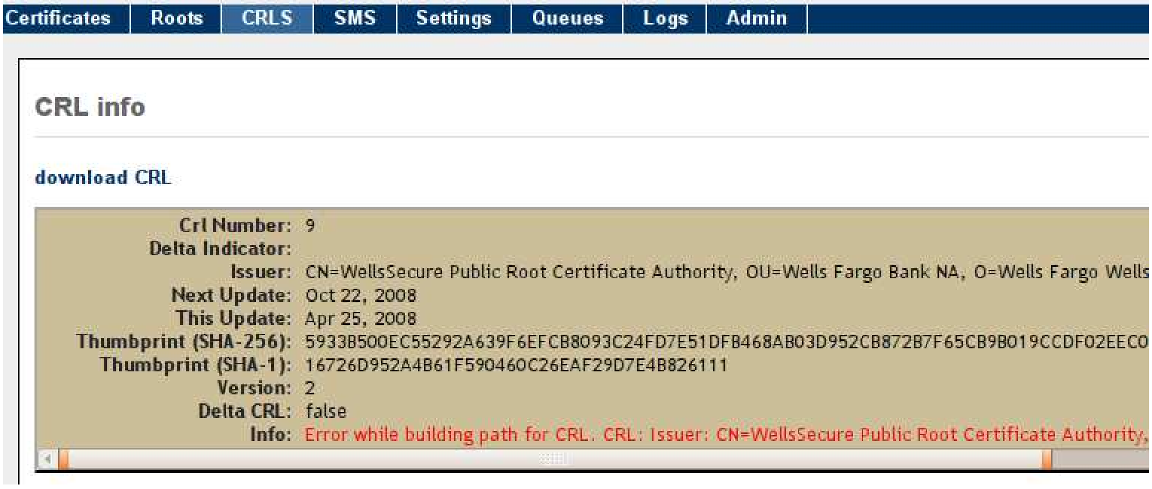
Figure 19: CRL store

CRL details can be viewed by clicking on the CRL “Issuer” link (see Figure 20: CRL details). CRLs which are not trusted (incorrectly signed, no path to a trusted root

[17] By default only trusted certificates are scanned for distribution points.

[18] MailID supports http(s) and LDAP distribution points.

etc.) are shown in a gray color. The details page gives more info why a CRL is not trusted. The CRL store is periodically updated (by default every 30 minutes). An update can be forced by clicking “update CRL store” in the sub-menu.



CRL info

download CRL

Crl Number: 9
Delta Indicator:
Issuer: CN=WellsSecure Public Root Certificate Authority, OU=Wells Fargo Bank NA, O=Wells Fargo Wells
Next Update: Oct 22, 2008
This Update: Apr 25, 2008
Thumbprint (SHA-256): 5933B500EC55292A639F6EFCB8093C24FD7E51DFB468AB03D952CB872B7F65CB9B019CCDF02EEC0
Thumbprint (SHA-1): 16726D952A4B61F590460C26EAF29D7E4B826111
Version: 2
Delta CRL: false
Info: Error while building path for CRL. CRL: Issuer: CN=WellsSecure Public Root Certificate Authority,

Figure 20: CRL details

CA

MailID contains a built-in CA server which can be used to create end-user certificates for internal and external users. This allows you to quickly setup your S/MIME infrastructure with external recipients without having to resort to external CAs for your certificates. Certificates and private keys can be easily and securely transported to external recipients using a password encrypted certificate store (sent as a password protected PFX file attached to an email message). The external recipients can use the certificate with any S/MIME capable email client (Outlook, Outlook express, Lotus Notes etc.) and start receiving and sending S/MIME encrypted email without having to install additional software.

Note that the built-in CA has limited functionality. If you need to support multiple CA profiles, OCSP, CRL for intermediate and root etc. you are advised to use an external CA (for example EJBCA).

We will now briefly explain the CA functionality. For a more thorough guide on how to setup your S/MIME infrastructure see the S/MIME setup guide.

Before you can start creating end-user certificates you have to create a root and intermediate certificate[19]. If there is no CA certificate available or selected you will receive a warning that you must select or create a new CA certificate.

Create new CA

Root and intermediate certificates (and an intermediate private key) are required before you can start creating end-user certificates. You can use the "Create new CA" page to create your new CA certificates (see Figure 21: Create new CA).

You must specify some details for the root and intermediate certificate.

Validity

The time in days this CA certificate is valid starting from the day it is created. Your advised to make the certificate valid period not too short.

Key length

The length of the public key in bits. You can choose between 1024, 2048, 4096. Your advised to use a 2048 bits key.

Email

The email address will be added to the certificate. The email address is not required. You are advised to leave it empty unless your policy requires an email address for your CA.

Common name

[19] If you already have a root and intermediate certificate you can use them instead of making new CA certificates.

The common name of the certificate is the main identifier of the certificate and is therefore required. The common name of the root certificate must be different than the common name of the intermediate certificate. You are also strongly advised to choose a unique common name and never to reuse a common name for a new CA certificate.

More

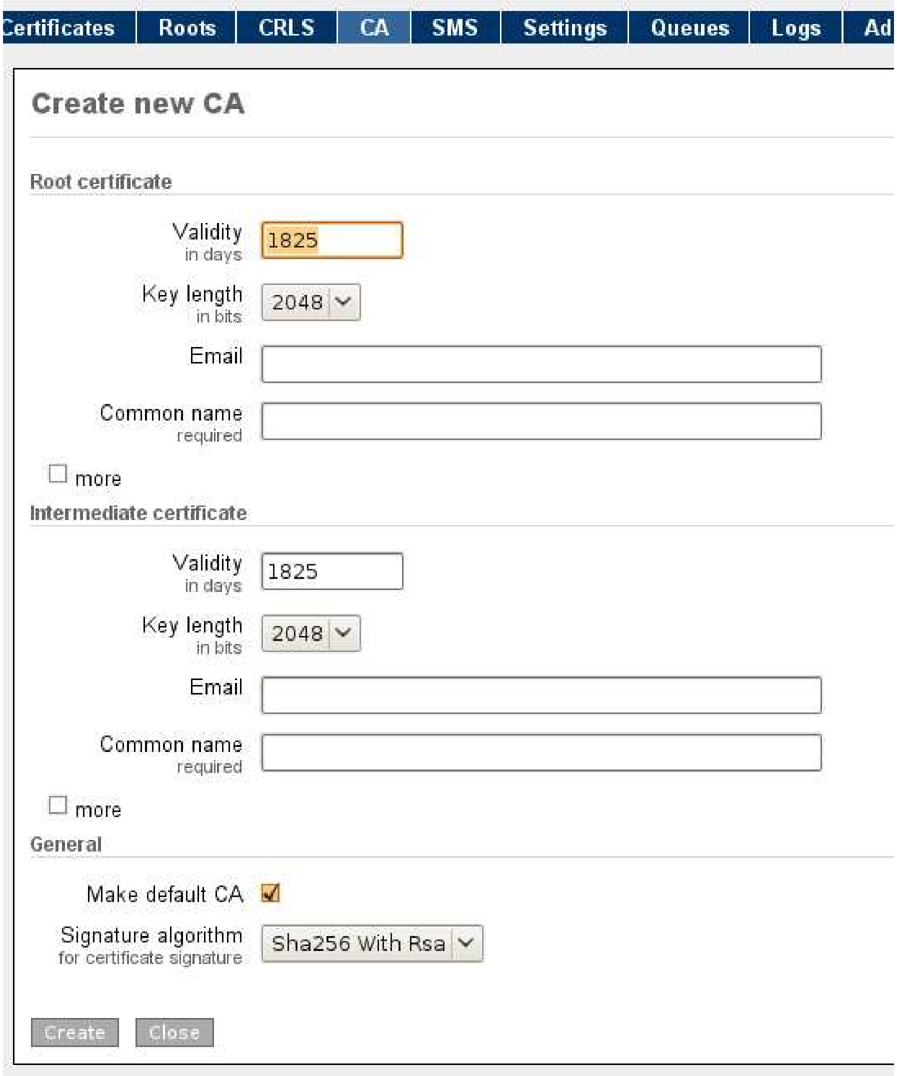
More settings allows you to specify organization, first name and last name. These settings are only used to make it easier for end users to identify your CA certificate.

Make default CA

If checked the newly created CA will be the default CA

Signature algorithm

The algorithm used to sign the certificate with. You are advised to use "SHA256 With RSA".



Create new CA

Root certificate

Validity in days: 1825

Key length in bits: 2048

Email:

Common name required:

□ more

Intermediate certificate

Validity in days: 1825

Key length in bits: 2048

Email:

Common name required:

□ more

General

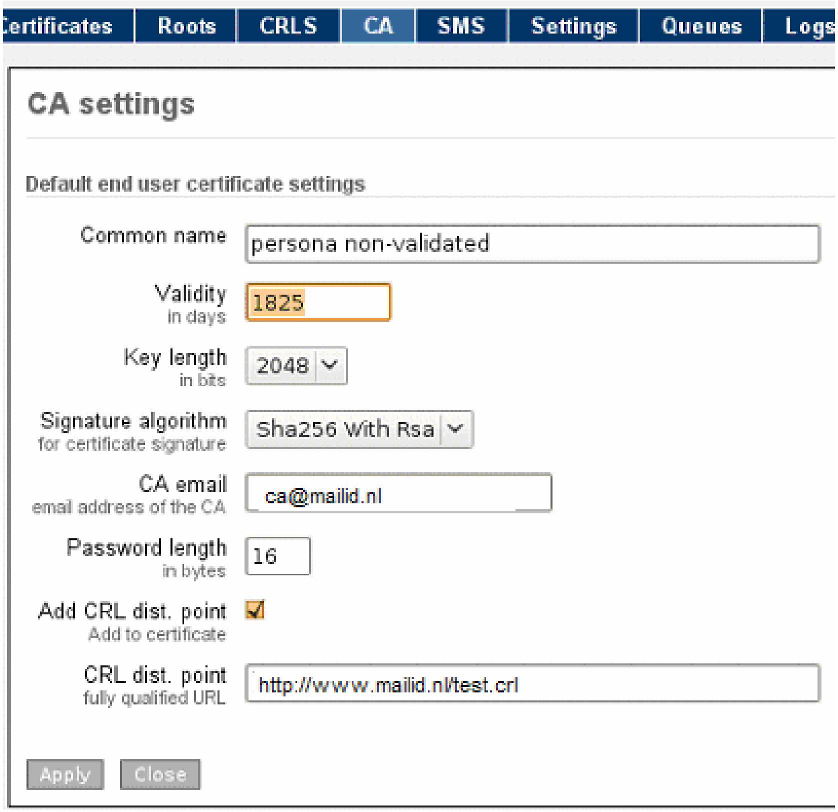
Make default CA ☑

Signature algorithm for certificate signature: Sha256 With Rsa

Figure 21: Create new CA

CA settings

The CA settings page can be used to specify the default settings for the CA (see



CA settings

Default end user certificate settings

Common name: persona non-validated

Validity (in days): 1825

Key length (in bits): 2048

Signature algorithm (for certificate signature): Sha256 With Rsa

CA email (email address of the CA): ca@mailid.nl

Password length (in bytes): 16

Add CRL dist. point (Add to certificate): ☑

CRL dist. point (fully qualified URL): http://www.mailid.nl/test.crl

Figure 22: CA settings

Figure 22: CA settings)

Common name

The default common name used for the new end-user certificate creation page.

Validity

The default validity (in days) for a new end-user certificate.

key length

The default key length for a new end-user certificate.

Signature algorithm

CA email

The sender email address used when sending certificates to end-users by email. You should make sure that the CA email address is a valid email address. Because the email containing the encrypted certificate is sent by MailID you should make sure that the settings for the CA email user are such that the email is not encrypted by MailID (i.e. set encrypt mode of the CA user to "No Encryption"). If you want to sent a certificate and key to a recipient you must specify the CA email address.

Note: don't forget to set “encrypt mode” of the CA user to “No Encryption” !

Password length

The certificate creation page allows you to automatically generate a password which is used to encrypt the certificate and key with. The length of the generated password depends on the password length setting.

Add CRL dist. Point

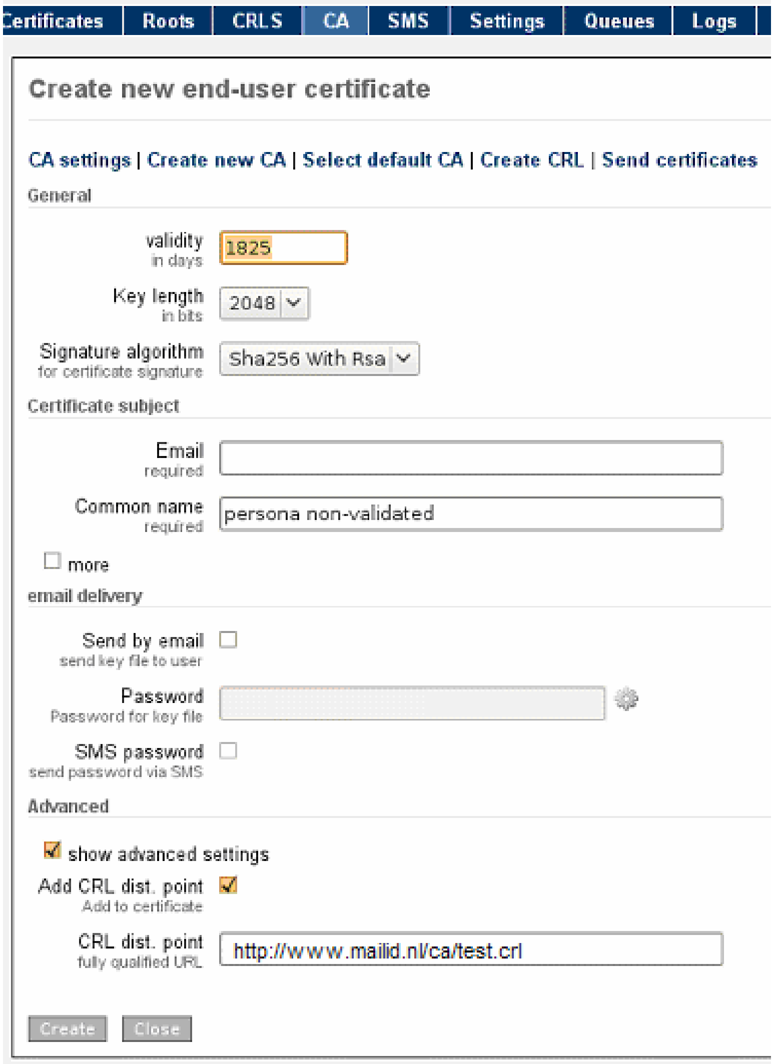
This is the default value for “Add CRL dist. Point” on the “Create new end-user certificate” page. If checked and the CRL distribution point is set the CRL distribution point value will be added to the end-user certificate.

CRL dist. Point

The CRL distribution point added to the end-user certificate (if “Add CRL dist. Point” is set). This is the default value for the “CRL distribution point” setting on the “Create new end-user certificate” page.

Create new end-user certificate

The default CA page allows you to create a new end-user certificate (see Figure 23: Create new end-user certificate). Before an end-user certificate can be created a CA should be available. A warning will be shown if the CA is incorrectly setup.



Create new end-user certificate

CA settings | Create new CA | Select default CA | Create CRL | Send certificates

General

validity in days: 1825

Key length in bits: 2048

Signature algorithm for certificate signature: Sha256 With Rsa

Certificate subject

Email required:

Common name required: persona non-validated

□ more

email delivery

Send by email send key file to user: □

Password Password for key file:

SMS password send password via SMS: □

Advanced

☑ show advanced settings

Add CRL dist. point Add to certificate: ☑

CRL dist. point fully qualified URL: http://www.mailid.nl/ca/test.crl

Figure 23: Create new end-user certificate

The general and Certificate subject settings have already been discussed.

Email delivery

The email delivery settings are required when you want to securely sent the newly created certificate and private key to an external recipient by email. If the “Send by email” checkbox is selected you should also enter the password which is used to protect the certificate and private key. A password can be randomly generated by pressing the 'gear' icon on the right hand side of the password edit field. If you manually create a password you have to make sure that the password is strong enough. The password should be handed out to the recipient in a secure way i.e. it should not be emailed. For example you can sent it by regular post or give the password in person. Alternatively you can have MailID sent the password by a SMS Text message.

SMS password

If the “SMS password” checkbox is selected the password for the protected certificate and private key file will be sent to the recipient by SMS. This requires that the SMS gateway is correctly setup (see SMS gateway) and that the recipients telephone number is added to the user settings of the recipient.

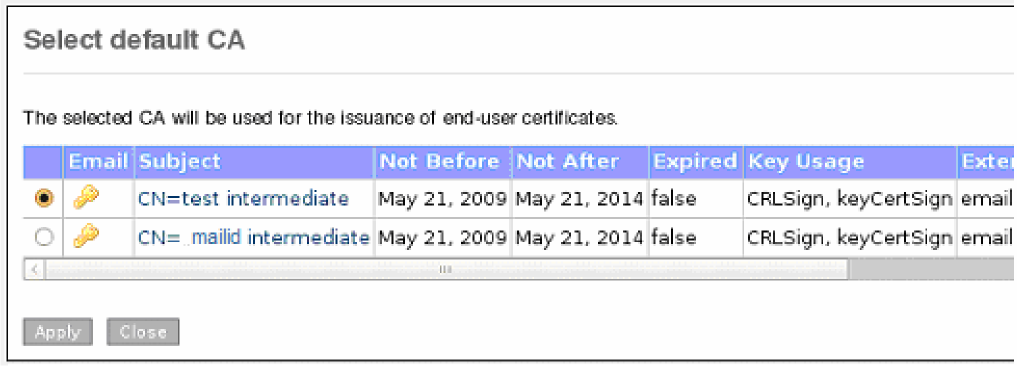
Advanced settings

Advanced settings allows you to specify the CRL distribution point. A CRL distribution point should be a fully qualified URL pointing to the location where you can download the latest CRL for the CA. If you are planning to create a CRL for your CA and would like to publish the CRL for external recipients you should be sure that you specify the correct URL. The URL cannot be changed after the certificate has been issued. The default value for the CRL distribution point is taken from the CA settings.

When the create button is clicked and all settings are valid a new end-user certificate is created using the default CA. If “Send by email” was selected the certificate and key will be password protected with the password and sent to the recipient by email. If “SMS password” was selected the password will be sent by a SMS Text message to the recipients telephone number. For a more thorough explanation of this procedure see the S/MIME administration guide.

Select default CA

There can be multiple CAs but only one can be active. You can select the default CA using the “Select default CA” page (see Figure 24: Select default CA).



Select default CA

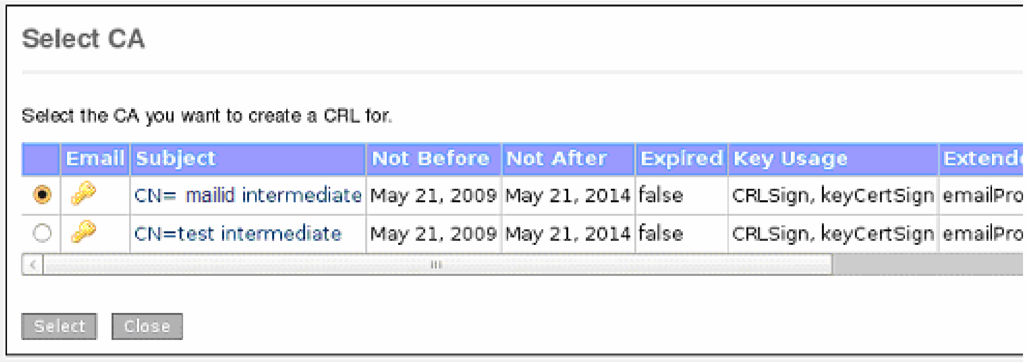
The selected CA will be used for the issuance of end-user certificates.

	Email	Subject	Not Before	Not After	Expired	Key Usage	Exte
●	🔑	CN=test intermediate	May 21, 2009	May 21, 2014	false	CRLSign, keyCertSign	email
○	🔑	CN= mailid intermediate	May 21, 2009	May 21, 2014	false	CRLSign, keyCertSign	email

Figure 24: Select default CA

Create CRL

Sometimes you want to make sure that a certificate is no longer used. A certificate revocation list (CRL) allows you to revoke a specific certificate issued by a CA. With the "Create CRL" page you can create or update a CRL for your CAs. Before creating the CRL you have to select the CA for which you want to create a CRL (see Figure 25: Select CA for CRL).



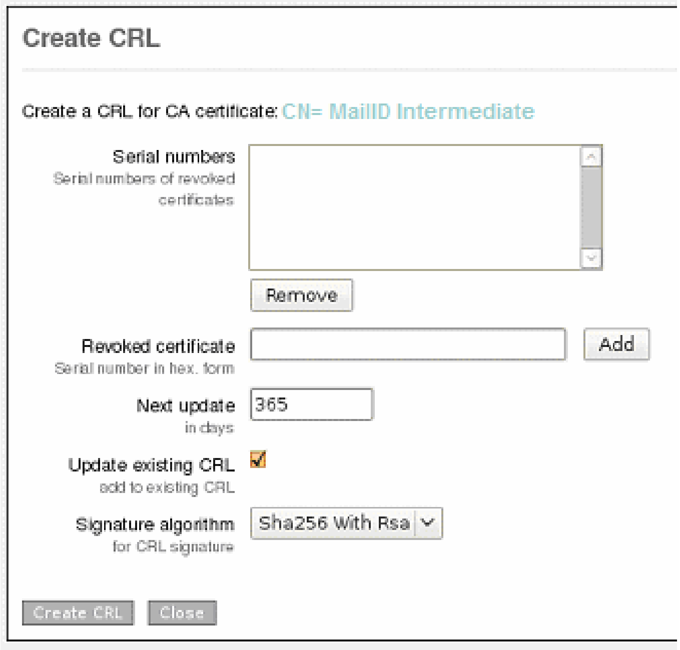
Select CA

Select the CA you want to create a CRL for.

	Email	Subject	Not Before	Not After	Expired	Key Usage	Extend
●	🔑	CN= mailid intermediate	May 21, 2009	May 21, 2014	false	CRLSign, keyCertSign	emailPro
○	🔑	CN=test intermediate	May 21, 2009	May 21, 2014	false	CRLSign, keyCertSign	emailPro

Figure 25: Select CA for CRL

after selecting the CA the "Create CRL" page is opened (see Figure 26: Create CRL) on which you can specify which certificates should be revoked.



Create CRL

Create a CRL for CA certificate: CN= MailID Intermediate

Serial numbers
Serial numbers of revoked certificates

Remove

Revoked certificate
Serial number in hex. form

Add

Next update
in days
365

Update existing CRL
add to existing CRL
☑

Signature algorithm
for CRL signature
Sha256 With Rsa

Create CRL
Close

Figure 26: Create CRL

Serial numbers

A certificate, issued by a CA, is uniquely identified by it's serial number[20]. The serial numbers list contains all the serial numbers that are about to be revoked.

Revoked certificate

You can add a new certificate to the list of certificates to be revoked by pasting the serial number of the certificate (in hex form) in the “Revoked certificate” edit box and clicking the Add button.

Next update

The “next update” is the date at which the CA claims it will issue a new CRL[21]. If your CA contains a CRL distribution point (see Create new CA) you should make sure that an updated CRL is available and download-able from the CRL distribution point URL before the CRL expiration date. The next update is specified in days from the date of the CRL creation.

Update existing CRL

If “update existing CRL” is selected an existing CRL is updated with the new serial numbers. In other words the new CRL will contain the serial numbers of the old CRL and the new serial numbers. If “update existing CRL” is not selected a completely new CRL will be created with only the new serial numbers. You are

[20] A CA should never reuse a serial number.

[21] The next update is the date at which a new CRL must be available. A CA is allowed to issue a new CRL before this date.

advised to always update an existing CRL because certificates that are previously revoked should stay revoked.

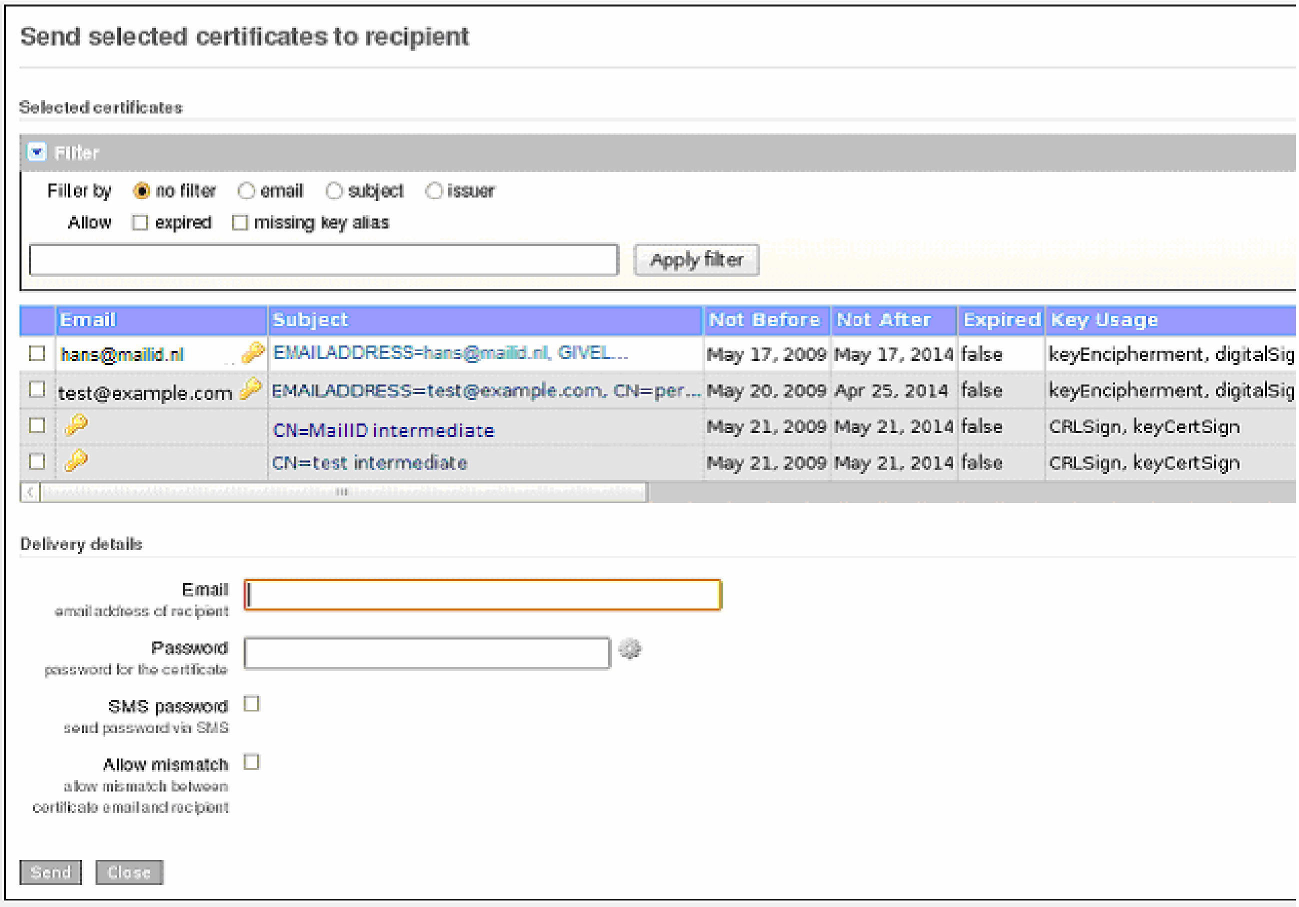
Signature algorithm

The CRL will be signed by the issuing CA. This is done to ensure that only the CA is allowed to issue a CRL. The signature algorithm can be specified. You are advised to use “SHA256 With RSA”.

Clicking the “Create CRL” button will start the CRL creation process. The new CRL will be automatically added to the CRL store. If your CA uses a CRL distribution point you should publish the CRL by downloading the CRL from the CRL store and uploading it to the CRL distribution point URL.

Send certificates

Sometimes end-users require a copy of their certificates (and private keys). For example when they experienced a system crashed and had to completely reinstall the operating system but forgot to make a copy of the certificates. The send certificates page can be used to sent an end-user a new copy of their certificates. Such a feature is known as “key escrow”. Clicking “Send certificates” opens the “Send selected certificates to recipient” page (see Figure 27: Send selected certificates to recipient). Normally you should only sent certificates with an email address that matches the recipient but there are situations where you want to sent the certificates to a different email address. Sending CA certificates by email is not allowed to prevent accidental leakage of CA certificates.



Send selected certificates to recipient

Selected certificates

Filter by ● no filter ○ email ○ subject ○ issuer

Allow □ expired □ missing key alias

	Email	Subject	Not Before	Not After	Expired	Key Usage
□	hans@mailid.nl	EMAILADDRESS=hans@mailid.nl, GIVEL...	May 17, 2009	May 17, 2014	false	keyEncipherment, digitalSig
□	test@example.com	EMAILADDRESS=test@example.com, CN=per...	May 20, 2009	Apr 25, 2014	false	keyEncipherment, digitalSig
□		CN=MailID intermediate	May 21, 2009	May 21, 2014	false	CRLSign, keyCertSign
□		CN=test intermediate	May 21, 2009	May 21, 2014	false	CRLSign, keyCertSign

Delivery details

Email
email address of recipient

Password
password for the certificate

SMS password □
send password via SMS

Allow mismatch □
allow mismatch between certificate email and recipient

Figure 27: Send selected certificates to recipient

Email

This is the email address of the recipient to which the certificate(s) will be sent.

“Password” and “SMS password” settings were already explained (see **Create new end-user certificate**).

Allow mismatch

If allow mismatch is checked you are allowed to sent the selected certificate(s) to a different recipient than the email address from the certificate(s). This check is added to prevent any leakage of certificate(s) because of an accidental mistype of the recipients address.

The sending and certificate protection process is exactly similar to the process described in part **Create new end-user certificate**.

PDF encryption

Introduction

PDF encryption can be used as a light-weight alternative to S/MIME encryption that does not require PKI[22]. PDF allows you to decrypt and read encrypted PDF documents. Attachments can be added to a PDF document and the attachments are encrypted as well. The password for the PDF can be manually set per recipient or a password can be randomly generated and sent to the recipient via a SMS Text message.

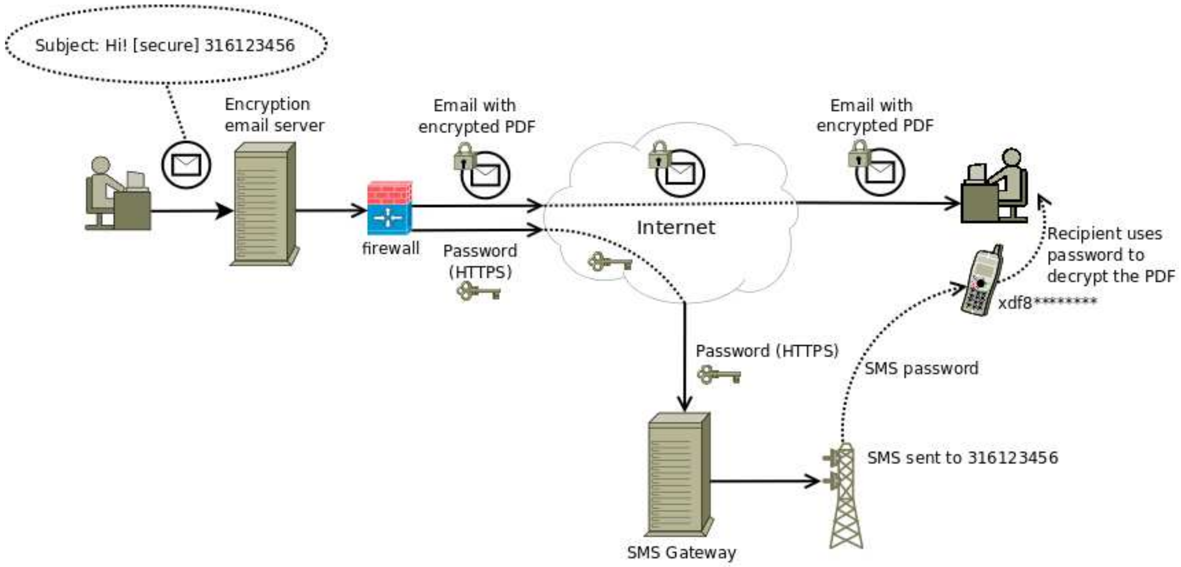


Figure 28: PDF encryption

The basic idea of MailID PDF email encryption is that the message sent by the user is converted to a password encrypted PDF[23] (including all attachments). A standard message is sent to the recipient containing the encrypted PDF. The recipient can open the PDF by entering the password. The password can be a pre-negotiated password or it can be a randomly generated password which is sent by a SMS Text message. The recipient can securely reply to the encrypted PDF by clicking the reply link. This will bring the user to an on-line portal (see "reply URL" setting in the preference page). Figure 28: PDF encryption shows the complete PDF encryption process.

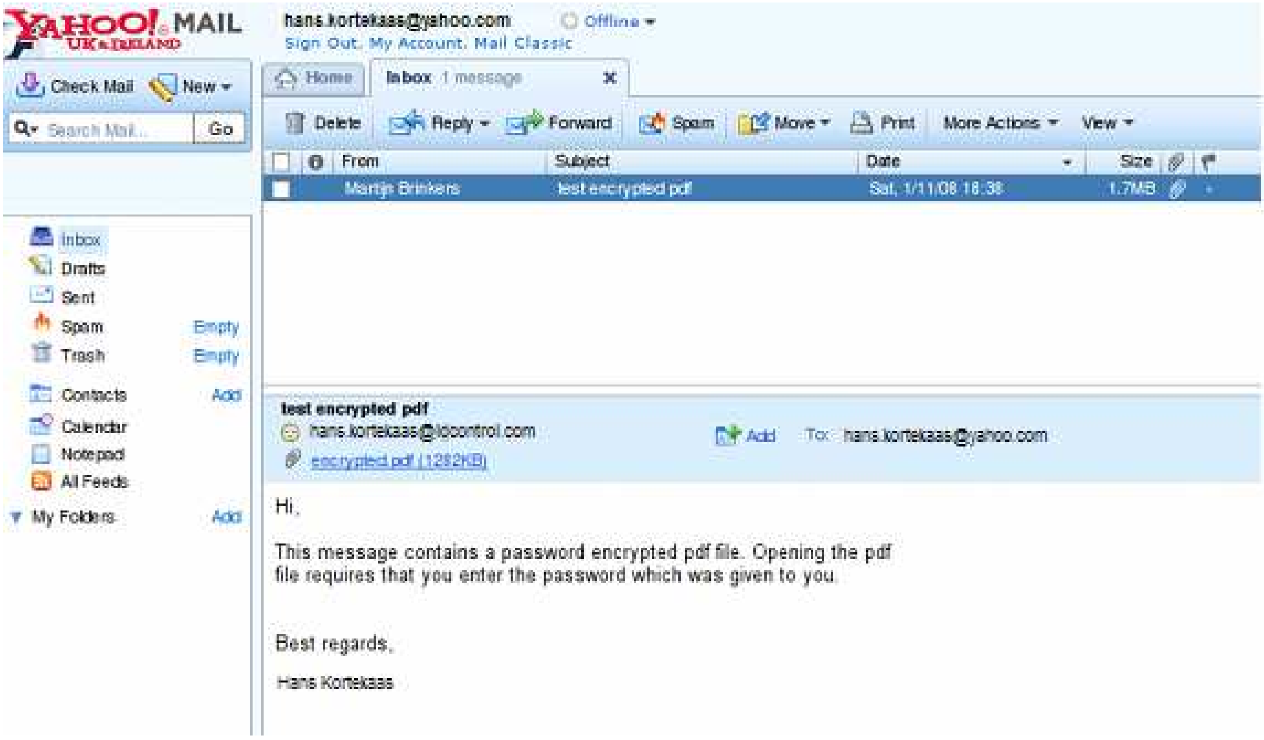
The recipient opens the message in the email client[24]. The message contains a general message body (based on the "encrypted PDF" template) and an

[22] PDFs can be encrypted with X.509 certificates but this is currently not supported.

[23] The PDF is encrypted with AES-128

[24] All email clients, including webmail, are supported.

encrypted PDF (see Figure 29: Encrypted PDF message).



From	Subject	Date	Size
Martijn Brinkers	test encrypted pdf	Sat, 1/11/08 18:38	1.7MB

test encrypted pdf

hans.kortekaas@ldcontrol.com Add To: hans.kortekaas@yahoo.com

encrypted.pdf (1282KB)

Hi,

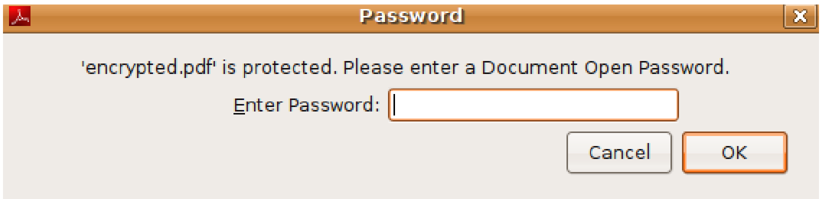
This message contains a password encrypted pdf file. Opening the pdf file requires that you enter the password which was given to you.

Best regards,

Hans Kortekaas

Figure 29: Encrypted PDF message

After opening the PDF the PDF reader asks for the password which was used for the encryption (see Figure 30: PDF password). After entering the correct password the PDF content will be shown. The

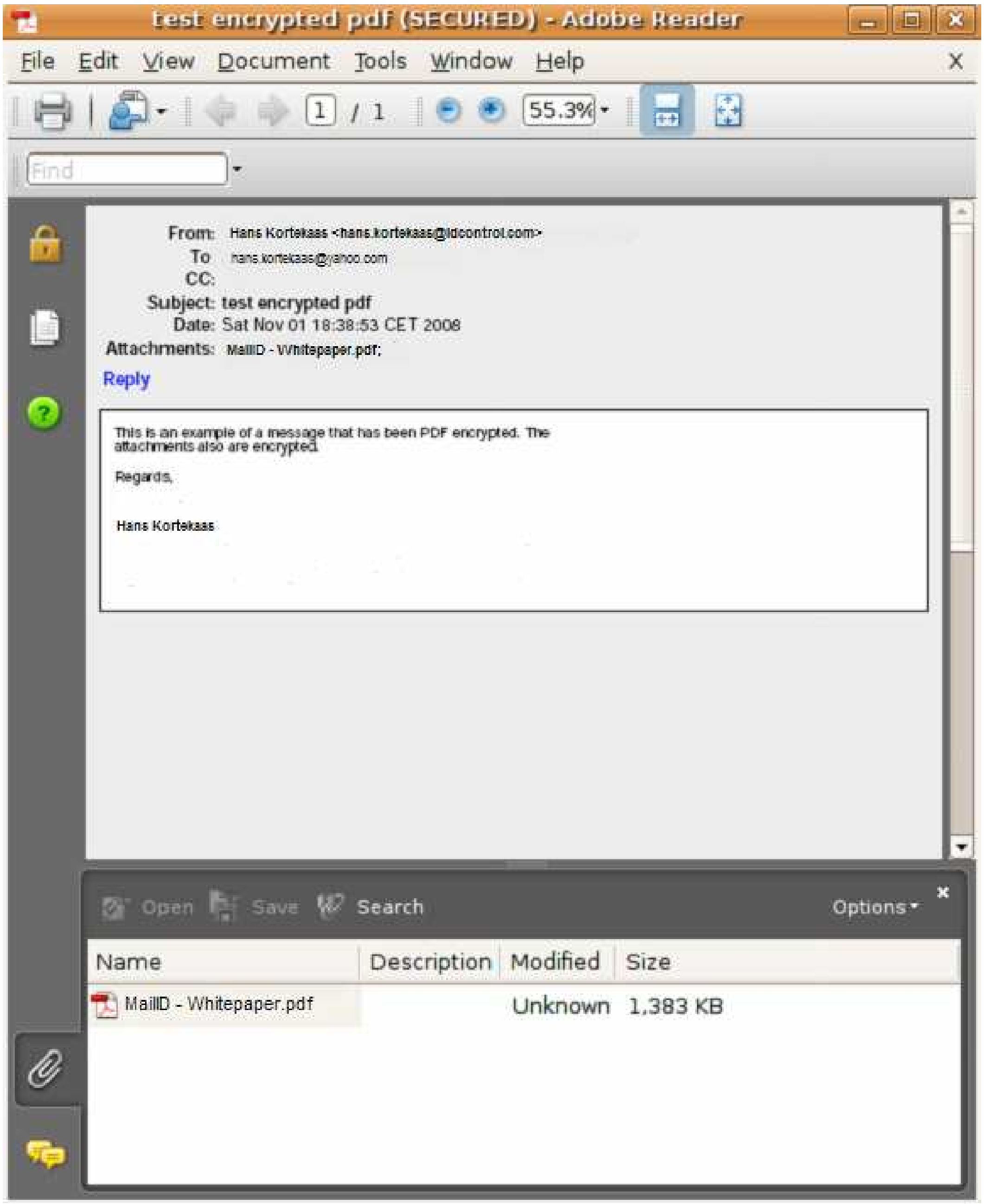


'encrypted.pdf' is protected. Please enter a Document Open Password.

Enter Password:

Figure 30: PDF password

PDF is formatted to make it look like a normal email message. The attachments can be accessed from the bottom attachment pane (see Figure 31: PDF decrypted).



From: Hans Kortekaas <hans.kortekaas@idcontrol.com>
To hans.kortekaas@yahoo.com
CC:
Subject: test encrypted pdf
Date: Sat Nov 01 18:38:53 CET 2008
Attachments: MailID - Whitepaper.pdf;

This is an example of a message that has been PDF encrypted. The attachments also are encrypted.

Regards,

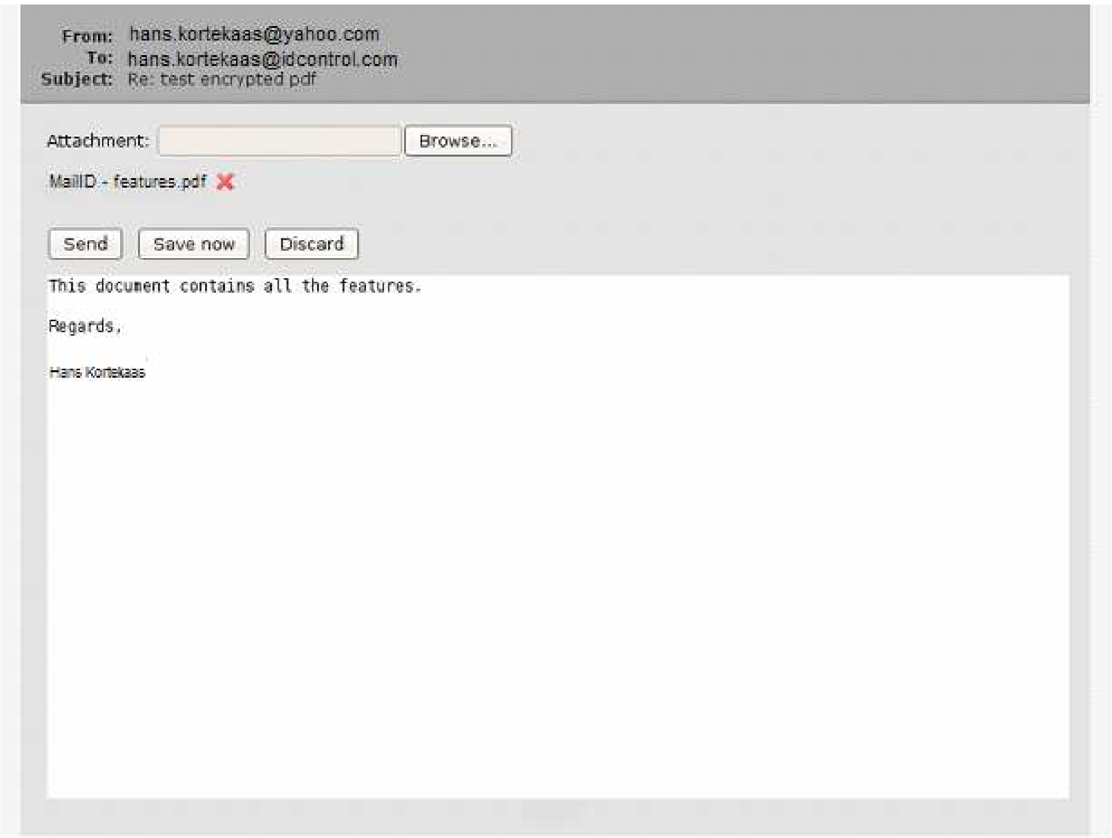
Hans Kortekaas

Name	Description	Modified	Size
MailID - Whitepaper.pdf		Unknown	1,383 KB

Figure 31: PDF decrypted

Replying to PDF

The recipient can reply to the encrypted message by clicking the “Reply” link (see Figure 31: PDF decrypted). An on-line portal will be opened (using a secure https connection) in the browser (see Figure 32: PDF reply). The reply URL in the PDF is equal to the “Reply URL” parameter at the time the encrypted PDF was created.



From: hans.kortekaas@yahoo.com
To: hans.kortekaas@idcontrol.com
Subject: Re: test encrypted pdf

Attachment:

MailID - features.pdf

This document contains all the features.

Regards,

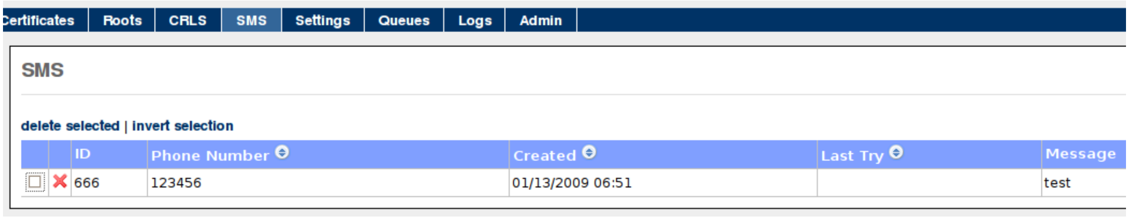
Hans Kortekaas

Figure 32: PDF reply

The user can now enter a message body and add attachments (maximum 3). The reply will be sent via the MailID server. Because the reply is sent via the MailID server it can be encrypted as well.

SMS gateway

MailID contains a SMS gateway which is used to sent the generated passwords to the recipients. The SMS gateway can use different SMS transports for the delivery of SMS Text messages[25]. The default SMS transport uses Clickatell[26] for the actual delivery of SMS Text messages (SMS is sent via a secure HTTPS connection to Clickatell). When a SMS Text message is sent it is queued for delivery until the message has been sent with the SMS transport (see Figure 33: SMS gateway).



		ID	Phone Number	Created	Last Try	Message
☐	✗	666	123456	01/13/2009 06:51		test

Figure 33: SMS gateway

A SMS Text message can be manually added using "Add SMS" on the left-hand side menu[27].

Clickatell transport

The default SMS transport is the Clickatell transport. This transport forwards all the SMS Text messages to an external SMS gateway (using a secure HTTPS connection). You need to sign up for a Clickatell account and configure the Clickatell transport before you are able to sent SMS Text messages. See www.clickatell.com for the sign up procedure.

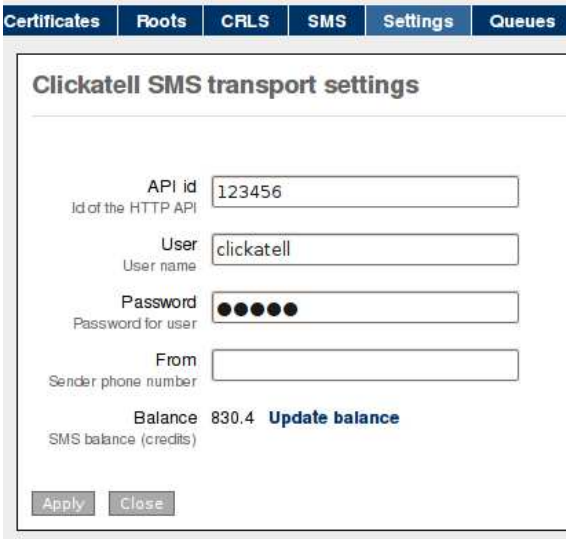
Once you are signed up you need to add a HTTP connection (see the Clickatell "HTTP API Specification v.2.x.x" document for more info) and leave the "Callback" parameters empty. The connection has an associated "API ID" which you will need to configure the Clickatell transport. Open the Clickatell transport configuration page by opening the "Settings" page and click the "Clickatell settings" sub-menu link (see Figure 34: Clickatell settings). The first three settings are mandatory. The "From" parameter can be set to the sender of the SMS Text message (i.e. the telephone number of the sender[28]).

[25] Currently only Clickatell and Gnokii (direct connection to Nokia phones) are supported.

[26] www.clickatell.com

[27] Normally only used for testing the SMS transport.

[28] The telephone number must be approved by Clickatell.



Clickatell SMS transport settings

API id 123456
Id of the HTTP API

User clickatell
User name

Password ●●●●●
Password for user

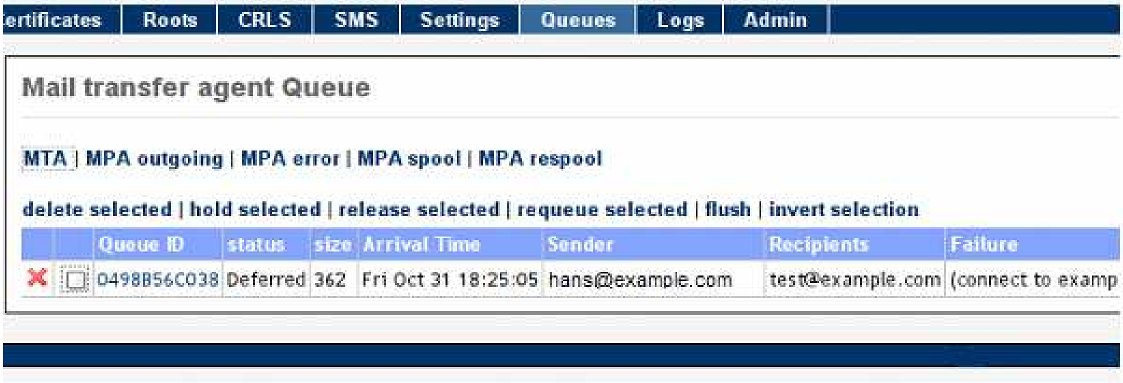
From
Sender phone number

Balance 830.4 **Update balance**
SMS balance (credits)

Figure 34: Clickatell settings

Clickatell uses message credits. To see how many credits are available (and for testing the credentials) you can click the “update balance” link.

Mail queues


ertificates
Roots
CRLS
SMS
Settings
Queues
Logs
Admin
MTA | MPA outgoing | MPA error | MPA spool | MPA respool
delete selected | hold selected | release selected | requeue selected | flush | invert selection

Mail transfer agent Queue

		Queue ID	status	size	Arrival Time	Sender	Recipients	Failure
✗	□	0498B56C038	Deferred	362	Fri Oct 31 18:25:05	hans@example.com	test@example.com	(connect to examp

Figure 35: Mail queues

MailID uses Postfix for sending and receiving of email (MTA). Internally MailID uses a Java based SMTP server[29] for encryption, decryption and other message processing. We will call this internal email server the “Mail Processing Agent” (MPA). The MTA and MPA stores the messages it handles into different mail queues. The mail queues can be viewed and administered by the “Queues” page (see Figure 35: Mail queues).

MTA queue

The MTA queue allows you to remove message from the queue, put messages on hold, view messages etc.

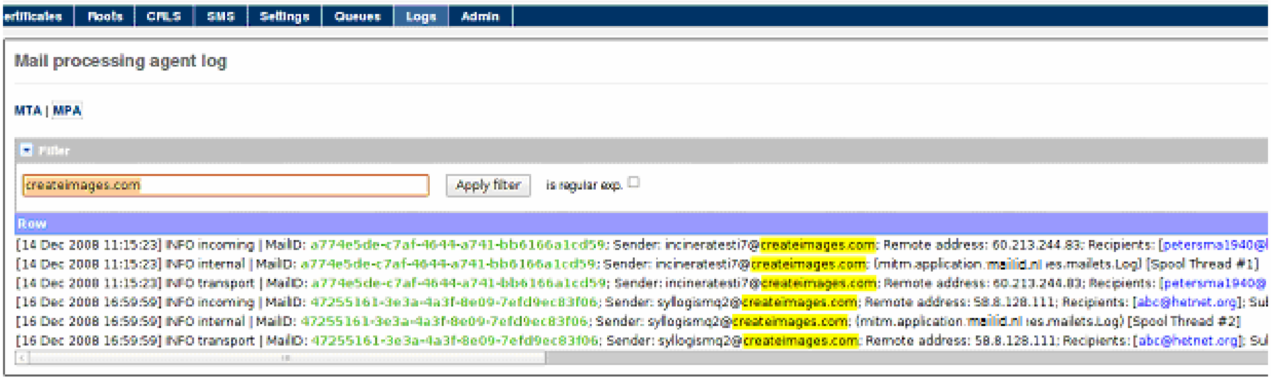
MPA queues

The MPA contains four queues: MPA outgoing, MPA error, MPA spool, MPA respool. Normally the error and respool queue should be empty. The other two queues should only contain email for a short period while the email is processed. Processed email is sent to the MTA for further delivery.

[29] A slightly modified Apache James server (http://james.apache.org/) which is configured as a Postfix filter.

Logs

The “Logs” page can be used to view MTA and MPA log files. A filter can be set to view only a subset (see Figure 36: MPA logs).



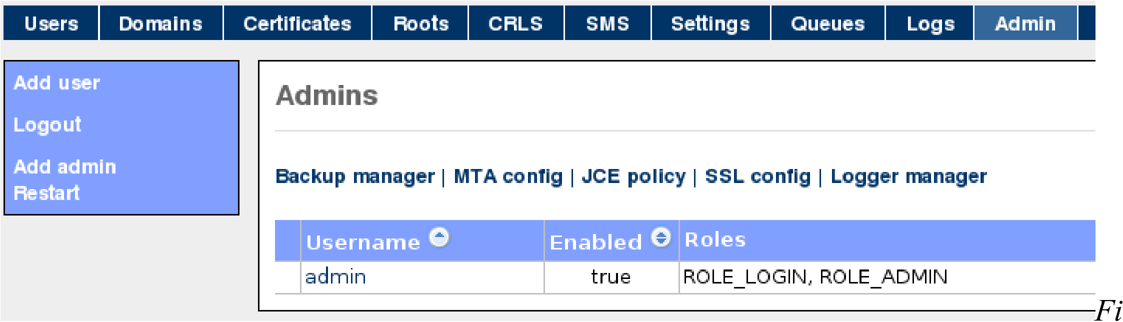
createimages.com

```
[14 Dec 2008 11:15:23] INFO incoming | MailID: a774e5de-c7af-4644-a741-bb6166a1cd59; Sender: incineratesti7@createimages.com; Remote address: 60.213.244.83; Recipients: [petersma1940@
[14 Dec 2008 11:15:23] INFO internal | MailID: a774e5de-c7af-4644-a741-bb6166a1cd59; Sender: incineratesti7@createimages.com; (mitm.application.mailid.nl ies.mailets.Log] [Spool Thread #1]
[14 Dec 2008 11:15:23] INFO transport | MailID: a774e5de-c7af-4644-a741-bb6166a1cd59; Sender: incineratesti7@createimages.com; Remote address: 60.213.244.83; Recipients: [petersma1940@
[16 Dec 2008 16:59:59] INFO incoming | MailID: 47255161-3e3a-4a3f-8e09-7efd9ec83f06; Sender: syllogismq2@createimages.com; Remote address: 58.8.128.111; Recipients: [abc@hetnet.org]; Sul
[16 Dec 2008 16:59:59] INFO internal | MailID: 47255161-3e3a-4a3f-8e09-7efd9ec83f06; Sender: syllogismq2@createimages.com; (mitm.application.mailid.nl ies.mailets.Log) [Spool Thread #2]
[16 Dec 2008 16:59:59] INFO transport | MailID: 47255161-3e3a-4a3f-8e09-7efd9ec83f06; Sender: syllogismq2@createimages.com; Remote address: 58.8.128.111; Recipients: [abc@hetnet.org]; Sul
```

Figure 36: MPA logs

Administrators

It is possible to add multiple administrators each with a different set of roles. The “Admin” gives an overview of all the administrators (see Figure 37: Administrators).



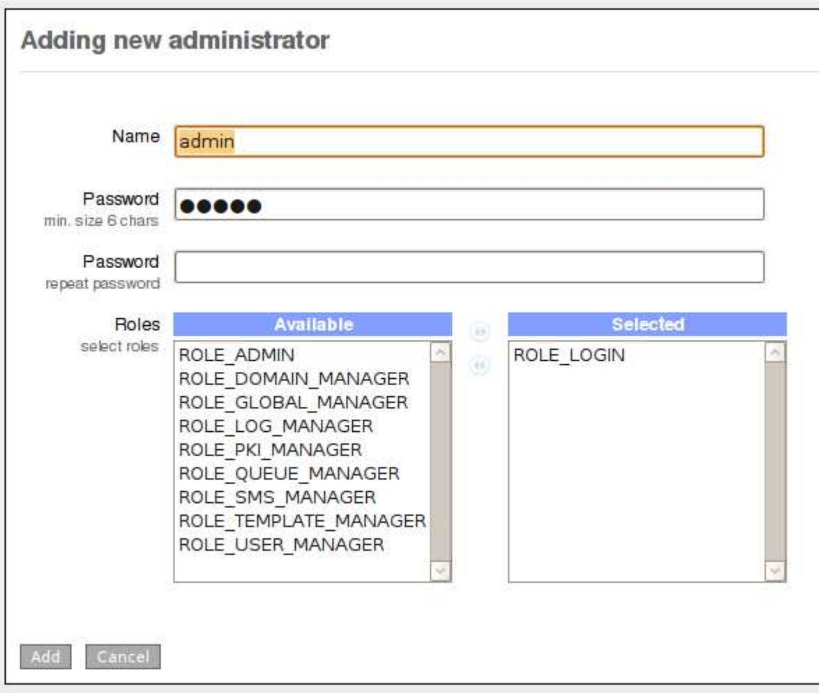
Username	Enabled	Roles
admin	true	ROLE_LOGIN, ROLE_ADMIN

Figure 37: Administrators

A new administrator can be added by clicking “Add admin” on the left-hand side menu which will open the “Adding new administrator” page (see Figure 38: Add new administrator).

The following roles are available:

- ROLE_LOGIN
- ROLE_ADMIN
- ROLE_DOMAIN_MANAGER
- ROLE_GLOBAL_MANAGER
- ROLE_LOG_MANAGER
- ROLE_PKI_MANAGER
- ROLE_QUEUE_MANAGER
- ROLE_SMS_MANAGER
- ROLE_TEMPLATE_MANAGER
- ROLE_USER_MANAGE


Adding new administrator

Name: admin

Password (min. size 6 chars): ●●●●●

Password (repeat password):

Roles (select roles)

Available: ROLE_ADMIN, ROLE_DOMAIN_MANAGER, ROLE_GLOBAL_MANAGER, ROLE_LOG_MANAGER, ROLE_PKI_MANAGER, ROLE_QUEUE_MANAGER, ROLE_SMS_MANAGER, ROLE_TEMPLATE_MANAGER, ROLE_USER_MANAGER

Selected: ROLE_LOGIN

Figure 38: Add new administrator

ROLE_LOGIN

This is a required role. Every administrator must have the ROLE_LOGIN role. An administrator with only ROLE_LOGIN is allowed to only view some basic settings.

ROLE_ADMIN

This role is similar to having all roles (i.e. an administrator with ROLE_ADMIN is allowed to do anything).

ROLE_DOMAIN_MANAGER

This role is allowed to “add domain”, “delete domain”, “edit domain”, “select domain certificates”, “select domain signing certificate”

ROLE_GLOBAL_MANAGER

This role is allowed to edit the global settings.

ROLE_LOG_MANAGER

This role is allowed to view the log files.

ROLE_PKI_MANAGER

This role is allowed to “import certificates”, “delete certificates”, “import keys”, “download keys”, “import CRLs”, “delete CRLs”, “update CRL store” and "manage the CA".

ROLE_QUEUE_MANAGER

This role is allowed to manage the mail queues.

ROLE_SMS_MANAGER

This role is allowed to manage the SMS gateway.

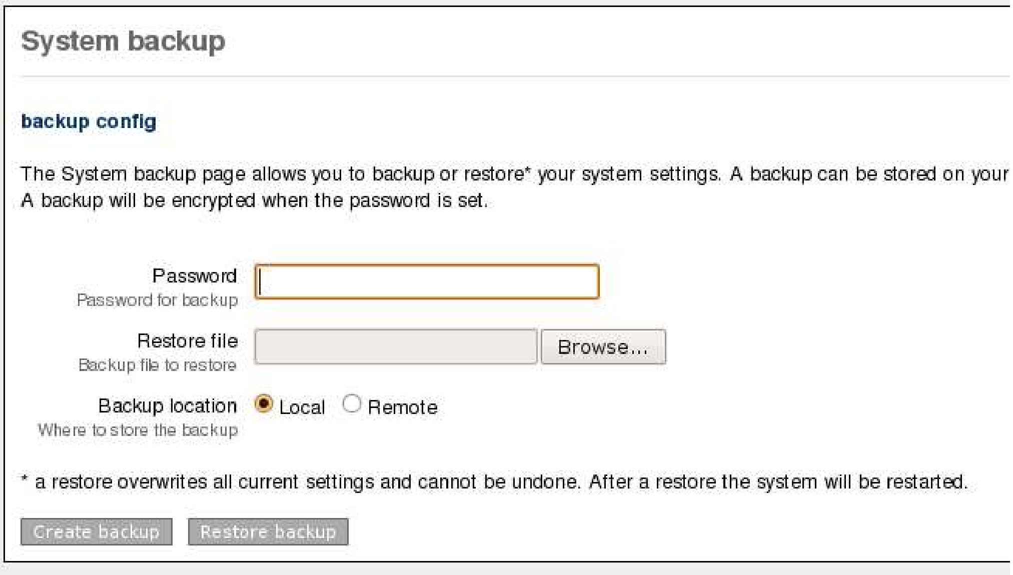
ROLE_TEMPLATE_MANAGER

This role is allowed to edit templates.

ROLE_USER_MANAGE R

This role is allowed to edit templates.

Backup Manager



System backup

backup config

The System backup page allows you to backup or restore* your system settings. A backup can be stored on your
A backup will be encrypted when the password is set.

Password
Password for backup

Restore file
Backup file to restore

Backup location ● Local ○ Remote
Where to store the backup

* a restore overwrites all current settings and cannot be undone. After a restore the system will be restarted.

Figure 39: System backup

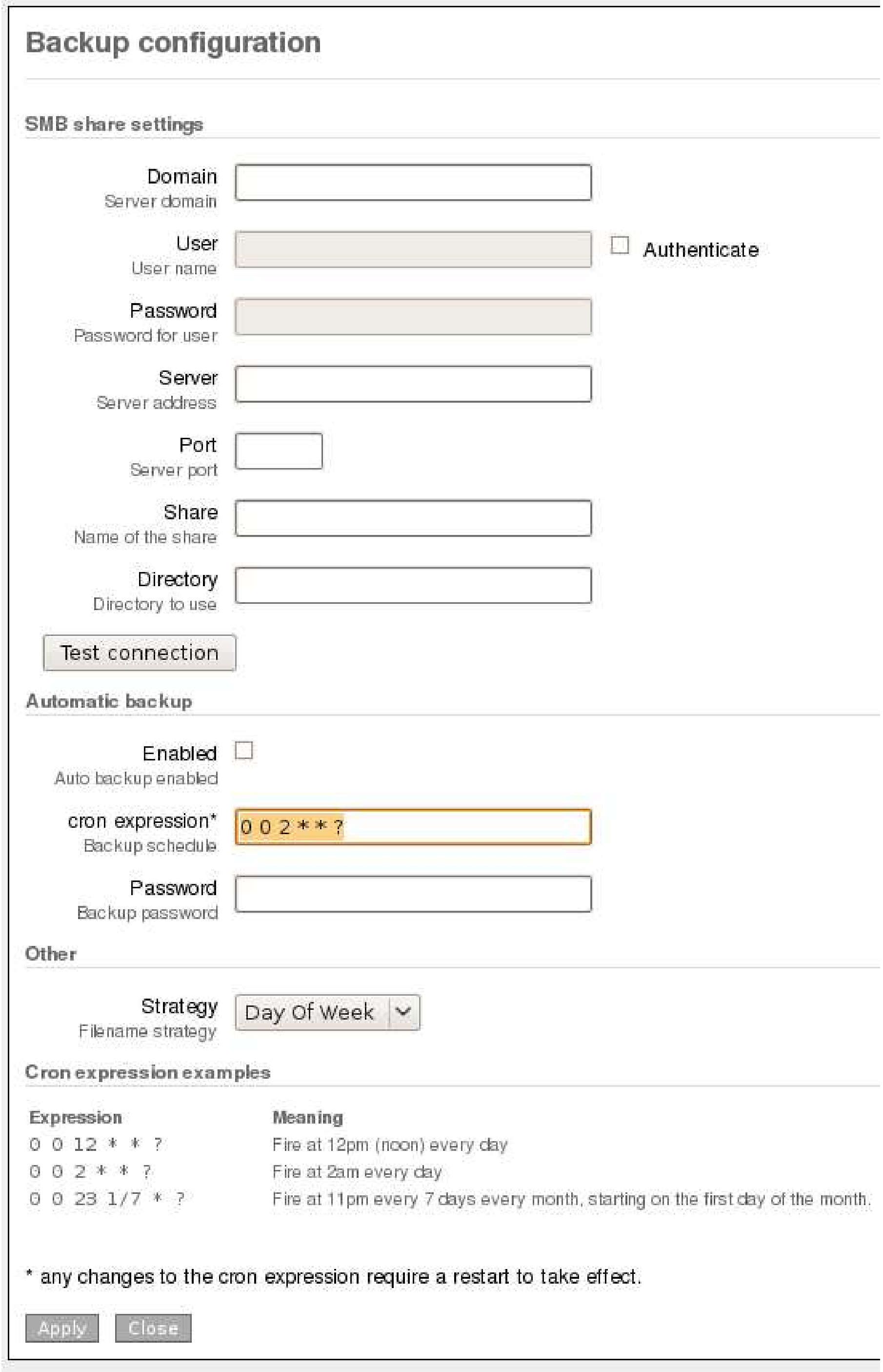
You can use the backup manager to backup and restore all the relevant system settings. A backup can be created and downloaded to your local system with your browser or a backup can be stored on a remote share (see Figure 39: System backup). A backup can be automatically initiated at set intervals and stored (encrypted or non encrypted) on a remote share.

A backup can be password encrypted. If no password is specified the backup will not be encrypted.

Note: restoring a backup overwrites all local settings and cannot be undone.

Backup configuration

The backup configuration page can be used to configure the remote share and configure the automatic backup (see Figure 40: Backup configuration).



Backup configuration

SMB share settings

Domain Server domain	
User User name	□ Authenticate
Password Password for user	
Server Server address	
Port Server port	
Share Name of the share	
Directory Directory to use	

Automatic backup

Enabled Auto backup enabled	□
cron expression* Backup schedule	0 0 2 * * ?
Password Backup password	

Other

Strategy Filename strategy	Day Of Week

Cron expression examples

Expression	Meaning
0 0 12 * * ?	Fire at 12pm (noon) every day
0 0 2 * * ?	Fire at 2am every day
0 0 23 1/7 * ?	Fire at 11pm every 7 days every month, starting on the first day of the month.

* any changes to the cron expression require a restart to take effect.

Figure 40: Backup configuration

SMB share settings

The SMB share settings allows you to specify which remote share to use for the remote backups (automatic backups can only be stored on the remote share). The remote share can be any server that supports the SMB protocol (for example Microsoft Windows Network or SAMBA). You can use "Test connection" to test if the specified share allows you to connect to the remote share with the provided settings.

Automatic backup

MailID can automatically initiate remote backups at set intervals. To enable automatic backups you should select the "enabled" checkbox.

Cron expression

The cron expression determines at which intervals a backup will be started. A restart is required after changing the cron expression[30]. The default cron expression "0 0 2 * * ?" automatically starts a backup every night at 2 o'clock (see Appendix C for more cron expression examples).

Other

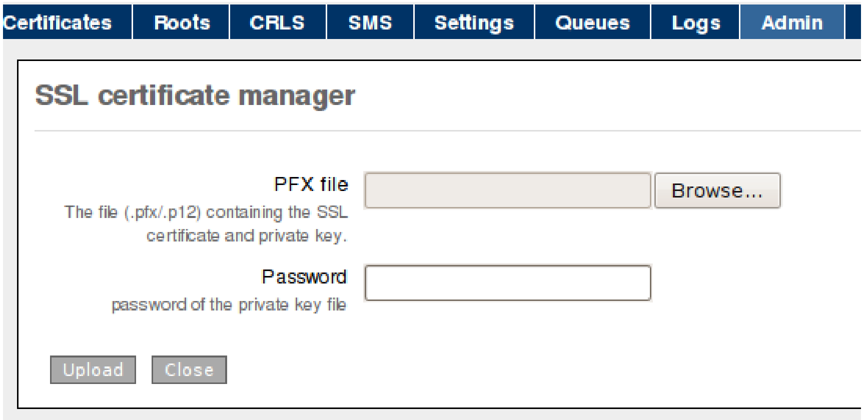
Strategy

The filename strategy determines how the filenames of the backups are created. You can choose between "day of week", "day of month", "day of year" and "timestamp". Day of week uses the day of the week as a backup postfix (1-7). Day of month the day number as a postfix (1-31). Day of year as a number postfix (1-365). Timestamp creates a filename based on the number of milliseconds since January 1, 1970 UTC.

[30] For more info on cron trigger format see http://www.opensymphony.com/quartz/wikidocs/CronTriggers%20Tutorial.html

SSL certificate manager

The default MailID installation uses Jetty for the web server. MailID requires https for the web admin and PDF reply page. During installation a default SSL certificate is installed. It is advised that a new SSL certificate is installed after installation of MailID. You can use the “SSL certificate manager” page to install a new SSL certificate by clicking the “SSL config” sub-menu link on “Admin” page, upload the password protected PKCS#12 file (.pfx or .p12) and press the upload button (see Figure 41: SSL certificate manager).



SSL certificate manager

PFX file
The file (.pfx/.p12) containing the SSL certificate and private key.

Password
password of the private key file

Figure 41: SSL certificate manager

After the installation of the SSL certificate you should restart the system. The system can be restarted by clicking "Restart". The system can also be restarted by going to the “Admin” menu and click “Restart” on the left-side menu or by selecting “Restart services” in the virtual appliance console.

Appendix A

Security considerations

When the PDF reply functionality is used you have to allow access to the MailID server for external users (otherwise they are not able to open the reply page). This also allows access to the administration pages. It is therefore important that the administrator passwords cannot be guessed. A better solution is to only allow access to the PDF reply pages and block access to all other pages. Access to the following URLs should be allowed:

https://192.168.178.24:8443/external/pdf/*

Where the IP should be the external IP and * means that access should be granted to all parent URLs.

Possible ways to block access to other URLs

- Block access in your firewall.
- Use Apache as a front-end and block access using an Apache configuration.
- Configure the IP filter in MailID (set the Java system property MailID.ipfilter.network)

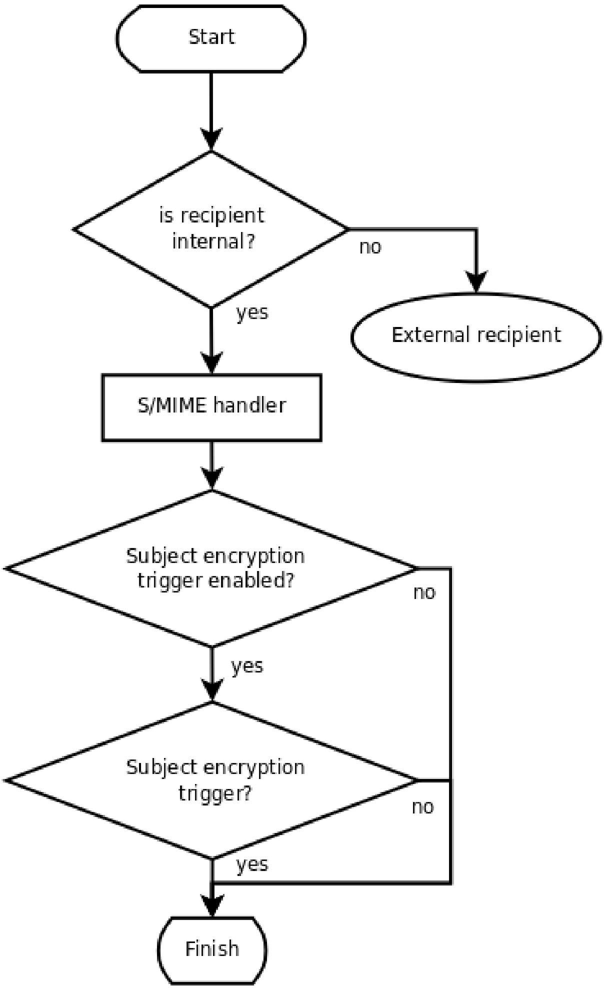
Another option is to install MailID web application with only support for PDF reply (see MailID-external.war).

Installation instructions of any of the above solutions are not discussed in this guide.

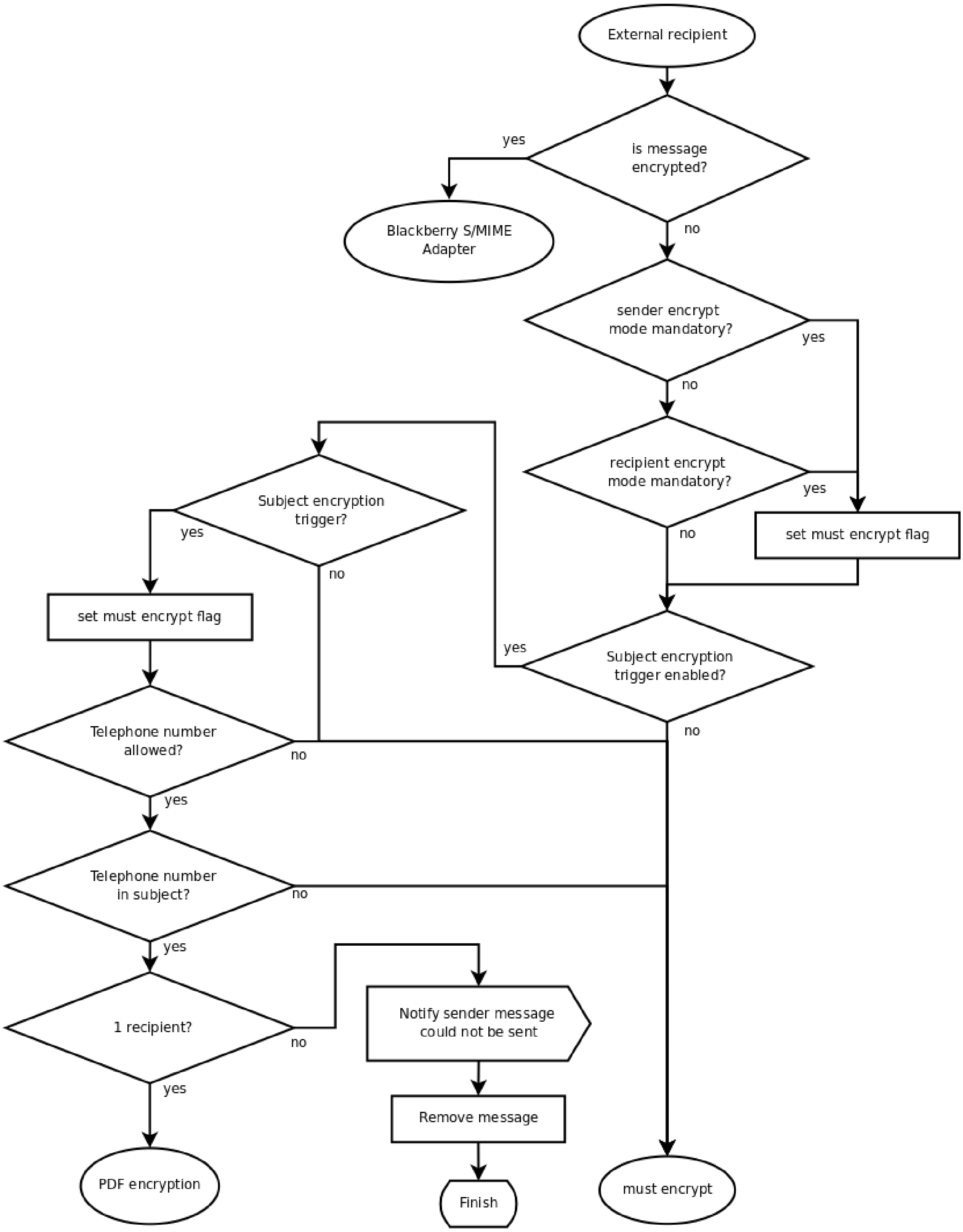
Appendix B

Mail flow

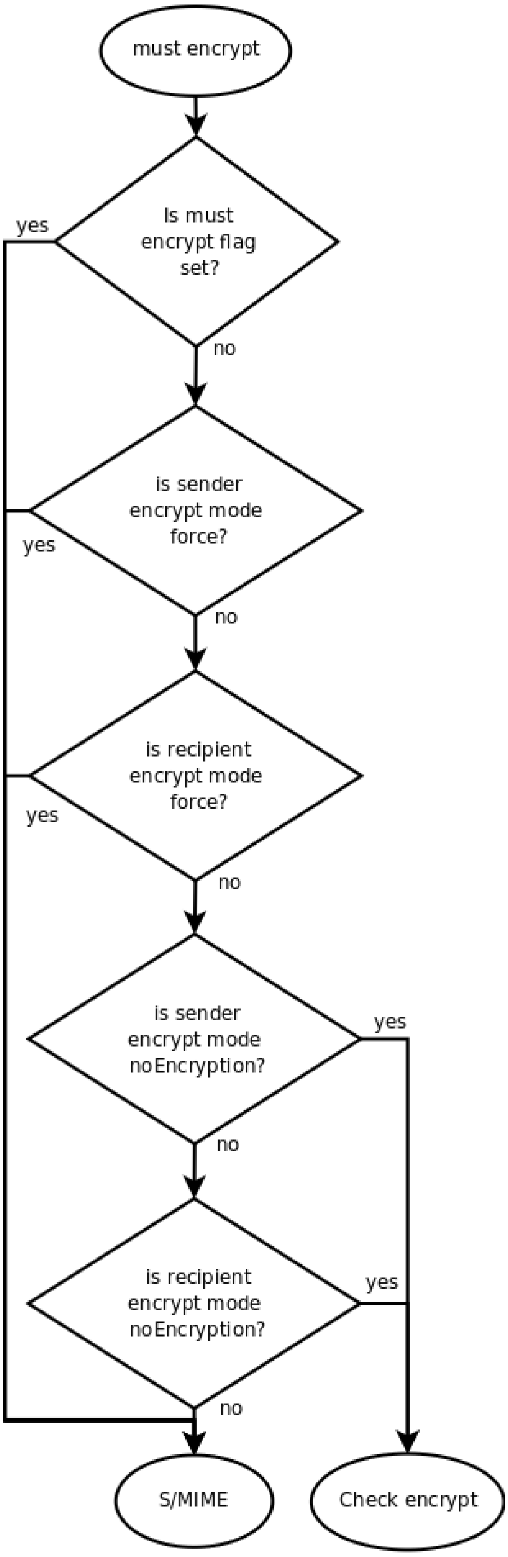
The following flow-charts will show how email is processed by MailID. Because the flow-charts are too big to fit on one page they have been split-up into separate charts.



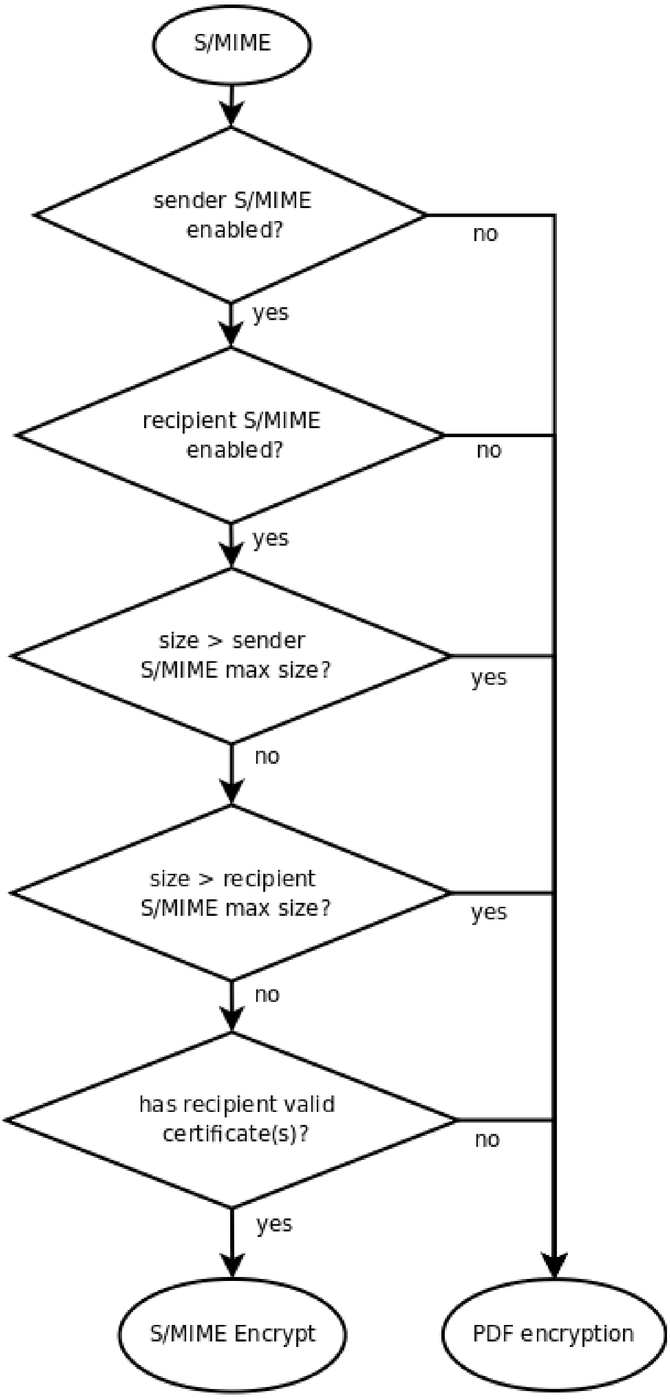
Drawing 1: Start


External recipient
is message encrypted?
yes
Blackberry S/MIME Adapter
no
sender encrypt mode mandatory?
yes
no
recipient encrypt mode mandatory?
yes
no
set must encrypt flag
Subject encryption trigger enabled?
yes
no
Subject encryption trigger?
yes
no
set must encrypt flag
Telephone number allowed?
no
yes
Telephone number in subject?
no
yes
1 recipient?
no
yes
Notify sender message could not be sent
Remove message
Finish
PDF encryption
must encrypt

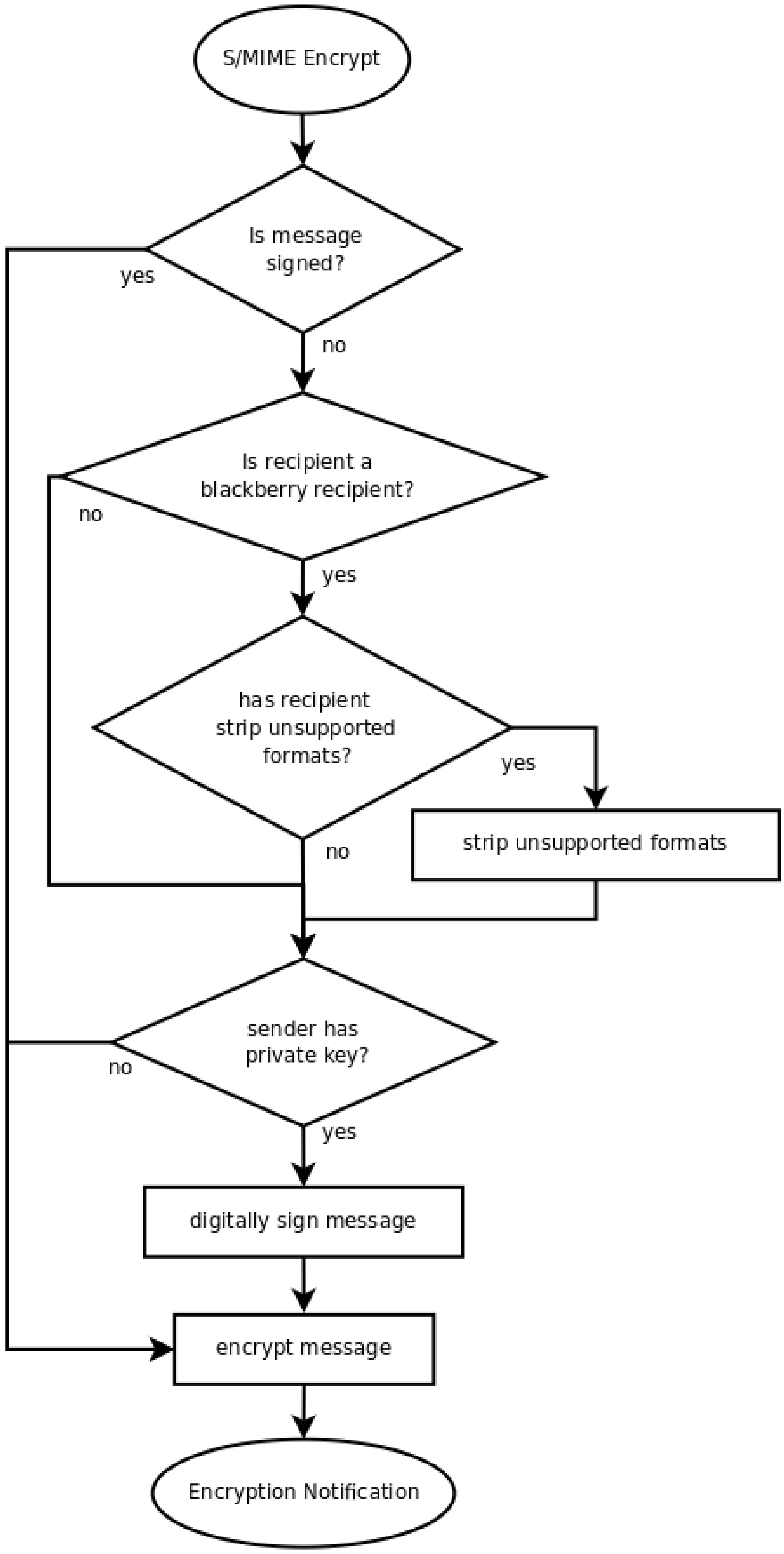
Drawing 2: External recipient


must encrypt
Is must encrypt flag set?
yes
no
is sender encrypt mode force?
yes
no
is recipient encrypt mode force?
yes
no
is sender encrypt mode noEncryption?
yes
no
is recipient encrypt mode noEncryption?
yes
no
S/MIME
Check encrypt

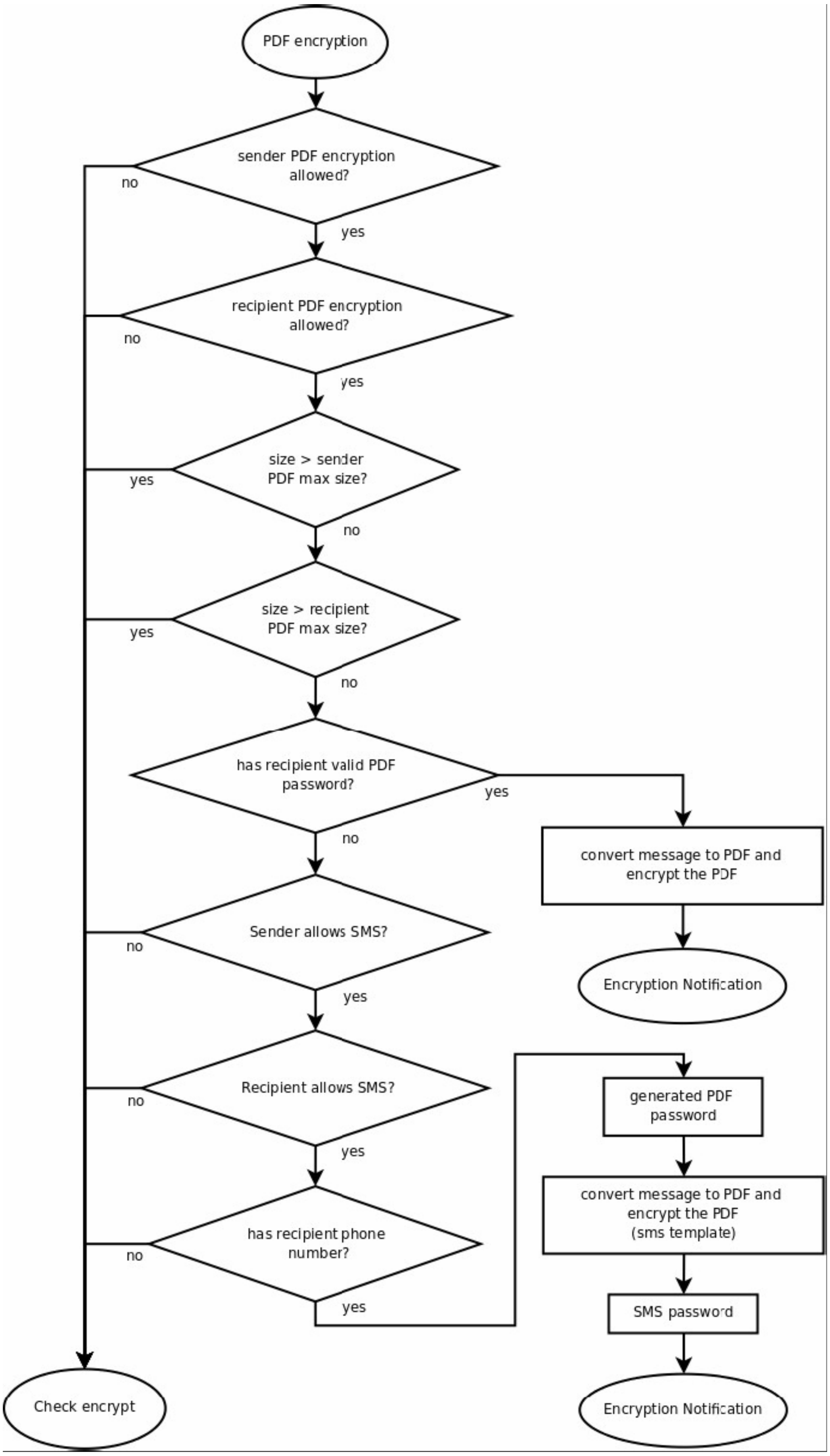
Drawing 3: Must encrypt


S/MIME
sender S/MIME enabled?
no
yes
recipient S/MIME enabled?
no
yes
size > sender S/MIME max size?
yes
no
size > recipient S/MIME max size?
yes
no
has recipient valid certificate(s)?
no
yes
S/MIME Encrypt
PDF encryption

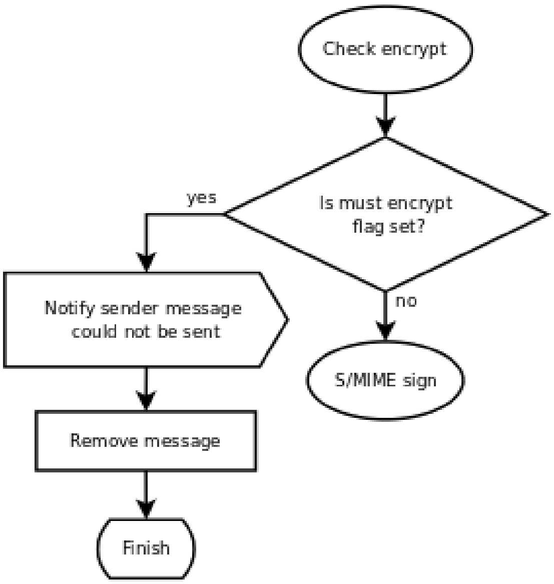
Drawing 4: S/MIME



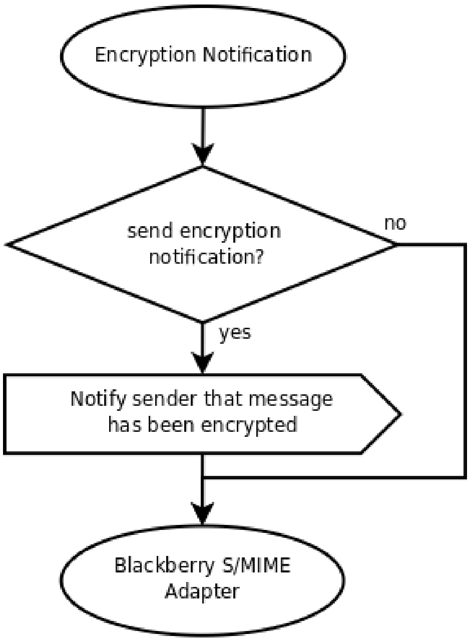
Drawing 5: S/MIME encrypt


PDF encryption
sender PDF encryption allowed?
no
yes
recipient PDF encryption allowed?
no
yes
size > sender PDF max size?
yes
no
size > recipient PDF max size?
yes
no
has recipient valid PDF password?
yes
no
convert message to PDF and encrypt the PDF
Encryption Notification
Sender allows SMS?
no
yes
Recipient allows SMS?
no
yes
generated PDF password
has recipient phone number?
no
yes
convert message to PDF and encrypt the PDF (sms template)
SMS password
Check encrypt
Encryption Notification

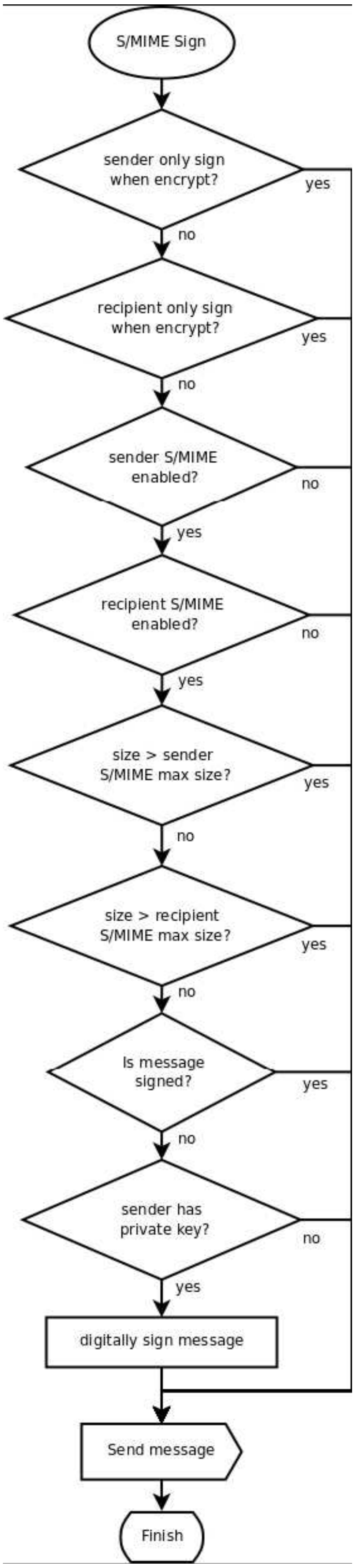
Drawing 6: PDF encrypt


Check encrypt
Is must encrypt flag set?
yes
no
Notify sender message could not be sent
S/MIME sign
Remove message
Finish

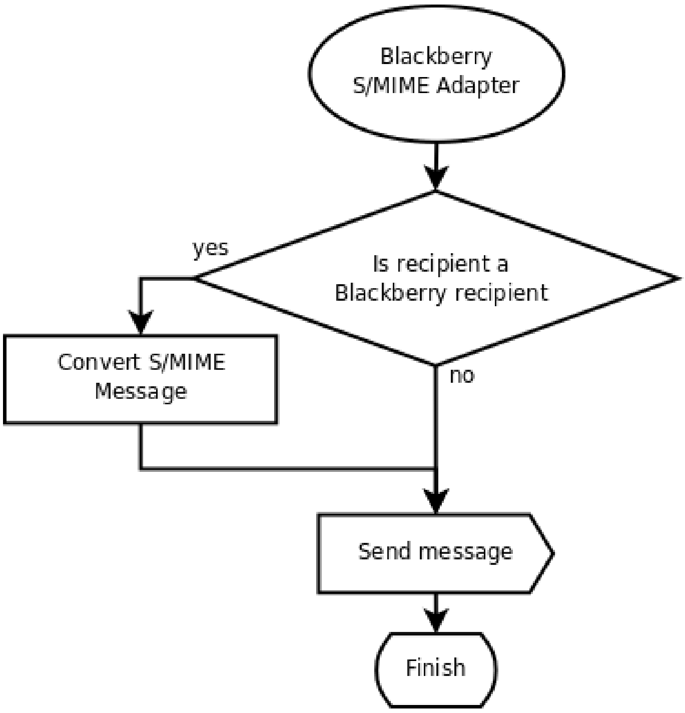
Drawing 7: Check encrypt


Encryption Notification
send encryption notification?
no
yes
Notify sender that message has been encrypted
Blackberry S/MIME Adapter

Drawing 8: Encryption notification



Drawing 9: S/MIME sign


Blackberry S/MIME Adapter
Is recipient a Blackberry recipient
yes
no
Convert S/MIME Message
Send message
Finish

Drawing 10: Blackberry S/MIME adapter

Appendix C

Cron expressions

(examples taken from: www.opensymphony.com)

Here are some full examples:

Expression	Meaning
0 0 12 * * ?	Fire at 12pm (noon) every day
0 15 10 ? * *	Fire at 10:15am every day
0 15 10 * * ?	Fire at 10:15am every day
0 15 10 * * ? *	Fire at 10:15am every day
0 15 10 * * ? 2005	Fire at 10:15am every day during the year 2005
0 * 14 * * ?	Fire every minute starting at 2pm and ending at 2:59pm, every day
0 0/5 14 * * ?	Fire every 5 minutes starting at 2pm and ending at 2:55pm, every day
0 0/5 14,18 * * ?	Fire every 5 minutes starting at 2pm and ending at 2:55pm, AND fire every 5 minutes starting at 6pm and ending at 6:55pm, every day
0 0-5 14 * * ?	Fire every minute starting at 2pm and ending at 2:05pm, every day
0 10,44 14 ? 3 WED	Fire at 2:10pm and at 2:44pm every Wednesday in the month of March.
0 15 10 ? * MON-FRI	Fire at 10:15am every Monday, Tuesday, Wednesday, Thursday and Friday
0 15 10 15 * ?	Fire at 10:15am on the 15th day of every month
0 15 10 L * ?	Fire at 10:15am on the last day of every month
0 15 10 ? * 6L	Fire at 10:15am on the last Friday of every month
0 15 10 ? * 6L	Fire at 10:15am on the last Friday of every month
0 15 10 ? * 6L 2002-2005	Fire at 10:15am on every last friday of every month during the years 2002, 2003, 2004 and 2005
0 15 10 ? * 6#3	Fire at 10:15am on the third Friday of every month
0 0 12 1/5 * ?	Fire at 12pm (noon) every 5 days every month, starting on the first day of the month.
0 11 11 11 11 ?	Fire every November 11th at 11:11am.

⛔ Pay attention to the effects of '?' and '*' in the day-of-week and day-of-month fields!